EBA/GL/2017/05

11/09/2017

Smjernice

Smjernice o procjeni rizika IKT-a u okviru postupka nadzorne provjere i ocjene (SREP)

1. Obveze usklađivanja i izvješćivanja

Status ovih smjernica

1. Ovaj dokument sadrži smjernice izdane na temelju članka 16. Uredbe (EU) br. 1093/20101. 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. Smjernice iznose EBA-ino stajalište o odgovarajućim nadzornim praksama unutar Europskog sustava financijskog nadzora ili o tome kako bi se pravo 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 postupaka), uključujući i u slučajevima kada su smjernice prvenstveno upućene institucijama.

Zahtjevi za izvješćivanje

3. U skladu s člankom 16. stavkom 3. Uredbe (EU) 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 13.11.2017. U slučaju izostanka takve obavijesti unutar ovog 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 uputom „EBA/GL/2017/05”. 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 EBA-inoj internetskoj stranici 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.).

2. Predmet, područje primjene i definicije

Predmet i područje primjene

5. Ovim smjernicama, sastavljenima sukladno članku 107. stavku 3. Direktive 2013/36/EU[2], nastoji se osigurati usklađenost nadzornih praksi pri procjeni rizika informacijsko-komunikacijske tehnologije (IKT) u okviru postupka nadzorne provjere i ocjene (SREP) iz članka 97. Direktive 2013/36/EU koji je dodatno određen u Smjernicama EBA-e o zajedničkim postupcima i metodologijama za postupak nadzorne provjere i ocjene (SREP)[3]. U ovim se Smjernicama osobito određuju kriteriji procjene koje bi nadležna tijela trebala primjenjivati pri nadzornoj procjeni upravljanja i strategija institucija u pogledu IKT-a te pri nadzornoj procjeni izloženosti institucija riziku IKT-a i kontrola IKT-a. Ove su Smjernice sastavni dio Smjernica EBA-e o SREP-u.

6. Nadležna tijela trebala bi primjenjivati ove Smjernice u skladu s razinom primjene SREP-a određenom u Smjernicama EBA-e o SREP-u te u skladu s modelom minimalnog angažmana i zahtjevima o proporcionalnosti koji su njima određeni.

Adresati

7. Ove Smjernice upućene su nadležnim tijelima koja su utvrđena u članku 4. stavku 2. točci (i) Uredbe (EU) br. 1093/2010.

Definicije

8. Ako nije drukčije navedeno, pojmovi upotrijebljeni i definirani u Direktivi 2013/36/EU i Uredbi (EU) br. 575/2013, kao i definicije iz Smjernica EBA-e o SREP-u, imaju isto značenje u ovim Smjernicama. Osim toga, za potrebe ovih Smjernica primjenjuju se sljedeće definicije:

Sustavi IKT-a	IKT koji je uređen kao dio mehanizma ili međusobno povezane mreže koji su podrška poslovanju institucije.
Usluge IKT-a	Usluge koje sustavi IKT-a pružaju unutarnjim ili vanjskim korisnicima. Primjeri obuhvaćaju unos podataka, pohranu podataka, obradu podataka i usluge izvješćivanja, ali i

[2] Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (1) – SL L 176, 27. 6. 2013.

[3] EBA/GL/2014/13

	pomoćne usluge za potrebe praćenja, poslovanja i odlučivanja.
Rizik povezan s dostupnošću i kontinuitetom IKT-a	Rizik od nastanka nepovoljnih utjecaja na rad i dostupnost sustava IKT-a i podataka, uključujući nemogućnost pravodobnog oporavka usluga institucije uslijed kvara hardverskih ili softverskih komponenata IKT-a, manjkavosti upravljanja sustavom IKT-a te ostalih događaja, kako je podrobnije opisano u Prilogu.
Sigurnosni rizik IKT-a	Rizik od neovlaštenog pristupa sustavima IKT-a i podatcima unutar institucije ili izvan nje (npr. kibernetički napadi), kako je podrobnije opisano u Prilogu.
Rizik promjena IKT-a	Rizik koji proizlazi iz nemogućnosti institucija da pravodobno i kontrolirano upravljaju promjenama u sustavu IKT-a, osobito kad je riječ o velikim i složenim programskim promjenama, kako je podrobnije opisano u Prilogu.
Rizik IKT-a povezan s integritetom podataka	Rizik od toga da su podatci koji se pohranjuju i obrađuju u sustavima IKT-a nepotpuni, netočni ili nekonzistentni u različitim sustavima IKT-a, primjerice zbog slabih ili nepostojećih kontrola tijekom raznih faza životnog ciklusa podataka IKT-a (tj. dizajniranja podatkovne arhitekture, izgradnje podatkovnog modela i/ili podatkovnih rječnika, provjere unosa podataka, kontrole izdvajanja podataka, prijenosa i obrade, uključujući i izlazne podatke), čime se narušava mogućnost institucije da ispravno i pravodobno pruža usluge te osigura informacije povezane s upravljanjem (rizikom) i financijske informacije, kako je podrobnije opisano u Prilogu.
Rizik povezan s eksternalizacijom IKT-a	Rizik od toga da angažiranje treće strane ili nekog drugog subjekta grupe (eksternalizacija unutar grupe) radi pružanja sustava IKT-a ili povezanih usluga negativno utječe na rad institucije i njezino upravljanje rizicima, kako je podrobnije opisano u Prilogu.

3. Provedba

Datum primjene

9. Ove Smjernice primjenjuju se od 1. siječnja 2018.

4. Zahtjevi za procjenu rizika IKT-a

Glava 1. – Opće odredbe

10. Nadležna tijela bi u okviru SREP postupka trebala provesti procjenu rizika IKT-a, sustava upravljanja i strategije IKT-a pridržavajući se modela minimalnog angažmana i kriterija proporcionalnosti određenih u glavi 2. Smjernica EBA-e o SREP-u. To ponajprije znači sljedeće:

    a. učestalost procjena rizika IKT-a ovisila bi o modelu minimalnog angažmana koji je uvjetovan kategorijom SREP-a u koju je institucija razvrstana te o konkretnom planu nadzora institucije;

    b. dubina, podrobnost i intenzitet procjene IKT-a trebali bi biti razmjerni veličini, ustroju i operativnim uvjetima institucije, kao i naravi, opsegu i složenosti njezinih aktivnosti.

11. Načelo proporcionalnosti u cijelim se Smjernicama primjenjuje na opseg, učestalost i intenzitet angažmana nadzornih tijela i dijaloga s institucijom te na nadzorna očekivanja standarda koje institucija treba zadovoljiti.

12. Nadležna tijela mogu uzeti u obzir aktivnosti koje su institucija ili nadležno tijelo već obavili u okviru procjena drugih rizika ili elemenata SREP-a te se mogu osloniti na njih kako bi imala na raspolaganju ažuriranu procjenu. Konkretno, pri provedbi procjena iz ovih Smjernica nadležna tijela trebala bi odabrati najprimjereniji pristup i metodologiju nadzorne procjene koji su najprikladniji za određenu instituciju i razmjerni toj instituciji; uz to, nadležna bi tijela trebala upotrijebiti postojeće i dostupne resurse (npr. odgovarajuća izvješća i druge dokumente, sastanke s funkcijama odgovornima za upravljanje (rizicima) , rezultate izravnih nadzora) i temeljiti svoju procjenu na njima.

13. Nadležna tijela trebala bi sažeti rezultate svojih procjena kriterija određenih u ovim Smjernicama i upotrijebiti ih prilikom donošenja zaključaka o procjeni elemenata SREP-a, kako je određeno u Smjernicama EBA-e o SREP-u.

14. Prije svega, iz procjene upravljanja i strategije IKT-a provedene u skladu s glavom 2. ovih Smjernica trebali bi proizaći rezultati na kojima će se temeljiti sažetak nalaza procjene elementa SREP-a koji se odnosi na interno upravljanje i kontrolu na razini institucije, kako je određeno u glavi 5. Smjernica EBA-e o SREP-u, te bi se ta procjena trebala odražavati u ocjeni tog elementa SREP-a. Osim toga, nadležna tijela trebala bi imati na umu da se svi značajni nepovoljni učinci procjene strategije IKT-a na poslovnu strategiju institucije, kao i zabrinutosti da institucija možda nema dovoljno resursa i kapaciteta IKT-a za provedbu i potporu važnih planiranih strateških promjena, trebaju obuhvatiti analizom poslovnog modela u skladu s glavom 4. Smjernica EBA-e o SREP-u.

15. Rezultat procjene rizika IKT-a, kako je određeno u glavi 3. ovih Smjernica, trebao bi se ugraditi u rezultate procjene operativnog rizika te bi se trebalo smatrati da utječe na njezinu ocjenu, kako je određeno glavom 6.4. Smjernica EBA-e o SREP-u.

16. Napominje se da bi nadležna tijela načelno trebala procijeniti potkategorije rizika u okviru glavnih kategorija (tj. rizik IKT-a procijenit će se u sklopu operativnog rizika), no ako nadležna tijela zaključe da su neke potkategorije značajne, te potkategorije mogu procijeniti pojedinačno. Stoga, u slučaju da nadležno tijelo utvrdi da je rizik IKT-a značajan rizik, u ovim se Smjernicama nalazi tablica za ocjenjivanje (tablica 1.) koja se treba upotrebljavati za ocjenjivanje rizika IKT-a kao zasebne kategorije, pridržavajući se općeg pristupa ocjenjivanju rizika za kapital iz Smjernica EBA-e o SREP-u.

17. Kako bi odredila treba li se rizik IKT-a smatrati značajnim te procjenjivati i ocjenjivati kao samostalna kategorija operativnog rizika, nadležna tijela mogu upotrijebiti kriterije navedene u odjeljku 6.1. Smjernica EBA-e o SREP-u.

18. Pri primjeni ovih Smjernica nadležna tijela trebala bi, u slučajevima u kojima je to potrebno, uzeti u obzir nepotpun popis potkategorija rizika IKT-a i scenarija rizika određenih u Prilogu, imajući na umu da je Prilog usmjeren na rizike IKT-a koji mogu prouzročiti vrlo ozbiljne gubitke. Nadležna tijela mogu isključiti neke rizike IKT-a obuhvaćene klasifikacijom ako se ne odnose na njihovu procjenu. Institucije bi trebale uspostaviti vlastite klasifikacije rizika, a ne upotrebljavati klasifikaciju rizika IKT-a iz Priloga.

19. Kada se ove Smjernice primjenjuju na prekogranične grupe banaka i njihove subjekte, a osnovan je kolegij nadzornih tijela, uključena nadležna tijela trebala bi u kontekstu suradnje za potrebe procjene u okviru SREP-a u skladu s odjeljkom 11.1. Smjernica EBA-e o SREP-u koordinirati u najvećoj mogućoj mjeri precizni i detaljni obuhvat svake stavke informacija, jednako za sve subjekte grupe.

Glava 2. – Procjena upravljanja i strategije institucije u pogledu IKT-a

2.1 Opća načela

20. Nadležna tijela trebala bi procijeniti jesu li sustavi IKT-a i povezani rizici propisno obuhvaćeni općim upravljanjem institucije i okvirom unutarnjih kontrola te uvažava li upravljačko tijelo te aspekte i upravlja li njima na primjeren način, s obzirom na to da je IKT iznimno važan za pravilno funkcioniranje institucija.

21. Nadležna tijela trebala bi pri provođenju te procjene slijediti zahtjeve i standarde za dobro interno upravljanje i mehanizme kontrole rizika koji su određeni u Smjernicama EBA-e o internom upravljanju (GL 44)[4] te međunarodnim smjernicama za to područje, u mjeri u kojoj su oni primjenjivi s obzirom na specifičnost sustava i rizika IKT-a.

22. Procjena iz ove glave ne obuhvaća posebne elemente upravljanja sustavima IKT-a, upravljanja rizicima i kontrolama koji su usmjereni na upravljanje specifičnim rizicima IKT-a o kojima je riječ u glavi 3. ovih Smjernica, nego je usmjerena na sljedeća područja:

    a. strategiju IKT-a – ima li institucija strategiju IKT-a kojom se primjereno upravlja i koja je usklađena s poslovnom strategijom institucije;

    b. opće interno upravljanje – jesu li sustavi općeg internog upravljanja institucije primjereni u odnosu na sustave IKT-a institucije;

    c. rizike IKT-a unutar okvira institucije za upravljanje rizicima – jesu li okvirom institucije za upravljanje rizicima i unutarnju kontrolu primjereno zaštićeni sustavi IKT-a institucije.

23. Iako točka a) iz stavka 22. pruža podatke o elementima upravljanja institucije, ponajprije bi se trebala ugraditi u procjenu poslovnog modela iz glave 4. Smjernica EBA-e o SREP-u. Točkama (b) i (c) dopunjuju se procjene područja obuhvaćenih glavom 5. smjernica EBA-e o SREP-u te bi se procjena opisana u ovim Smjernicama trebala ugraditi u odgovarajuću procjenu iz glave 5. Smjernica EBA-e o SREP-u.

24. Rezultate te procjene trebalo bi uzeti u obzir, u slučajevima u kojima su oni relevantni, pri procjeni upravljanja rizicima i kontrola rizika iz glave 3. ovih Smjernica.

2.2 Strategija IKT-a

25. U okviru ovog odjeljka nadležna tijela trebala bi procijeniti postoji li u instituciji strategija IKT-a koju upravljačko tijelo institucije primjereno nadzire, koja je u skladu s poslovnom strategijom, osobito u

[4] Smjernice EBA-e o internom upravljanju, GL 44, 27. rujna 2011.

pogledu redovitog održavanja IKT-a te planiranja i provedbe važnih i složenih promjena povezanih s IKT-om, te koja podupire poslovni model institucije.

2.2.1 Razvoj i primjerenost strategije IKT-a

26. Nadležna tijela trebala bi procijeniti postoji li u instituciji okvir za pripremu i razvoj strategije IKT-a institucije koji je razmjeran prirodi, opsegu i složenosti njezinih aktivnosti povezanih s IKT-om. Pri provedbi te procjene nadležna bi tijela trebala razmotriti sljedeće:

    a. je li više rukovodstvo[5] poslovne linije ili poslovnih linija primjereno uključeno u definiranje strateških prioriteta IKT-a institucije i je li više rukovodstvo funkcije IKT-a upoznato s razvojem, osmišljavanjem i pokretanjem važnih poslovnih strategija i inicijativa kako bi se osigurala stalna usklađenost među sustavima IKT-a, uslugama IKT-a i funkcijom IKT-a (odnosno osobama odgovornima za uvođenje tih sustava i usluga i upravljanje njima) te poslovnom strategijom institucije, kao i učinkovito ažuriranje IKT-a;

    b. je li strategija IKT-a dokumentirana i poduprta konkretnim planovima provedbe, osobito u pogledu ključnih pitanja i planiranja resursa (uključujući financijske i ljudske resurse) kako bi se osiguralo da su realni i kako bi se omogućila provedba strategije IKT-a;

    c. ažurira li institucija redovito svoju strategiju IKT-a, osobito pri promjenama poslovne strategije, kako bi se osigurala stalna usklađenost između IKT-a i srednjoročnih do dugoročnih poslovnih ciljeva, planova i aktivnosti;

    d. odobrava li upravljačko tijelo institucije strategiju IKT-a i provedbene planove te prati li njihovu provedbu.

2.2.2 Provedba strategije IKT-a

27. Ako strategija IKT-a institucije zahtijeva provedbu važnih i složenih promjena povezanih s IKT-om ili promjena koje će značajno utjecati na poslovni model institucije, nadležna tijela trebala bi procijeniti postoji li u instituciji kontrolni okvir primjeren njezinoj veličini, aktivnostima povezanim s IKT-om i razini promjena kojim se osigurava učinkovita provedba strategije IKT-a institucije. Pri provedbi te procjene nadležna bi tijela trebala razmotriti sljedeće:

    a. jesu li kontrolnim okvirom obuhvaćeni postupci upravljanja (npr. praćenje napretka i proračuna te izvješćivanje o njima) i odgovarajuća tijela (npr. ured za upravljanje projektima, koordinacijska skupina za IKT ili odgovarajuće drugo tijelo) koji učinkovito podržavaju provedbu strateških programa IKT-a;

    b. jesu li u kontrolnom okviru definirane i raspodijeljene uloge i odgovornosti za provedbu strateških programa IKT-a, pri čemu posebnu pozornost treba obratiti na iskustvo ključnih dionika koji se bave organizacijom, koordinacijom i praćenjem važnih i složenih promjena povezanih s IKT-om te na upravljanje širim učincima na organizaciju i osoblje (npr. postupanje u slučaju otpora promjenama, osposobljavanje, komunikacija);

[5] Značenje „višeg rukovodstva” i „upravljačkog tijela” u skladu je s definicijama iz Direktive 2013/36/EU od 26. lipnja 2013. iz članka 3. točke 7. za „upravljačko tijelo” i članka 3. točke 9. za „više rukovodstvo”.

c. postoje li u kontrolnom okviru neovisne kontrolne funkcije i funkcija unutarnje revizije koje jamče da se rizici povezani s provedbom strategije IKT-a prepoznaju, procjenjuju i učinkovito smanjuju te da je okvir upravljanja koji je uspostavljen radi provedbe strategije IKT-a učinkovit;

d. sadržava li kontrolni okvir postupak planiranja i revizije planiranja koji je dovoljno fleksibilan i omogućuje reagiranje na važne uočene probleme (npr. probleme s provedbom ili kašnjenja) ili vanjske događaje (npr. važne promjene u poslovnom okruženju, tehnološke probleme ili inovacije) radi osiguravanja pravodobnog prilagođavanja strateškog plana provedbe.

2.3 Opće interno upravljanje

28. U skladu s glavom 5. Smjernica EBA-e o SREP-u nadležna tijela trebala bi procijeniti ima li institucija primjerenu i transparentnu korporativnu strukturu koja „odgovara namjeni" i je li primijenila primjerene postupke upravljanja. S posebnim naglaskom na sustave IKT-a i u skladu sa Smjernicama EBA-e o internom upravljanju tom bi se procjenom trebalo procijeniti i sljedeće:

a. ima li institucija robusnu i transparentnu organizacijsku strukturu s jasnim zaduženjima za IKT, uključujući upravljačko tijelo i njegove odbore, te imaju li ključne osobe odgovorne za IKT (npr. voditelj organizacijske jedinice za informacijsku tehnologiju, voditelj organizacijske jedinice za operacije ili odgovarajuća druga osoba) primjeren izravni ili neizravni pristup upravljačkom tijelu kako bi se osiguralo da se na razini upravljačkog tijela primjereno izvješćuje, raspravlja i odlučuje o važnim informacijama ili pitanjima povezanim s IKT-om;

b. je li upravljačko tijelo institucije upoznato s rizicima povezanim s IKT-om i bavi li se njima.

29. Nastavno na odjeljak 5.2. Smjernica EBA-e o SREP-u nadležna bi tijela trebala procijeniti je li u politici i strategiji eksternalizacije u području IKT-a uzet u obzir, u slučajevima u kojima je to relevantno, učinak eksternalizacije u području IKT-a na poslovanje i poslovni model institucije.

2.4 Rizik IKT-a unutar okvira institucije za upravljanje rizicima

30. Pri procjeni upravljanja rizicima i unutarnjih kontrola u cijeloj instituciji, kako je predviđeno u glavi 5. Smjernica EBA-e o SREP-u, nadležna tijela trebala bi razmotriti jesu li unutar okvira institucije za upravljanje rizicima i okvira unutarnjih kontrola sustavi IKT-a primjereno zaštićeni na način razmjeran veličini i aktivnostima institucije te njezinom profilu rizičnosti u pogledu IKT-a, kako je definirano u glavi 3. Nadležna tijela trebala bi posebice utvrditi sljedeće:

a. jesu li rizici IKT-a, kao dio šire kategorije operativnog rizika, obuhvaćeni sklonošću preuzimanju rizika i postupkom procjene adekvatnosti internog kapitala (ICAAP) pri definiranju opće strategije rizika i određivanju internog kapitala;

b. jesu li rizici IKT-a obuhvaćeni okvirom za upravljanje rizicima i unutarnjih kontrola na razini cijele institucije.

31. Nadležna tijela trebala bi provesti procjenu navedenu pod točkom (a) uzimajući u obzir i očekivane i nepovoljne scenarije, npr. scenarije obuhvaćene testiranjem otpornosti na stres specifičnim za instituciju ili nadzornim testiranjem otpornosti na stres.

32. S posebnim naglaskom na točku (b), nadležna tijela trebala bi procijeniti jesu li funkcije neovisne kontrolne funkcije i funkcija unutarnje revizije, opisane u stavku 104. točkama (a) i (d) te stavku 105. točkama (a) i (c) Smjernica EBA-e o SREP-u, primjerene za osiguravanje dostatne razine neovisnosti između IKT-a i funkcija kontrole i revizije, s obzirom na veličinu institucije i njezin profil rizičnosti u pogledu IKT-a.

2.5 Sažetak nalaza

33. Ti rezultati trebaju se uključiti u sažetak nalaza iz glave 5. Smjernica EBA-e o SREP-u i trebaju biti obuhvaćeni odgovarajućim ocjenama u skladu s razmatranjima iz tablice 3. Smjernica EBA-e o SREP-u.

34. Kada je riječ o procjeni strategije IKT-a, pri zaključivanju navedene procjene potrebno je razmotriti sljedeće:

    a. ako nadležna tijela zaključe da je upravljački okvir institucije neprimjeren za razvoj i provedbu strategije IKT-a institucije iz odjeljka 2.2., onda bi se to trebalo odraziti na procjenu internog upravljanja institucije iz stavka 87. točke (a) glave 5. Smjernica EBA-e o SREP-u;

    b. ako nadležna tijela na temelju procjena iz odjeljka 2.2. zaključe da bi moglo doći do znatnog razilaženja između strategije IKT-a i poslovne strategije koje bi moglo imati znatan nepovoljan utjecaj na dugoročne poslovne i/ili financijske ciljeve institucije, na održivost i/ili poslovni model institucije ili na poslovna područja / poslovne linije institucije koje su u stavku 62. točki (a) Smjernica EBA-e o SREP-u određene kao najznačajnije, onda bi se to trebalo odraziti na procjenu poslovnog modela iz stavka 70. točaka (b) i (c) glave 4. Smjernica o SREP-u;

    c. ako nadležna tijela na temelju procjena iz odjeljka 2.2. zaključe da institucija možda neće imati dostatne resurse IKT-a i provedbene sposobnosti IKT-a za uvođenje i potporu važnih planiranih strateških promjena, to bi trebalo utjecati na procjenu poslovnog modela iz stavka 70. točke (b) glave 4. Smjernica EBA-e o SREP-u.

Glava 3. – Procjena izloženosti institucija riziku IKT-a i kontrola IKT-a

3.1 Opća pitanja

35. Nadležna tijela trebala bi procijeniti je li institucija pravilno utvrdila, procijenila i smanjila svoje rizike IKT-a. Taj postupak trebao bi biti dio okvira upravljanja operativnim rizikom i podudarati se s pristupom koji se primjenjuje na operativni rizik.

36. Nadležna tijela najprije trebaju utvrditi značajne inherentne rizike IKT-a kojima je institucija izložena ili bi mogla biti izložena, a zatim provesti procjenu učinkovitosti okvira institucije za upravljanje rizicima IKT-a te postupaka i kontrola za smanjenje tih rizika. Ishod procjene trebao bi biti obuhvaćen u sažetku nalaza, koji se ugrađuje u ocjenu operativnog rizika iz Smjernica o SREP-u. Ako se rizik IKT-a smatra značajnim i nadležna tijela žele mu dodijeliti zasebnu ocjenu, trebaju mu dodijeliti ocjenu kao podriziku operativnog rizika na temelju tablice 1.

37. Pri provedbi procjene iz ove glave nadležna tijela trebala bi, kao osnovu za utvrđivanje prioriteta nadzorne procjene, upotrijebiti sve dostupne izvore informacija određene u stavku 127. glave 6. Smjernica EBA-e o SREP-u, kao na primjer aktivnosti institucije, izvješća i rezultate u području upravljanja rizicima institucije, . Nadležna tijela trebala bi pri provođenju te procjene upotrijebiti i druge izvore informacija, uključujući i sljedeće, u slučajevima u kojima je to relevantno:

    a. samoprocjene rizika IKT-a i kontrola (ako se navode u informacijama o ICAAP-u);
    b. informacije povezane s rizikom IKT-a dostavljene upravljačkom tijelu institucije, npr. redovita izvješća i izvješća potaknuta incidentima povezanima s rizikom IKT-a (uključujući i bazu podataka operativnih gubitaka) i podatke o izloženosti riziku IKT-a dobivene od funkcije institucije za upravljanje rizicima;
    c. nalaze unutarnjih i vanjskih revizija povezanih s rizikom IKT-a koji su dostavljeni revizorskom odboru institucije.

3.2 Utvrđivanje značajnih rizika IKT-a

38. Nadležna tijela trebala bi utvrditi značajne rizike IKT-a kojima je institucija izložena ili bi mogla biti izložena slijedeći korake opisane u nastavku.

3.2.1 Preispitivanje profila rizičnosti institucije povezanog s IKT-om

39. Pri preispitivanju profila rizičnosti institucije povezanog s IKT-om nadležna tijela trebala bi uzeti u obzir sve relevantne informacije o izloženostima institucije riziku IKT-a, uključujući informacije iz stavka 37., uočene značajne nedostatke ili manjkavosti u organizaciji IKT-a te kontrole na razini institucije iz glave 2. ovih Smjernica i, u slučajevima u kojima je to relevantno, razmjerno preispitati te informacije. Nadležna bi tijela u sklopu tog preispitivanja trebala razmotriti sljedeće:

a. potencijalni učinak značajnog narušavanja sustava IKT-a institucije na financijski sustav na domaćoj ili međunarodnoj razini;
b. je li institucija možda izložena sigurnosnim rizicima IKT-a ili rizicima povezanima s dostupnošću i kontinuitetom IKT-a zbog prekomjernog oslanjanja na internet, visokog stupnja usvajanja inovativnih rješenja IKT-a ili drugih poslovnih distribucijskih kanala koji je mogu učiniti vjerojatnijom metom kibernetičkih napada;
c. je li institucija možda izloženija sigurnosnim rizicima IKT-a, rizicima povezanima s dostupnošću i kontinuitetom IKT-a, rizicima IKT-a povezanim s integritetom podataka ili rizicima promjene IKT-a zbog složenosti (npr. prouzročene spajanjem ili preuzimanjem) ili zastarjelosti svojih sustava IKT-a;
d. provodi li institucija značajne promjene na svojim sustavima IKT-a i/ili svojoj funkciji IKT-a (npr. zbog spajanja, preuzimanja, prodaja ili zbog zamjene svojih ključnih sustava IKT-a), koje bi mogle nepovoljno utjecati na stabilnost ili ispravno funkcioniranje sustava IKT-a i prouzročiti značajne rizike povezane s dostupnošću i kontinuitetom IKT-a, sigurnosne rizike IKT-a, rizike promjene IKT-a ili rizike IKT-a povezane s integritetom podataka;
e. je li institucija eksternalizirala svoje usluge IKT-a ili sustave IKT-a unutar grupe ili izvan nje, što bi je moglo izložiti značajnim rizicima povezanima s eksternalizacijom IKT-a;
f. provodi li institucija agresivne mjere smanjenja troškova IKT-a koje bi mogle prouzročiti smanjenje potrebnih ulaganja u IKT, resursa i stručnog znanja u području informacijskih tehnologija i povećati izloženost svim vrstama rizika IKT-a iz klasifikacije rizika;
g. može li lokacija važnih operativnih i podatkovnih centara povezanih s IKT-om (npr. regije, države) izložiti instituciju prirodnim nepogodama (npr. potresima, poplavama), političkoj nestabilnosti ili radničkim i građanskim nemirima, što bi moglo izazvati značajan porast rizika povezanih s dostupnošću i kontinuitetom IKT-a te sigurnosnih rizika IKT-a.

3.2.2 Preispitivanje ključnih sustava i usluga IKT-a

40. U sklopu postupka utvrđivanja rizika IKT-a s potencijalnim značajnim bonitetnim utjecajem na instituciju nadležna bi tijela trebala preispitati dokumente institucije i donijeti mišljenje o sustavima i uslugama IKT-a koji su ključni za pravilno funkcioniranje, dostupnost, kontinuitet i sigurnost osnovnih aktivnosti institucije.

41. Nadležna tijela radi toga bi trebala preispitati metodologiju i postupke koje je institucija primijenila kako bi odredila ključne sustave i usluge IKT-a, imajući na umu da institucija neke sustave i usluge IKT-a može smatrati ključnima sa stajališta kontinuiteta poslovanja i dostupnosti, sigurnosti (npr. sprečavanje prijevara) i/ili sa stajališta povjerljivosti (npr. povjerljivi podatci). Nadležna tijela trebala bi provesti to preispitivanje imajući na umu da ključni sustavi i usluge IKT-a trebaju ispunjavati barem jedan od sljedećih uvjeta:

a. podupiru osnovne poslovne operacije i distribucijske kanale institucije (npr. bankomate, internetsko i mobilno bankarstvo);
b. podupiru osnovne postupke upravljanja i poslovne funkcije, uključujući upravljanje rizicima (npr. sustav za upravljanje rizicima i sustav za upravljanje riznicom);

c. podliježu posebnim pravnim ili regulatornim zahtjevima (ako postoje) koji nalažu povećanu dostupnost, otpornost, povjerljivost ili sigurnost. Primjerice, zakonski propisi o zaštiti podataka ili moguća ciljana vremena oporavka - RTO (maksimalno vrijeme unutar kojeg se neki sustav ili postupak mora osposobiti nakon incidenta) i ciljane točke oporavka podataka - RPO (maksimalno vrijeme tijekom kojeg se podatci mogu izgubiti u slučaju incidenta) za neke sistemski važne usluge (ako je primjenjivo i u slučajevima u kojima je primjenjivo);

d. obrađuju ili pohranjuju povjerljive ili osjetljive podatke, kojima bi neovlašten pristup mogao znatno utjecati na ugled institucije, njezine financijske rezultate ili na sigurnost i kontinuitet njezina poslovanja (npr. baze podataka s osjetljivim podatcima o klijentima); i/ili

e. osiguravaju osnovne funkcionalnosti koje su nužne za pravilno funkcioniranje institucije (npr. telekomunikacijske usluge i usluge povezivanja, usluge povezane sa sigurnošću IKT-a i kibernetičkom sigurnošću).

3.2.3 Utvrđivanje značajnih rizika IKT-a za ključne sustave i usluge IKT-a

42. Uzimajući u obzir provedena preispitivanja profila rizičnosti institucije u pogledu IKT-a te preispitivanja ključnih sustava i usluga IKT-a, nadležna tijela trebala bi donijeti mišljenje o značajnim rizicima IKT-a koji, prema njihovom nadzornom mišljenju, mogu imati značajan bonitetni utjecaj na ključne sustave i usluge IKT-a institucije.

43. Pri procjeni potencijalnog učinka rizika IKT-a na ključne sustave i usluge IKT-a institucije, nadležna tijela trebala bi razmotriti sljedeće:

a. financijski učinak, uključujući (bez ograničenja) gubitak sredstava ili imovine, potencijalne naknade štete za klijente, pravne i sanacijske troškove, ugovorne odštete, izgubljene prihode;

b. izglede za prekid poslovanja, pri čemu treba razmotriti (bez ograničenja) važnost pogođenih financijskih usluga te broj potencijalno pogođenih klijenata i/ili poslovnica i zaposlenika;

c. potencijalni reputacijski učinak, koji treba razmotriti na temelju važnosti pogođenih bankovnih usluga ili operativnih radnji (npr. krađa podataka o klijentima) te vanjskog profila / vidljivosti pogođenih sustava i usluga IKT-a (npr. sustavi mobilnog ili internetskog bankarstva, POS uređaji, bankomati ili platni sustavi);

d. regulatorni učinak, uključujući mogućnost javnog ukora regulatora, novčane kazne ili čak izmjenu odobrenja za rad;

e. strateški učinak na instituciju, na primjer ako se ugroze ili ukradu strateški proizvodi ili poslovni planovi.

44. Nadležna tijela zatim trebaju mapirati utvrđene rizike IKT-a koji se smatraju značajnima u sljedeće kategorije rizika IKT-a, a dodatni opisi rizika i primjeri za njih nalaze se u Prilogu. Nadležna tijela trebaju razmotriti rizike IKT-a iz Priloga u sklopu procjene iz glave 3.:

a. rizik povezan s kontinuitetom i dostupnošću IKT-a;
b. sigurnosni rizik IKT-a;

c. rizik promjena IKT-a;
d. rizik IKT-a povezan s integritetom podataka;
e. rizik povezan s eksternalizacijom IKT-a.

Mapiranje služi kao pomoć nadležnim tijelima pri određivanju značajnih rizika (ako postoje) te bi ga stoga trebalo pozornije i/ili temeljitije preispitati tijekom sljedećih koraka procjene.

3.3 Procjena kontrola kojima se ublažavaju značajni rizici IKT-a

45. Kako bi procijenila preostalu izloženost institucije riziku IKT-a, nadležna tijela trebala bi preispitati kako institucija utvrđuje, prati, procjenjuje i smanjuje značajne rizike koje su nadležna tijela utvrdila tijekom navedene procjene.

46. U tu bi svrhu nadležna tijela za utvrđene značajne rizike IKT-a trebala preispitati sljedeće primjenjive stavke:

a. politiku upravljanja rizikom IKT-a, postupke i pragove tolerancije rizika;
b. okvir organizacijskog upravljanja i nadzora;
c. obuhvat i rezultate unutarnje revizije;
d. kontrole rizika IKT-a koje su specifične za utvrđeni značajni rizik IKT-a.

47. Pri procjeni bi trebalo uzeti u obzir rezultate analize cjelokupnog okvira za upravljanje rizicima i unutarnjih kontrola iz glave 5. Smjernica EBA-e o SREP-u, kao i upravljanje i strategiju institucije iz glave 2. ovih Smjernica, s obzirom na to da bi značajni nedostatci utvrđeni u tim područjima mogli utjecati na sposobnost institucije da upravlja svojim izloženostima riziku IKT-a i smanjuje ih. U slučajevima u kojima je to relevantno nadležna tijela trebala bi se poslužiti i izvorima informacija iz stavka 37. ovih Smjernica.

48. Nadležna tijela trebala bi izvršiti sljedeće korake procjene na način razmjeran prirodi, opsegu i složenosti aktivnosti institucije te uz primjenu nadzorne provjere koja je primjerena profilu rizičnosti institucije povezanom s IKT-om.

3.3.1 Politika upravljanja rizikom IKT-a, postupci i pragovi tolerancije

49. Nadležna tijela trebala bi preispitati postoje li u instituciji primjerene politike upravljanja rizikom, postupci i pragovi tolerancije za utvrđene značajne rizike IKT-a. Oni mogu obuhvaćeni okvirom za upravljanje operativnim rizikom ili mogu činiti zaseban dokument. Pri toj procjeni nadležna bi tijela trebala uzeti u obzir sljedeće:

a. je li politika upravljanja rizikom formalizirana, je li je odobrilo upravljačko tijelo i sadržava li dostatne smjernice o sklonosti preuzimanju rizika IKT-a, glavnim ciljevima upravljanja rizikom IKT-a i/ili pragovima tolerancije rizika IKT-a koji se primjenjuju. Svi relevantni dionici trebali bi biti obaviješteni o odgovarajućoj politici upravljanja rizikom IKT-a;
b. obuhvaća li mjerodavna politika sve važne elemente za upravljanje utvrđenim značajnim rizicima IKT-a;

c. je li institucija provela postupak i popratne radnje u cilju utvrđivanja (npr. samoprocjena kontrole rizika, analiza scenarija rizika) i praćenja značajnih rizika IKT-a o kojima je riječ; te
d. postoji li u instituciji izvješćivanje o upravljanju rizikom IKT-a kojim se višem rukovodstvu i upravljačkom tijelu pružaju pravodobne informacije i koji omogućava višem rukovodstvu i/ili upravljačkom tijelu da procijeni i prati jesu li planovi i mjere institucije za smanjenje rizika IKT-a u skladu s odobrenom sklonošću preuzimanju rizika i/ili pragovima tolerancije (u slučajevima u kojima je to relevantno) i da prati promjene značajnih rizika IKT-a

3.3.2 Okvir organizacijskog upravljanja i nadzora

50. Nadležna tijela trebala bi procijeniti kako su uloge i zaduženja za upravljanje rizicima ugrađeni i integrirani u unutarnju organizaciju radi upravljanja utvrđenim značajnim rizicima IKT-a i njihovog nadzora. Nadležna bi tijela u tom pogledu trebala procijeniti sljedeće:

a. postoje li u instituciji jasne uloge i zaduženja za utvrđivanje, procjenu, praćenje, smanjenje i nadzor značajnih rizika IKT-a te za izvješćivanje o njima;
b. jesu li zaduženja i uloge povezane s rizicima jasno priopćene, dodijeljene i ugrađene u sve relevantne dijelove (npr. poslovne linije, organizacijska jedinica za informacijske tehnologije) i postupke organizacije, uključujući uloge i zaduženja za prikupljanje i agregiranje informacija o rizicima i izvješćivanje višeg rukovodstva i/ili upravljačkog tijela o njima;
c. izvršavaju li se aktivnosti upravljanja rizikom IKT-a uz dovoljne i kvalitativno primjerene ljudske i tehničke resurse. Kako bi procijenila kredibilitet planova za smanjenje rizika, nadležna tijela trebala bi procijeniti i je li institucija predvidjela dovoljna financijska sredstva ili druge resurse potrebne za njihovu provedbu;
d. je li osigurano primjeno praćenje mjera i odgovor/reakcija od upravljačkog tijela povezanih s važnim nalazima u pogledu rizika IKT-a do kojih su došle neovisne kontrolne funkcije, pri čemu je moguće delegiranje nekih dijelova odboru, ako postoji;
e. bilježi li neovisna kontrolna funkcija i dokumentirano preispituje iznimke od mjerodavnih odredbi i politika o IKT-u i izvješćuje li o njima, s posebnim naglaskom na povezane rizike.

3.3.3 Obuhvat i nalazi unutarnje revizije

51. Nadležna tijela trebala bi razmotriti je li funkcija unutarnje revizije učinkovita u pogledu revizije okvira za kontrolu rizika IKT-a, preispitujući sljedeće:

a. jesu li revizije kontrolnog okvira za rizike IKT-a dovoljno kvalitetne, temeljite, učestale i razmjerne veličini, aktivnostima i profilu rizičnosti institucije u pogledu IKT-a;
b. jesu li planom revizije obuhvaćene revizije ključnih rizika IKT-a koje je institucija utvrdila;
c. je li upravljačko tijelo obaviješteno o važnim nalazima revizija IKT-a, uključujući dogovorene mjere; te
d. jesu li poduzete daljnje aktivnosti povezane s nalazima revizija IKT-a, uključujući dogovorene mjere i provjerava li više rukovodstvo i/ili revizorski odbor redovito izvješća o napretku.

3.3.4 Kontrole rizika IKT-a koje su specifične za utvrđene značajne rizike IKT-a

52. Kad je riječ o utvrđenim značajnim rizicima IKT-a, nadležna tijela trebala bi procijeniti je li institucija uspostavila specifične kontrole namijenjene rješavanju tih rizika. U odjeljcima u nastavku naveden je nepotpun popis specifičnih kontrola koje je potrebno razmotriti pri procjeni značajnih rizika utvrđenih u skladu s točkom 3.2.3., koji su klasificirani u sljedeće kategorije rizika IKT-a:

    a. rizici povezani s kontinuitetom i dostupnošću IKT-a;
    b. sigurnosni rizici IKT-a;
    c. rizici promjena IKT-a;
    d. rizici IKT-a povezani s integritetom podataka;
    e. rizici povezani s eksternalizacijom IKT-a.

(a) Kontrole za upravljanje značajnim rizicima povezanima s kontinuitetom i dostupnošću IKT-a

53. Uz zahtjeve iz Smjernica EBA-e o SREP-u (stavci od 279. do 281) nadležna tijela trebala bi procijeniti i postoji li u instituciji primjeren okvir za utvrđivanje, razumijevanje, mjerenje i smanjenje rizika povezanih s kontinuitetom i dostupnošću IKT-a.

54. Pri toj procjeni nadležna bi tijela ponajprije trebala razmotriti sljedeće:

    a. jesu li okvirom utvrđeni ključni procesi/postupci IKT-a i odgovarajući podržavajući sustavi IKT-a koji bi trebali biti obuhvaćeni planovima za poslovnu otpornost i kontinuitet poslovanja s pomoću:

        i. sveobuhvatne analize međuovisnosti ključnih poslovnih procesa/postupaka i podržavajućih sustava;

        ii. određivanja ciljeva oporavka za podržavajuće sustave IKT-a (npr. obično određeni poslovanjem i/ili odredbama u pogledu ciljanih vremena oporavaka – RTO ili i ciljanih točki oporavka podataka - RPO);

        iii. primjerenih kriznih planova kojima se omogućuju dostupnost, kontinuitet poslovanja i oporavak ključnih sustava i usluga IKT-a kako bi se poremećaji u poslovanju institucije sveli na prihvatljive razine.

    b. jesu li okvirom obuhvaćene politike i standardi poslovne otpornosti i kontrolna okruženja kontinuiteta poslovanja te operativne kontrole koje obuhvaćaju:

        i. mjere kojima se izbjegava mogućnost da samo jedan scenarij, incident ili katastrofa utječu i na sustave IKT-a za produkciju i za oporavak;

        ii. postupke izrade pričuvnih kopija i oporavka za ključnu programsku opremu i podatke, kojima se jamči da su pričuvne kopije podataka pohranjene na sigurnom i dovoljno udaljenom mjestu kako incident ili katastrofa ne bi mogli uništiti ili oštetiti te ključne podatke;

        iii. sustave praćenja za pravodobno otkrivanje incidenata povezanih s dostupnošću ili kontinuitetom IKT-a;

iv. dokumentiran proces/postupak za upravljanje incidentima i eskalaciju, kojim su obuhvaćene i smjernice za razne uloge i zaduženja u području upravljanja incidentima i eskalacijama, za članove kriznog odbora ili kriznih odbora i za zapovjedni lanac u slučaju kriznih situacija;

v. fizičke mjere za zaštitu ključnih dijelova infrastrukture IKT-a institucije (npr. podatkovni centri) od rizika povezanih s okolišem (npr. poplava i drugih prirodnih nepogoda) i za osiguravanje primjerenog operativnog okruženja za sustave IKT-a (npr. klimatizacijski uređaji);

vi. postupke, uloge i zaduženja kojima se osigurava da su i eksternalizirani sustavi i usluge IKT-a obuhvaćeni primjerenim rješenjima i planovima otpornosti i kontinuiteta poslovanja;

vii. rješenja za planiranje i praćenje performansi te kapaciteta za ključne sustave i usluge IKT-a u skladu s definiranim zahtjevima u pogledu dostupnosti, u cilju pravodobnog uočavanja ograničenja povezanih s performansama i kapacitetom;

viii. rješenja za zaštitu ključnih aktivnosti ili usluga pruženih putem interneta (npr. usluge internetskog bankarstva), u slučajevima u kojima je to nužno i primjereno, od uskraćivanja usluga ili drugih internetskih kibernetičkih napada s ciljem sprečavanja ili ometanja pristupa tim aktivnostima i uslugama.

c. provode li se unutar okvira testiranja rješenja za dostupnost i kontinuitet IKT-a, uvažavajući niz realističnih scenarija, među kojima su i kibernetički napadi, testiranja prebacivanjem na zamjenske sustave i testiranja pričuvnih kopija za ključne programe i podatke, koja:

i. su planirana, formalizirana i dokumentirana, a rezultati testiranja upotrebljavaju se za poboljšanje učinkovitosti rješenja za dostupnost i kontinuitet IKT-a;

ii. obuhvaćaju dionike i funkcije unutar organizacije, kao što je rukovodstvo poslovnih linija, uključujući tim za kontinuitet poslovanja te tim za odgovor na incidente i krizne situacije, kao i relevantne vanjske dionike;

iii. imaju primjerenu razinu uključenosti upravljačkog tijela i višeg rukovodstva (npr. u sklopu timova za upravljanje kriznim situacijama) te ih se obavještava o rezultatima testiranja.

(b) Kontrole za upravljanje značajnim sigurnosnim rizicima IKT-a

55. Nadležna tijela trebala bi procijeniti postoji li u instituciji učinkovit okvir za utvrđivanje, razumijevanje, mjerenje i smanjenje sigurnosnog rizika IKT-a. Pri toj procjeni nadležna bi tijela ponajprije trebala razmotriti obuhvaća li taj okvir sljedeće:

a. jasno definirane uloge i zaduženja u pogledu:

i. svih osoba i/ili odbora zaduženih i/ili odgovornih za svakodnevno sigurnosno upravljanje IKT-om i za razvoj općih sigurnosnih politika IKT-a, s posebnim naglaskom na potrebu za njihovom neovisnošću;

ii. osmišljavanja, provedbe i praćenja sigurnosnih kontrola IKT-a te upravljanja njima;

iii. zaštite ključnih sustava i usluga IKT-a usvajanjem, primjerice, postupaka za provjeru ranjivosti, upravljanja programskim zakrpama, zaštite na krajnjim točkama (npr. od zlonamjernih sadržaja ili virusa) i alata za detekciju i sprečavanje upada;
iv. praćenja i razvrstavanja vanjskih ili unutarnjih sigurnosnih incidenata IKT-a te postupanja s njima, uključujući reagiranje na incidente te ponovno osposobljavanje i oporavak sustava i usluga IKT-a;
v. redovitih i proaktivnih procjena prijetnji kojima se osiguravaju primjerene sigurnosne kontrole.

b. sigurnosnu politiku IKT-a koja uzima u obzir međunarodno priznate sigurnosne standarde i načela IKT-a (npr. načelo „najmanjih povlastica“ u upravljanju pristupnim pravima, odnosno ograničavanje pristupa na najmanju moguću razinu s kojom će biti moguće normalno funkcioniranje i načelo „obrane u dubinu“ u dizajniranju sigurnosne arhitekture, tj. slojeviti sigurnosni mehanizmi kojima se povećava sigurnost cijelog sustava) i koja ih se pridržava u slučajevima u kojima je to primjereno;

c. postupak za utvrđivanje sustava, usluga i razmjernih sigurnosnih zahtjeva IKT-a, koji su razmjerni mogućem riziku od prijevara i/ili mogućoj pogrešnoj uporabi i/ili zlouporabi povjerljivih podataka, te dokumentiranih sigurnosnih očekivanja kojih se treba pridržavati kad je riječ o tim utvrđenim sustavima, uslugama i podatcima, koji su usklađeni s tolerancijom rizika institucije i čija se ispravna provedba nadgleda;

d. dokumentiran postupak za upravljanje sigurnosnim incidentima i eskalaciju, kojim se pružaju smjernice za razne uloge i zaduženja povezana s upravljanjem incidentima i eskalacijama, za članove kriznog odbora ili kriznih odbora i za zapovjedni lanac u slučaju sigurnosnih kriznih situacija;

e. evidentiranje aktivnosti korisnika i administratora radi učinkovitog praćenja i pravodobnog uočavanja neovlaštenih aktivnosti i reagiranja na njih te radi olakšavanja i provedbe istraga o sigurnosnim incidentima. U instituciji trebaju postojati politike upravljanja zapisima kojima su definirane primjerene vrste zapisa koje se trebaju bilježiti, kao i razdoblje njihova čuvanja;

f. kampanje ili inicijative s ciljem podizanja svijesti i informiranja kojima će se sve razine institucije informirati o sigurnoj uporabi i zaštiti sustava IKT-a institucije te o glavnim sigurnosnim (i drugim) rizicima IKT-a kojih trebaju biti svjesni, osobito u pogledu postojećih i novorazvijenih kibernetičkih prijetnji (npr. računalni virusi, moguće unutarnje ili vanjske zlouporabe ili napadi, kibernetički napadi) i njihove uloge u ublažavanju povreda sigurnosti;

g. primjerene fizičke sigurnosne mjere (npr. nadzorne kamere, protuprovalni alarm, sigurnosna vrata) za sprječavanje neovlaštenog fizičkog pristupa ključnim i osjetljivim sustavima IKT-a (npr. podatkovni centri);

h. mjere za zaštitu sustava IKT-a od internetskih napada (tj. kibernetičkih napada) ili napada iz drugih vanjskih mreža (npr. tradicionalne telekomunikacijske veze ili veze s pouzdanim partnerima). Nadležna tijela trebala bi preispitati obuhvaća li okvir institucije sljedeće:

    i. postupak i rješenja za održavanje potpune i ažurne evidencije i pregleda svih izloženih točaka za povezivanje na mrežu (npr. internetske stranice, internetske aplikacije, *Wi-Fi*, pristup na daljinu) kroz koje bi treće strane mogle neovlašteno pristupiti internim sustavima IKT-a;

ii. strogo nadgledane sigurnosne mjere kojima se temeljito upravlja (npr. vatrozidi, *proxy* poslužitelji, posredovatelji elektroničke pošte, antivirusni programi i programi za skeniranje sadržaja) i koji služe za osiguravanje ulaznog i izlaznog mrežnog prometa (primjerice, elektronička pošta) i izloženih točaka za povezivanje na mrežu kroz koje bi treće strane mogle neovlašteno pristupiti internim sustavima IKT-a;

iii. postupke i rješenja za osiguravanje internetskih stranica i aplikacija koje se mogu izravno napasti s interneta i/ili izvana, koje bi služile kao ulazna točka u interne sustave IKT-a. Oni općenito obuhvaćaju kombinaciju priznatih sigurnih razvojnih praksi, praksi za ojačavanje sustava IKT-a i skeniranje ranjivosti i/ili provedbu dodatnih sigurnosnih rješenja poput vatrozida za aplikacije i/ili sustava za detekciju i/ili sprečavanje upada;

iv. povremeno provođenje sigurnosnih penetracijskih testiranja radi procjene učinkovitosti implementiranih kibernetičkih i internih sigurnosnih mjera i provedenih postupaka povezanih s IKT-om. Ta testiranja trebali bi provoditi zaposlenici i/ili vanjski stručnjaci koji raspolažu potrebnim stručnim znanjima, a dokumentirani rezultati testiranja i zaključci trebali bi se dostaviti višem rukovodstvu i/ili upravljačkom tijelu. U slučajevima u kojima je to potrebno i primjenjivo institucija bi iz tih testiranja trebala uvidjeti u kojim područjima treba dodatno unaprijediti sigurnosne kontrole i postupke i/ili dobiti bolje jamstvo njihove učinkovitosti.

(c) Kontrole za upravljanje značajnim rizicima promjena IKT-a

56. Nadležna tijela trebala bi procijeniti postoji li u instituciji učinkovit okvir za utvrđivanje, razumijevanje, mjerenje i smanjenje rizika promjena IKT-a, razmjeran prirodi, opsegu i složenosti aktivnosti institucije i profilu rizičnosti institucije u pogledu IKT-a. Okvir institucije trebao bi obuhvatiti rizike povezane s razvojem, testiranjem i odobravanjem promjena u sustavima IKT-a, uključujući razvoj ili promjenu programske opreme, prije uvođenja u produkcijsko okruženje te osigurati primjereno upravljanje životnim ciklusom IKT-a. Pri toj procjeni nadležna bi tijela ponajprije trebala razmotriti obuhvaća li taj okvir sljedeće:

a. dokumentirane postupke za upravljanje i kontroliranje promjena u sustavima IKT-a (npr. upravljanje konfiguracijama i zakrpama) te nad podatcima (npr. popravljanje grešaka i ispravak podataka), kojima se osigurava odgovarajuća primjena upravljanja rizikom IKT-a kad je riječ o važnim promjenama IKT-a koje bi mogle znatno utjecati na profil rizičnosti institucije ili njezinu izloženost riziku;

b. detalje povezane s potrebnom segregacijom dužnosti tijekom raznih faza postupaka uvođenja promjena IKT-a (npr. osmišljavanje i razvoj rješenja, testiranje i odobravanje novih programa i/ili promjena, migracija i implementacija u produkcijskom okruženju, popravljanje grešaka), s posebnim naglaskom na implementirana rješenja i podjelu zaduženja radi upravljanja i kontrole promjena koje zaposlenici IKT-a (npr. razvojni programeri, administratori sustava IKT-a, administratori baza podataka) ili neka druga strana (npr. poslovni korisnici, pružatelji usluga) unose u produkcijske sustave IKT i nad pripadnih podacima;

c. okruženja za testiranje koja primjereno odgovaraju produkcijskim okruženjima;

d. evidenciju postojećih aplikacija i sustava IKT-a u produkcijskom okruženju, kao i u testnom i razvojnom okruženju, kako bi se potrebne promjene (npr. ažuriranja ili nadogradnje verzija, zakrpe sustava, konfiguracijske promjene) mogle pravilno provesti i pratiti te kako bi se njima moglo upravljati kad je riječ o tim sustavima IKT-a;

e. postupke upravljanja i praćenja životnog ciklusa sustava IKT-a koji se upotrebljavaju ,kako bi se zajamčilo da i dalje zadovoljavaju i podržavaju stvarne poslovne zahtjeve i zahtjeve povezane s upravljanjem rizicima te kako bi se osiguralo da dobavljači još podržavaju rješenja i sustave IKT-a koji se upotrebljavaju, a ti postupci trebali bi biti popraćeni odgovarajućim postupcima povezanim sa životnim ciklusom razvoja programske podrške;

f. sustav kontrole izvornog programskog koda i primjerene postupke za sprječavanje neovlaštenih izmjena izvornog programskog koda razvijenog unutar institucije;

g. postupak za provjeru sigurnosti i ranjivosti novih ili značajno izmijenjenih sustava ili programske podrške IKT-a, prije nego što se uvedu u produkciju i izlože mogućim kibernetičkim napadima;

h. postupak i rješenja za sprječavanje neovlaštenog ili nenamjernog otkrivanja povjerljivih podataka pri zamjeni, arhiviranju, uklanjanju ili uništavanju sustava IKT-a;

i. neovisan postupak provjere i validacije kako bi se smanjio rizik ljudske pogreške pri izvršavanju promjena na sustavima IKT-a koje bi mogle imati važan nepovoljan učinak na dostupnost, kontinuitet ili sigurnost poslovanja institucije (npr. važne promjene u konfiguraciji vatrozida) ili samo na sigurnost institucije (npr. promjene vatrozida).

(d) Kontrole za upravljanje značajnim rizicima IKT-a povezanim s integritetom podataka

57. Nadležna tijela trebala bi procijeniti postoji li u instituciji učinkovit okvir za utvrđivanje, razumijevanje, mjerenje i smanjenje rizika IKT-a povezanog s integritetom podataka, razmjeran prirodi, opsegu i složenosti aktivnosti institucije i profilu rizičnosti institucije u pogledu IKT-a. U okviru institucije trebalo bi uzeti u obzir rizike povezane s očuvanjem integriteta podataka koji su pohranjeni u sustavima IKT-a i koje ti sustavi obrađuju. Pri toj procjeni nadležna bi tijela ponajprije trebala razmotriti obuhvaća li taj okvir sljedeće:

a. politiku kojom se utvrđuju uloge i zaduženja za upravljanje integritetom podataka u sustavima IKT-a (npr. arhitekti podataka, službenici za podatke[6], skrbnici za podatke[7], vlasnici/nadzornici podataka[8]) i osiguravaju smjernice za utvrđivanje podataka koji su ključni s gledišta integriteta podataka i na koje bi se trebale primjenjivati posebne kontrole IKT-a (npr. kontrole validacije automatiziranog unosa, kontrole prijenosa podataka, usklađivanje itd.) ili provjere IKT-a (npr. provjera kompatibilnosti s arhitekturom podataka) u raznim fazama životnog ciklusa podataka IKT-a;

[6] Službenici za podatke zaduženi su za obradu i uporabu podataka.

[7] Skrbnici za podatke zaduženi su za sigurno čuvanje, prijenos i pohranu podataka.

[8] Nadzornici podataka zaduženi su za upravljanje podatkovnim elementima i njihovu ispravnost, što se odnosi i na sadržaj i na metapodatke.

b. dokumentiranu arhitekturu podataka, model podataka i/ili rječnik podataka, koji su validirani s relevantnim poslovnim dionicima i dionicima iz područja informacijske tehnologije kako bi se osigurala potrebna konzistencija podataka u svim sustavima IKT-a i kako bi se osiguralo da su arhitektura podataka, model podataka i/ili rječnik podataka usklađeni s poslovnim potrebama i potrebama u pogledu upravljanja rizicima;

c. politiku povezanu s dopuštenom uporabom programskih rješenja/alata razvijenih od strane krajnjih korisnika i oslanjanjem na njih, osobito u pogledu utvrđivanja, registriranja i dokumentiranja važnih programskih rješenja razvijenih od krajnjih korisnika (npr. pri obradi važnih podataka) te s očekivanim razinama sigurnosti za sprečavanje neovlaštenih izmjena samog alata, ali i podataka pohranjenih u njemu;

d. dokumentirane postupke za postupanje s iznimkama za rješavanje uočenih problema povezanih s integritetom podataka IKT-a u skladu s njihovom važnošću i osjetljivošću.

58. U slučaju nadziranih institucija koje su obuhvaćene Načelima BCBS-a br. 239 za učinkovito agregiranje podatka o riziku i izvješćivanje o riziku[9] nadležna tijela trebala bi preispitati analizu rizika institucije povezanu s njezinim mogućnostima za izvješćivanje o riziku i agregiranje podataka u odnosu na načela i pripremljenu dokumentaciju o tome, uzimajući u obzir vremenski okvir provedbe i prijelazne odredbe u tim načelima.

(e) Kontrole za upravljanje značajnim rizicima povezanim s eksternalizacijom IKT-a

59. Nadležna tijela trebala bi procijeniti, sukladno zahtjevima iz Smjernica za eksternalizaciju Odbora europskih nadzornih tijela za bankarstvo (CEBS) iz 2006. i nastavno na zahtjev iz stavka 85. točke (d) Smjernica EBA-e o SREP-u, primjenjuje li se strategija institucije za eksternalizaciju na primjeren način na eksternalizaciju IKT-a, uključujući eksternalizaciju unutar grupe. Pri procjeni rizika povezanih s eksternalizacijom IKT-a nadležna tijela trebala bi imati na umu da rizici povezani s eksternalizacijom IKT-a mogu biti obuhvaćeni procjenom inherentnih operativnih rizika iz stavka 240. točke (j) Smjernica EBA-e o SREP-u kako bi se izbjeglo dvostruko obavljanje posla ili dvostruki obračun.

60. Nadležna tijela osobito bi trebala procijeniti postoji li u instituciji učinkovit okvir za utvrđivanje, razumijevanje i mjerenje rizika povezanog s eksternalizacijom IKT-a i, prije svega, postoje li kontrole i kontrolna okruženja za smanjenje rizika povezanih s ključnim eksternaliziranim uslugama IKT-a, koji su razmjerni veličini i aktivnostima institucije te njezinom profilu rizičnosti u pogledu IKT-a, a obuhvaćaju sljedeće:

a. procjenu utjecaja eksternalizacije IKT-a na upravljanje rizikom institucije povezano s angažiranjem pružatelja usluga (npr. pružatelji usluga u oblaku) i korištenjem njihovih usluga tijekom postupka nabave, koja se dokumentira i koju više rukovodstvo ili upravljačko tijelo uzima u obzir pri odlučivanju o eksternalizaciji usluga. Institucija bi trebala preispitati politike upravljanja rizikom IKT-a, kontrole IKT-a i kontrolno okruženje pružatelja usluga kako bi osigurala da zadovoljavaju ciljeve i sklonosti preuzimanju rizika povezane s internim upravljanjem rizikom institucije. To

[9] Bazelski odbor za nadzor banaka, Načela za učinkovito agregiranje podatka o riziku i izvješćivanje o riziku, siječanj 2013., dostupno na internetskoj stranici http://www.bis.org/publ/bcbs239.pdf.

preispitivanje trebalo bi se povremeno ažurirati tijekom ugovornog razdoblja eksternalizacije, uzimajući u obzir značajke eksternaliziranih usluga;

b. praćenje rizika IKT-a povezanih s eksternaliziranim aktivnostima tijekom ugovornog razdoblja eksternalizacije kao dijela upravljanja rizicima institucije, koje se ugrađuje u izvješćivanje institucije o upravljanju rizikom IKT-a (npr. izvješćivanje o kontinuitetu poslovanja, izvješćivanje o sigurnosti);

c. praćenje i usporedbu primljenih razina usluga s ugovorno dogovorenim razinama usluga, koje bi trebale biti sastavni dio ugovora o eksternalizaciji ili ugovora o razini usluga;

d. primjerenost zaposlenika, resursa i kompetencija za praćenje rizika IKT-a koji proizlaze iz eksternaliziranih aktivnosti i za upravljanje njima.

3.4 Sažetak nalaza i ocjena

61. Nakon provođenja navedene procjene nadležna tijela trebala bi donijeti mišljenje o riziku IKT-a institucije. To mišljenje trebalo bi biti obuhvaćeno sažetkom nalaza, koje nadležna tijela trebaju uzeti u obzir pri dodjeljivanju ocjene o operativnom riziku u skladu s tablicom 6. Smjernica EBA-e o SREP-u. Nadležna tijela trebala bi svoje mišljenje temeljiti na značajnim rizicima IKT-a, a pri procjeni operativnog rizika trebala bi uzeti u obzir sljedeća razmatranja:

a. razmatranja o riziku

i. profil rizičnosti institucije u pogledu IKT-a i njezina izloženost riziku IKT-a;
ii. utvrđeni najvažniji sustavi i usluge IKT-a;
iii. značajnost rizika IKT-a u pogledu najvažnijih sustava IKT-a.

b. razmatranja o upravljanju i kontrolama

i. jesu li politika i strategija upravljanja rizikom IKT-a institucije usklađene s njezinom općom strategijom i sklonosti preuzimanju rizika;
ii. je li organizacijski okvir za upravljanje rizikom IKT-a robustan i postoje li u njemu jasna zaduženja i jasna podjela zadataka između vlasnika rizika, s jedne strane, te upravljačkih i kontrolnih funkcija, s druge strane;
iii. jesu li sustavi za mjerenje i praćenje rizika IKT-a te za izvješćivanje o njemu primjereni;
iv. jesu li kontrolni okviri za značajne rizike IKT-a stabilni.

62. Ako nadležna tijela smatraju da je rizik IKT-a značajan i nadležno tijelo odluči procijeniti i procijeniti taj rizik kao potkategoriju operativnog rizika, razmatranja za ocjenjivanje rizika IKT-a nalaze se u nastavku (tablica 1.).

Tablica 1.: nadzorna razmatranja za dodjelu ocjene riziku IKT-a

Ocjena rizika	Mišljenje nadzornih tijela	Razmatranja o inherentnom riziku	Razmatranja o odgovarajućem upravljanju i kontrolama
1	Ne postoji primjetan rizik značajnog	• Izvori informacija koja treba razmotriti sukladno stavku 37. nisu	

	bonitetnog učinka na instituciju uzimajući u obzir razinu inherentnog rizika te upravljanje i kontrole.	pokazali nikakve znatne izloženosti riziku IKT-a. • Priroda profila rizičnosti institucije povezanog s IKT-om u kombinaciji s provjerom najvažnijih sustava IKT-a i značajnih rizika IKT-a za sustave i usluge IKT-a nije pokazala nikakve značajne rizike IKT-a.	
2	Postoji nizak rizik značajnog bonitetnog učinka na instituciju uzimajući u obzir razinu inherentnog rizika te upravljanje i kontrole.	• Izvori informacija koje treba razmotriti sukladno stavku 37. nisu pokazali nikakve znatne izloženosti riziku IKT-a. • Priroda profila rizičnosti institucije povezanog s IKT-om u kombinaciji s provjerom najvažnijih sustava IKT-a i značajnih rizika IKT-a za sustave i usluge IKT-a pokazala je ograničenu izloženost riziku IKT-a (npr. najviše dvije od ukupno pet unaprijed određenih kategorija rizika IKT-a).	• Politika i strategija institucije u pogledu rizika IKT-a razmjerne su njezinoj općoj strategiji i sklonosti preuzimanju rizika. • Organizacijski je okvir za rizik IKT-a robustan i u njemu postoje jasna zaduženja i jasna podjela zadataka između nositelja rizika, s jedne strane, te upravljačkih i kontrolnih funkcija, s druge strane. • Sustavi za mjerenje i praćenje rizika IKT-a te za izvješćivanje o njemu su primjereni. • Okvir kontrole za rizik IKT-a je stabilan.
3	Postoji umjeren rizik značajnog bonitetnog učinka na instituciju uzimajući u obzir razinu inherentnog rizika te upravljanje i kontrole.	• Izvori informacija koje treba razmotriti sukladno stavku 37. pokazali su znakove moguće znatne izloženosti riziku IKT-a. • Priroda profila rizičnosti institucije povezanog s IKT-om u kombinaciji s provjerom najvažnijih sustava IKT-a i značajnih rizika IKT-a za sustave i usluge IKT-a pokazala je povišenu izloženost riziku IKT-a (npr. tri ili više od ukupno pet unaprijed određenih kategorija rizika IKT-a).	
4	Postoji visok rizik značajnog bonitetnog učinka na instituciju uzimajući u obzir razinu inherentnog rizika te upravljanje i kontrole.	• Izvori informacija koje treba razmotriti sukladno stavku 37. pokazali su više znakova znatne izloženosti riziku IKT-a. • Priroda profila rizičnosti institucije povezanog s IKT-om u kombinaciji s provjerom najvažnijih sustava IKT-a i značajnih rizika IKT-a za sustave i usluge IKT-a pokazala je visoku izloženost riziku IKT-a (npr. četiri ili pet od ukupno pet unaprijed određenih kategorija rizika IKT-a).	

Prilog – Klasifikacija rizika IKT-a

Pet kategorija rizika IKT-a uz nepotpun popis rizika IKT- s mogućim teškim posljedicama i/ili operativnim, reputacijskim ili financijskim učinkom

Kategorije rizika IKT-a	Rizici IKT-a (nepotpun popis[10])	Opis rizika	Primjeri
Rizici povezani s kontinuitetom i dostupnošću IKT-a	Neprimjereno upravljanje kapacitetima	Nedostatak resursa (npr. sklopovske opreme, programske podrške, osoblja, pružatelja usluga) mogao bi prouzročiti nemogućnost prilagodbe opsega usluga radi zadovoljavanja poslovnih potreba, prekide sustava, pad kvalitete usluga i/ili operativne pogreške.	• Manjak kapaciteta mogao bi utjecati na brzinu prijenosa i dostupnost mreže (interneta) za usluge poput internetskog bankarstva. • Nedostatak osoblja (internog ili trećih strana) mogao bi prouzročiti prekide rada sustava i/ili operativne pogreške.
	Kvarovi sustava IKT-a	Gubitak dostupnosti zbog kvarova sklopovske opreme	• Kvarovi/pogreške u pohrani (tvrdi diskovi), poslužiteljima ili drugoj opremi IKT-a prouzročeni npr. nedovoljnim održavanjem
		Gubitak dostupnosti zbog kvarova i pogrešaka programske podrške	• Beskonačna petlja u programu aplikacije sprečava izvršenje transakcije. • Prekidi zbog uporabe zastarjelih sustava i rješenja IKT-a koji više ne zadovoljavaju trenutačne zahtjeve u pogledu dostupnosti i otpornosti i/ili koje dobavljači više ne podržavaju.
	Neprimjeren kontinuitet IKT-a i planiranje oporavka od katastrofa	Kvar planiranih rješenja IKT-a za dostupnost i/ili kontinuitet i/ili oporavak od katastrofa (npr. rezervni podatkovni centar) pri njihovoj aktivaciji u slučaju incidenta	• Konfiguracijske razlike između primarnog i sekundarnog podatkovnog centra mogu onemogućiti rezervnom podatkovnom centru pružanje planiranog kontinuiteta usluga.
	Kibernetički napadi koji remete i ruše sustave	Napadi raznih svrha (npr. aktivizam, ucjenjivanje) koji izazivaju preopterećenje sustava i mreže i tako sprečavaju legitimne korisnike da pristupe svojim internetskim računalnim uslugama	• Distribuirani napadi uskraćivanjem usluga provode se posredstvom velikog broja računalnih sustava na internetu koje kontrolira haker i koji šalju internetskim (npr. bankovnim) uslugama velike

[10] Rizici IKT-a navedeni su u kategoriji rizika na koju najviše utječu, no mogli bi utjecati i na druge kategorije rizika.

Kategorije rizika IKT-a	Rizici IKT-a (nepotpun popis[10])	Opis rizika	Primjeri
			količine naizgled legitimnih zahtjeva za uslugama.
Sigurnosni rizici IKT-a	Kibernetički napadi i drugi vanjski napadi temeljeni na IKT-u	Napadi koji se izvršavaju s interneta ili s vanjskih mreža radi različitih svrha (npr. prijevare, špijunaža, aktivizam/sabotaža, kibernetički terorizam) s pomoću raznih postupaka (npr. socijalni inženjering, pokušaji neovlaštenog upadanja iskorištavanjem ranjivosti, uporaba zlonamjernih programa), a čiji je rezultat preuzimanje kontrole nad internim sustavima IKT-a	Razne vrste napada: • napredne ustrajne prijetnje (APT) radi preuzimanja kontrole nad internim sustavima ili radi krađe podataka (npr. podatci povezani s krađom identiteta, podatci o kreditnim karticama); • zlonamjerni programi (npr. *ransomware*) koji kriptiraju podatke s ciljem ucjene; • zaraza internih sustava IKT-a trojanskim konjem radi potajnog provođenja zlonamjernih radnji; • iskorištavanje ranjivosti sustava IKT-a i/ili (web) aplikacija (npr. umetanje SQL koda) radi pristupanja internim sustavima IKT-a.
		Prijevarne platne transakcije koje izvršavaju hakeri kršenjem ili zaobilaženjem sigurnosnih mehanizama platnih usluga i usluga internetskog bankarstva i/ili napadanjem ili iskorištavanjem sigurnosnih ranjivosti u internom platnom sustavu institucije	• Napadi na usluge internetskog bankarstva ili platne usluge radi izvršavanja neovlaštenih transakcija • Stvaranje i slanje prijevarnih platnih transakcija iz internog platnog sustava institucije (npr. prijevarne SWIFT poruke)
		Prijevarne transakcije vrijednosnim papirima koje izvršavaju hakeri kršenjem ili zaobilaženjem sigurnosnih mehanizama usluga internetskog bankarstva koje omogućuju i pristup klijentovim računima vrijednosnih papira	• Napadi *pump and dump*, pri kojima napadači stječu pristup računima vrijednosnih papira klijenata u internetskom bankarstvu i provode prijevarne kupovne ili prodajne naloge kako bi utjecali na tržišnu cijenu i/ili ostvarili dobit na temelju prethodno utvrđenih pozicija vrijednosnih papira
		Napadi na komunikacijske veze i razgovore svih vrsta ili na sustave IKT-a radi prikupljanja informacija i/ili izvršavanja prijevara	• Presretanje nezaštićenih prijenosa autentifikacijskih podataka koji su u obliku nekriptiranog teksta
	Neprimjerena interna sigurnost IKT-a	Stjecanje neovlaštenog pristupa ključnim sustavima IKT-a unutar institucije radi raznih svrha (npr. prijevare, izvršavanje i prikrivanje nedopuštenih aktivnosti trgovanja, krađa podataka, aktivizam/sabotaža) na	• Instaliranje programa/uređaja za bilježenje pritisaka na tipke (engl. *key logger*) za krađu korisničkih imena i zaporki radi stjecanja neovlaštenog pristupa povjerljivim podatcima i/ili izvršavanja prijevara

Kategorije rizika IKT-a	Rizici IKT-a (nepotpun popis[10])	Opis rizika	Primjeri
		razne načine (npr. zlouporaba i/ili povećanje ovlasti, krađa identiteta, socijalni inženjering, iskorištavanje ranjivosti u sustavima IKT, uporaba zlonamjernih programa)	• Probijanje/pogađanje slabih zaporki radi stjecanja nezakonitih ili povećanih pristupnih prava • Administrator sustava upotrebljava operativne sustave ili alate baza podataka (za izravne izmjene baza podataka) kako bi počinio prijevare.
		Neovlašteno manipuliranje IKT-om zbog neprimjerenih postupaka i praksi upravljanja pristupom IKT-u	• Neprovođenje deaktivacije i brisanja nepotrebnih računa, npr. računa zaposlenika koji su promijenili radna mjesta ili otišli iz institucije, uključujući goste ili dobavljače kojima pristup više nije potreban, što može omogućiti neovlašten pristup sustavima IKT-a • Odobravanje prekomjernih pristupnih prava i ovlasti, kojima se omogućuje neovlašten pristup i/ili prikrivanje nedopuštenih aktivnosti
		Sigurnosne prijetnje zbog nedostatka sigurnosne osviještenosti, pri čemu zaposlenici ne razumiju ili zanemaruju sigurnosne politike i postupke IKT-a ili ih se ne pridržavaju	• Zaposlenici koji su prijevarom navedeni da pomognu u izvršavanju napada (tj. socijalni inženjering) • Loše prakse povezane s korisničkim podatcima: dijeljenje zaporki, uporaba zaporki koje je lako pogoditi, uporaba jedne zaporke za mnoštvo različitih svrha itd. • Pohranjivanje nekriptiranih povjerljivih podataka na prijenosnim računalima i prenosivim rješenjima za pohranu podataka (npr. ključevi na USB uređaju) koji se mogu izgubiti ili ukrasti
		Neovlaštena pohrana ili prijenos povjerljivih podataka izvan institucije	• Osobe koje kradu ili namjerno odaju ili krijumčare povjerljive podatke neovlaštenim osobama ili javnosti
	Neprimjerena fizička sigurnost IKT-a	Zlouporaba ili krađa imovine IKT-a fizičkim pristupom čime je izazvana šteta, gubitak imovine ili podataka ili su omogućene druge prijetnje	• Fizičke provale u zgrade/urede i/ili podatkovne centre radi krađe opreme IKT-a (npr. računala, prijenosna računala, rješenja za pohranu) i/ili radi umnožavanja podataka fizičkim pristupom IKT-u

Kategorije rizika IKT-a	Rizici IKT-a (nepotpun popis[10])	Opis rizika	Primjeri
		Namjerno ili slučajno oštećenje fizičke imovine IKT-a prouzročeno terorizmom, nezgodama ili nehotičnim/pogrešnim postupcima zaposlenika institucije i/ili trećih strana (dobavljači, osoblje za održavanje/popravke)	• Fizički terorizam (tj. teroristička bombe) ili sabotaža na sustavima IKT-a • Uništenje podatkovnog centra prouzročeno požarom, curenjem vode ili drugim čimbenicima
		Nedovoljna fizička zaštita od prirodnih nepogoda, uslijed koje prirodne nepogode djelomično ili potpuno uništavaju sustave / podatkovne centre IKT-a	• Potresi, ekstremna vrućina, olujni vjetar, snažne snježne mećave, poplave, požari, udari groma
Rizici promjena IKT-a	Neprimjerene kontrole nad promjenama sustava IKT-a i razvojem IKT-a	Incidenti prouzročeni neotkrivenim pogreškama ili ranjivostima izazvanima promjenama (npr. nepredviđeni učinci promjena ili promjena kojima se loše upravlja zbog nedostatka testiranja ili loših praksi upravljanja promjenama) npr. programa, sustava IKT-a i podataka	• Puštanje u produkciju nedovoljno testiranih programskih ili konfiguracijskih promjena s neočekivanim nepovoljnim učincima na podatke (npr. oštećenje, brisanje) i/ili rad sustava IKT-a (npr. kvar ili degradacija performansi) • Nekontrolirane promjene sustava ili podataka IKT-a u produkcijsko okruženje. • Puštanje u produkciju nedovoljno sigurnih sustava IKT-a i internetskih aplikacija, čime se hakerima daje mogućnost napada na pružene internetske usluge i/ili provale u interne sustave IKT-a • Nekontrolirane promjene izvornog koda interno razvijenih programa • Nedovoljno testiranje zbog nedostatka primjerenog testnog okruženja
	Neprimjerena arhitektura IKT-a	Loše upravljanje arhitekturom IKT-a pri dizajniranju, uspostavljanju i održavanju sustava IKT-a (npr. programska podrška, sklopovska oprema, podatci) s vremenom može dovesti do pojave složenih, teških i rigidnih sustava IKT-a s visokim troškovima održavanja, koji više nisu dovoljno usklađeni s poslovnim potrebama i koji ne ispunjavaju stvarne zahtjeve za upravljanje rizikom.	• Neprimjereno upravljanje promjenama sustava IKT-a, programske podrške ili podataka tijekom duljeg razdoblja dovodi do pojave sustava i arhitektura IKT-a koji su složeni, heterogeni i teški za upravljanje, što izaziva mnoge nepovoljne učinke na poslovanje i upravljanje rizicima (npr. nedostatak fleksibilnosti i agilnosti, kvarovi i incidenti u pogledu IKT-a, visoki operativni troškovi, oslabljena

Kategorije rizika IKT-a	Rizici IKT-a (nepotpun popis[10])	Opis rizika	Primjeri
			sigurnost i otpornost IKT-a, smanjenje kvalitete podataka i mogućnosti izvješćivanja) • Prekomjerna prilagodba i proširenje komercijalnih programskih paketa s pomoću interno razvijenih programa uzrokuje nemogućnost puštanja budućih izdanja/verzija i nadogradnji komercijalnih programa te izlažu riziku da ih dobavljači više neće podržavati
	Neprimjereno upravljanje životnim ciklusom i zakrpama	Neodržavanje primjerene evidencije sve imovine IKT-a temeljem koje bi se podržale, odnosno vodile dobre prakse upravljanja životnim ciklusom i zakrpama; to dovodi do nedovoljno zakrpanih (i stoga ranjivijih) i zastarjelih sustava IKT-a koji možda neće moći podržavati poslovne potrebe i potrebe upravljanja rizikom.	• Nezakrpani i zastarjeli sustavi IKT-a koji mogu prouzročiti nepovoljne poslovne učinke i učinke u pogledu upravljanja rizicima (npr. nedostatak fleksibilnosti i agilnosti, prekidi IKT-a, oslabljena sigurnost i otpornost IKT-a)
Rizici IKT-a povezani s integritetom podataka	Disfunkcionalna obrada podataka IKT-a i postupanje s njima	Zbog pogrešaka ili kvarova povezanih sa sustavom, komunikacijom ili aplikacijama, te zbog pogrešnog izdvajanja, prijenosa i punjenja podataka (ETL), podatci bi se mogli oštetiti ili izgubiti.	• Pogreška u informatičkom sustavu pri skupnoj (noćnoj) obradi, što uzrokuje pogrešna salda na bankovnim računima klijenata • Pogrešno izvršeni upiti • Gubitak podataka zbog pogreške u replikaciji podataka (izradi pričuvnih kopija)
	Loše osmišljene validacijske kontrole podataka u sustavima IKT-a	Pogreške povezane s nedostatkom ili neučinkovitošću automatiziranog unosa podataka i kontrola prihvata (npr. za korištene podatke trećih strana), prijenosa podataka, kontrola obrade i izlaznih kontrola u sustavima IKT-a (npr. kontrole valjanosti ulaznih podataka, usklađenja podataka)	• Nedovoljno ili nepravilno formatiranje/validacija ulaznih podataka u aplikacijama i/ili korisničkim sučeljima • Nedostatak kontrola usklađivanja podataka za izlazne podatke • Nedostatak kontrola prilikom provođenje izdvajanja podataka (npr. u upitima bazi podataka), što dovodi do pogrešnih podataka • Uporaba neispravnih vanjskih podataka
	Loše kontrolirane izmjene podataka	Pogreške u podatcima nastale zbog nedostatka kontrole točnosti i opravdanosti manipulacija	• Razvojni programeri ili administratori baza podataka koji izravno pristupaju podatcima u

Kategorije rizika IKT-a	Rizici IKT-a (nepotpun popis[10])	Opis rizika	Primjeri
	u produkcijskim sustavima IKT-a	podatcima koje se provode u produkciji sustava IKT-a	produkcijskim sustavima IKT-a i mijenjaju ih bez kontrole, npr. u slučaju pojave incidenta u sustavu IKT-a
	Arhitektura podataka, tijek podataka, modeli podataka ili rječnici podataka koji su loše osmišljeni i/ili kojima se loše upravlja	Arhitekture podataka, modeli podataka, tijek podataka ili rječnici podataka kojima se loše upravlja mogu prouzročiti više verzija istih podataka u sustavima IKT-a, koje više nisu konzistentne zbog različito primijenjenih modela podataka ili definicija podataka i/ili zbog razlika u temeljnom postupku stvaranja i izmjene podataka.	• Postojanje različitih baza podataka o klijentima za zasebne proizvode ili poslovne jedinice s različitim definicijama i poljima za unos podataka, što na razini cijele financijske institucije ili grupe uzrokuje neusklađene podatke o klijentima koje je teško usporediti i integrirati
Rizici povezani s eksternalizacijom IKT-a	Neprimjerena otpornost usluga trećih strana ili nekog drugog subjekta grupe	Nedostupnost ključnih eksternaliziranih aktivnosti IKT-a, telekomunikacijskih i komunalnih usluga. Gubitak ili oštećenje kritičnih/osjetljivih podataka povjerenih pružatelju usluga	• Nedostupnost temeljnih usluga zbog kvarova u (eksternaliziranim) sustavima ili aplikacijama IKT-a dobavljača • Prekidi telekomunikacijskih veza • Prekidi napajanja električnom energijom
	Neprimjereno upravljanje eksternalizacijom	Znatan pad kvalitete ili obustava pružanja usluga zbog neodgovarajuće pripremljenosti ili neodgovarajućih postupaka kontrole pružatelja eksternaliziranih usluga. Neučinkovito upravljanje eksternalizacijom moglo bi prouzročiti manjak odgovarajućih vještina i sposobnosti potrebnih za potpuno utvrđivanje, procjenu, smanjenje i praćenje rizika IKT-a te bi moglo ograničiti operativne mogućnosti institucije.	• Loši postupci za rješavanje incidenata, ugovorni kontrolni mehanizmi i jamstva definirana ugovorom o pružanju usluga kojima se povećava ovisnost o trećim stranama i dobavljačima u pogledu ključnih osoba • Neprimjerene kontrole upravljanja promjenama povezane s okruženjem IKT-a pružatelja usluga mogu prouzročiti znatan pad kvalitete ili obustavu pružanja usluga.
	Neprimjerena sigurnost trećih strana ili nekog drugog subjekta grupe	Hakiranje sustava IKT-a pružatelja usluga, tj. treće strane, s izravnim učinkom na eksternalizirane usluge ili kritične/povjerljive podatke pohranjene kod pružatelja usluga, Zaposlenici pružatelja usluga koji stječu neovlašten	• Kriminalci ili teroristi koji hakiraju sustave pružatelja usluga radi ulaska u sustave IKT-a institucije ili radi pristupa kritičnim ili osjetljivim podatcima pohranjenima kod pružatelja usluga odnosno radi uništavanja tih podataka

Kategorije rizika IKT-a	Rizici IKT-a (nepotpun popis[10])	Opis rizika	Primjeri
		pristup kritičnim/osjetljivim podatcima pohranjenima kod pružatelja usluga	• Zlonamjerne osobe na strani pružatelja usluga koje žele ukrasti i prodati osjetljive podatke