EBA/GL/2017/05

11/09/2017

Smernice

Smernice o oceni tveganja, povezanega z IKT, v skladu s procesom nadzorniškega pregledovanja in vrednotenja (SREP)

1. Obveznosti glede skladnosti in poročanja

Vloga teh smernic

1. Dokument vsebuje smernice, izdane v skladu s členom 16 Uredbe (EU) št. 1093/2010[1]. V skladu s členom 16(3) Uredbe (EU) št. 1093/2010 si morajo pristojni organi in finančne institucije na vsak način prizadevati za upoštevanje smernic.

2. V smernicah je predstavljeno stališče organa EBA o ustreznih nadzorniških praksah v Evropskem sistemu finančnega nadzora in o tem, kako bi bilo treba zakonodajo Unije uporabljati na določenem področju. Pristojni organi iz člena 4(2) Uredbe (EU) št. 1093/2010, za katere smernice veljajo, bi jih morali upoštevali tako, da jih ustrezno vključijo v svoje prakse (npr. s spremembo svojega pravnega okvira ali nadzorniških postopkov), tudi če so smernice namenjene predvsem institucijam.

Dolžnost poročanja

3. Pristojni organi morajo v skladu s členom 16(3) Uredbe (EU) št. 1093/2010 do 13.11.2017 organ EBA uradno obvestiti, ali ravnajo oziroma ali nameravajo ravnati v skladu s temi smernicami, ali pa mu sporočiti razloge za njihovo neupoštevanje. Če pristojni organi do tega roka ne bodo poslali uradnega obvestila, bo organ EBA štel, da jih ne upoštevajo. Uradna obvestila je treba poslati na obrazcu, ki je na voljo na spletni strani organa EBA, na elektronski naslov compliance@eba.europa.eu z navedbo sklica „EBA/GL/2017/05“. Predložiti jih morajo osebe, ki so pooblaščene za poročanje o skladnosti v imenu svojih pristojnih organov. Organu EBA je treba sporočiti tudi vsako spremembo stanja glede upoštevanja smernic.

4. Uradna obvestila bodo v skladu s členom 16(3) objavljena na spletni strani organa EBA.

[1] Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12).

2. Vsebina, področje uporabe in opredelitve pojmov

Predmet urejanja in področje uporabe

5. Cilj teh smernic, ki so bile pripravljene v skladu s členom 107(3) Direktive 2013/36/EU[2], je zagotoviti konvergenco nadzornih praks pri oceni tveganja, povezanega z informacijskimi in komunikacijskimi tehnologijami (IKT), v skladu s procesom nadzorniškega pregledovanja in vrednotenja (SREP) iz člena 97 Direktive 2013/36/EU, ki je dodatno opredeljen v Smernicah organa EBA o skupnih postopkih in metodologijah za proces nadzorniškega pregledovanja in ovrednotenja (SREP)[3]. Te smernice zlasti določajo merila za ocenjevanje, ki bi jih morali pristojni organi uporabljati pri nadzornih ocenah upravljanja institucij in njihovih strategij IKT ter nadzornih ocen izpostavljenosti institucij tveganju, povezanemu z IKT, ter njihovih kontrol IKT. Te smernice so sestavni del Smernic organa EBA o SREP.

6. Pristojni organi te smernice uporabljajo v skladu z ravnjo uporabe SREP, določeno v Smernicah organa EBA o SREP, ter v skladu z modelom minimalnega posredovanja in zahtev glede sorazmernosti, ki so prav tako določeni v njih.

Naslovniki

7. Te smernice so namenjene pristojnim organom, kot so opredeljeni v členu 4(2)(i) Uredbe (EU) št. 1093/2010.

Opredelitve

8. Če ni določeno drugače, imajo pojmi v teh smernicah enak pomen kot pojmi, uporabljeni in opredeljeni v Direktivi 2013/36/EU in Uredbi (EU) št. 575/2013, opredelitve iz Smernic organa EBA o SREP pa imajo enak pomen tudi v teh smernicah. Poleg tega se v teh smernicah uporabljajo naslednje opredelitve:

[2] Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (1) - UL L 176, 27. 6. 2013.

[3] EBA/GL/2014/13

Sistemi IKT	IKT, vključene v mehanizem ali povezovalno omrežje, ki podpirajo delovanje institucije.
Storitve IKT	Storitve, ki jih sistemi IKT nudijo enemu ali več notranjim ali zunanjim uporabnikom. Primeri vključujejo storitve vnosa podatkov, hrambe podatkov, obdelovanja podatkov in poročanja, pa tudi podporne storitve za spremljanje, poslovanje in odločanje.
Tveganje glede razpoložljivosti in neprekinjenega delovanja IKT	Tveganje škodljivega učinka na delovanje in razpoložljivost sistemov in podatkov IKT, vključno z nezmožnostjo pravočasne obnovitve storitev institucije, ki nastane zaradi okvare delov strojne ali programske opreme IKT, slabosti v upravljanju sistema IKT ali drugega dogodka, kot je dodatno razloženo v Prilogi.
Tveganje glede varnosti IKT	Tveganje nepooblaščenega dostopa do sistemov in podatkov IKT iz institucije ali zunaj nje (npr. kibernetski napadi), kot je dodatno razloženo v Prilogi.
Tveganje glede sprememb IKT	Tveganje, ki izhaja iz nezmožnosti institucije, da bi pravočasno in nadzorovano obvladala spremembe sistema IKT, zlasti v primeru obsežnih in zapletenih programov sprememb, kot je dodatno razloženo v Prilogi.
Tveganje glede celovitosti podatkov IKT	Tveganje, da so podatki, ki so shranjeni ali obdelani v sistemih IKT, nepopolni, netočni ali nedosledni v različnih sistemih IKT, na primer kot posledica šibkih ali neobstoječih kontrol IKT v različnih fazah življenjskega cikla podatkov IKT (tj. načrtovanje podatkovne strukture, gradnja podatkovnega modela in/ali podatkovnih slovarjev, preverjanje vnosa podatkov ter nadzorovanje izvlečkov, prenosov in obdelave podatkov, vključno s prikazanimi izhodnimi podatki), kar bi oslabilo zmožnost institucije, da pravilno in pravočasno opravlja storitve ter zagotavlja informacije o upravljanju (tveganja) in finančne informacije, kot je dodatno razloženo v Prilogi.
Tveganje glede zunanjega izvajanja IKT	Tveganje, da ima najem tretje osebe ali drugega subjekta v skupini (oddajanje v zunanje izvajanje subjektu znotraj skupine) za zagotavljanje sistemov IKT ali z njimi povezanih storitev škodljiv učinek na uspešnost institucije in njeno upravljanje tveganja, kot je dodatno razloženo v Prilogi.

3. Izvajanje

Datum začetka uporabe

9. Te smernice se začnejo uporabljati 1. januarja 2018.

4. Zahteve za oceno tveganja, povezanega z IKT

Naslov 1 – Splošne določbe

10. Pristojni organi bi morali oceno tveganja, povezanega z IKT, ter ureditve upravljanja in strategije IKT opraviti v okviru procesa SREP v skladu z modelom minimalnega posredovanja in zahtevami glede sorazmernosti, ki so določeni v naslovu 2 Smernic organa EBA o SREP. To zlasti pomeni, da:

    a. bi bila pogostost ocen tveganja, povezanega z IKT, odvisna od modela minimalnega posredovanja na podlagi kategorije po SREP, ki bi ji bila institucija dodeljena, in njenega načrta nadzorniških pregledov in

    b. bi morale biti globina, podrobnost in intenzivnost ocene tveganja, povezanega z IKT, sorazmerne z velikostjo, strukturo in operativnim okoljem institucije, pa tudi naravo, obsegom in zapletenostjo njenih dejavnosti.

11. Načelo sorazmernosti se v teh smernicah uporablja za obseg, pogostost in intenzivnost nadzorniškega posredovanja in dialoga z institucijami ter nadzorniško pričakovanje glede standardov, ki bi jih morala institucija dosegati.

12. Pristojni organi se lahko opirajo na delo in upoštevajo delo, ki ga je institucija ali pristojni organ že opravil v okviru ocen drugih tveganj ali elementov SREP, da dobijo posodobitev ocene. Pri pripravi ocen, določenih v teh smernicah, bi morali pristojni organi posebej izbrati najprimernejši pristop za nadzorno oceno ter metodologijo, ki je najustreznejša in sorazmerna za institucijo, poleg tega pa bi morali uporabiti obstoječo in razpoložljivo dokumentacijo (npr. ustrezna poročila in druge dokumente, srečanja z odgovornimi za upravljanje (tveganja), ugotovitve inšpekcijskih pregledov na kraju samem), ki bi vplivala na njihovo oceno.

13. Pristojni organi bi morali ugotovitve svojih ocen meril, določenih v teh smernicah, povzeti in jih uporabiti za sklepanje o oceni elementov SREP, kot je določeno v Smernicah organa EBA o SREP.

14. Zlasti ocena upravljanja in strategije IKT, opravljena v skladu z naslovom 2 teh smernic, bi morala prinesti ugotovitve, ki bi vplivale na povzetek ugotovitev ocene elementa SREP, ki obsega notranje upravljanje in kontrolo na ravni celotne institucije, kot je določeno v naslovu 5 Smernic organa EBA o SREP, to oceno upravljanja in strategije IKT pa bi moral izražati tudi rezultat tega elementa SREP. Poleg tega bi morali pristojni organi upoštevati, da morebiten bistven škodljiv učinek ocene strategije IKT na poslovno strategijo institucije ali morebitni pomisleki, da institucija morda nima dovolj virov IKT in zmogljivosti IKT za izvedbo in podpiranje pomembnih načrtovanih strateških sprememb, vplivajo na analizo poslovnega modela, opravljeno v skladu z naslovom 4 Smernic organa EBA o SREP.

15. Rezultat ocene tveganja, povezanega z IKT, kot je določeno v naslovu 3 teh smernic, bi moral vplivati na ugotovitve ocene operativnega tveganja, šteti pa bi se moralo tudi, da vpliva na izračun ustreznega rezultata, kot je določeno v naslovu 6.4 Smernic organa EBA o SREP.

16. Opozarja se, da pristojni organi podkategorije tveganj na splošno sicer ocenjujejo kot del glavnih kategorij (npr. tveganje, povezano z IKT, bo ocenjeno kot del operativnega tveganja), če menijo, da so nekatere podkategorije pomembne, pa jih lahko ocenijo posebej. Če pristojni organ tveganje, povezano z IKT, opredeli kot pomembno, je v te smernice v ta namen vključena tabela za izračun rezultata (tabela 1), ki se uporabi za samostojen rezultat za podkategorijo tveganja, povezanega z IKT, pridobljen v skladu s splošnim pristopom k izračunu rezultatov za tveganja za kapital iz Smernic organa EBA za SREP.

17. Da bi pristojni organi ugotovili, ali bi bilo treba tveganje, povezano z IKT, obravnavati kot pomembno in ga torej oceniti posebej kot podkategorijo operativnega tveganja, lahko uporabijo merila, določena v oddelku 6.1 Smernic organa EBA o SREP.

18. Pri uporabi teh smernic bi morali pristojni organi, če je to ustrezno, proučiti neizčrpen seznam podkategorij tveganja, povezanega z IKT, in scenarijev tveganja, ki so navedeni v Prilogi, pri tem pa upoštevati, da se Priloga osredotoča na tveganja, povezana z IKT, ki lahko povzročijo zelo velike izgube. Nekatera tveganja, povezana z IKT, ki so vključena v taksonomijo, lahko pristojni organi izpustijo, če niso pomembna za njihovo oceno. Od institucij se pričakuje, da vodijo svojo taksonomijo tveganj, namesto da uporabljajo taksonomijo tveganja, povezanega z IKT, ki je navedena v Prilogi.

19. Če se te smernice uporabljajo za čezmejne bančne skupine in njihove subjekte ter je bil vzpostavljen kolegij nadzornikov, pristojni organi v okviru svojega sodelovanja za oceno SREP v skladu z oddelkom 11.1 Smernic organa EBA o SREP čim bolj uskladijo natančno in podrobno področje uporabe vsake informacijske postavke za vse subjekte skupine.

Naslov 2 – Ocena upravljanja institucij in njihove strategije IKT

2.1 Splošna načela

20. Pristojni organi bi morali oceniti, ali splošno upravljanje in okvir notranjih kontrol institucije ustrezno zajemata sisteme IKT in z njimi povezana tveganja ter ali upravljalni organ te vidike primerno obravnava in upravlja, saj so IKT bistvene za pravilno delovanje institucije.

21. Pri pripravi ocene bi morali pristojni organi upoštevati zahteve in standarde dobrega notranjega upravljanja in ureditve nadzora tveganj, kot je določeno v Smernicah organa EBA o notranjem upravljanju (GL 44)[4], ter mednarodne smernice na tem področju, če so te ustrezne glede na posebnost sistemov IKT in tveganj, povezanih z IKT.

22. Ocena v tem naslovu ne zajema posebnih elementov upravljanja sistemov IKT, upravljanja tveganja in kontrol, ki so osredotočene na upravljanje posebnih tveganj, povezanih z IKT in obravnavanih v naslovu 3 teh smernic, ampak je osredotočena na naslednja področja:

    a. strategijo IKT – ali ima institucija strategijo IKT, ki jo ustrezno upravlja in je v skladu z njeno poslovno strategijo;

    b. splošno notranje upravljanje – ali so ureditve splošnega notranjega upravljanja institucije ustrezne glede na njene sisteme IKT; in

    c. tveganje, povezano z IKT, v okviru institucije za upravljanje tveganja – ali so z upravljanjem tveganja in okvirom notranjih kontrol sistemi IKT ustrezno zaščiteni.

23. Točka a) odstavka 22 zagotavlja informacije o elementih upravljanja institucije, vplivati pa bi morala predvsem na oceno poslovnega modela iz naslova 4 Smernic organa EBA o SREP. Točki b) in c) dodatno dopolnjujeta ocene tem iz naslova 5 Smernic organa EBA o SREP, oceno, ki je opisana v teh smernicah, pa bi bilo treba uporabiti pri pripravi ustrezne ocene iz naslova 5 Smernic organa EBA o SREP.

24. Če je to ustrezno, rezultat te ocene vpliva na oceno upravljanja tveganja in kontrol iz naslova 3 teh smernic.

2.2 Strategija IKT

25. V tem oddelku pristojni organi ocenijo, ali ima institucija strategijo IKT, ali to strategijo ustrezno nadzoruje upravljalni organ institucije, ali je skladna s poslovno strategijo, zlasti kar zadeva posodabljanje IKT ter načrtovanje ali uvedbo pomembnih in zapletenih sprememb IKT, in ali podpira poslovni model institucije.

[4] Smernice organa EBA o notranjem upravljanju, GL 44, 27. september 2011.

2.2.1 Razvoj in ustreznost strategije IKT

26. Pristojni organi bi morali oceniti, ali je institucija sprejela okvir, sorazmeren z naravo, obsegom in zapletenostjo njenih dejavnosti IKT, za pripravo in razvoj strategije IKT. Pri pripravi ocene bi morali pristojni organi upoštevati, ali:

    a. je višje vodstvo [5] poslovnega področja (ali poslovnih področij) ustrezno vključeno v opredelitev strateških prednostnih nalog institucije v zvezi z IKT ter se tudi višje vodstvo funkcije IKT zaveda razvoja, oblikovanja in uvedbe večjih poslovnih strategij in pobud za zagotavljanje nadaljnje usklajenosti sistemov IKT, storitev IKT in funkcije IKT (tj. tistih, ki so odgovorni za upravljanje in razporejanje teh sistemov in storitev) ter poslovne strategije institucije in ali se IKT učinkovito posodabljajo;

    b. je strategija IKT dokumentirana in jo podpirajo konkretni načrti za izvedbo, zlasti kar zadeva pomembne mejnike in načrtovanje virov (vključno s finančnimi in človeškimi viri), za zagotovitev, da so ti realistični in omogočajo uresničitev strategije IKT;

    c. institucija strategijo IKT občasno posodablja, zlasti ko spremeni poslovno strategijo, da bi zagotovila nadaljnjo usklajenost IKT ter srednje- do dolgoročnih poslovnih ciljev, načrtov in dejavnosti; in

    d. je upravljalni organ institucije odobril strategijo IKT in načrte za izvedbo ter spremlja izvedbo strategije.

2.2.2 Izvedba strategije IKT

27. Če so za izvedbo strategije IKT, ki jo je sprejela institucija, potrebne pomembne in zapletene spremembe IKT ali spremembe, ki bodo pomembno vplivale na poslovni model institucije, bi morali pristojni organi oceniti, ali ima institucija okvir kontrol, ki ustreza njeni velikosti, njenim dejavnostim IKT in ravni dejavnosti za spremembe, da bo z njim podprla učinkovito izvedbo strategije IKT. Pri pripravi ocene bi morali pristojni organi upoštevati, ali okvir kontrol:

    a. vključuje procese upravljanja (npr. spremljanje napredka in proračuna ter poročanje o njima) in ustrezne organe (npr. projektno pisarno, usmerjevalno skupino za IKT ali enakovreden organ), ki bodo učinkovito podpirali izvedbo strateških programov IKT;

    b. opredeljuje in dodeljuje vloge in odgovornosti za izvedbo strateških programov IKT s posebnim poudarkom na izkušnji ključnih deležnikov pri organiziranju, usmerjanju in spremljanju pomembnih in zapletenih sprememb IKT ter obvladovanju širših vplivov na organizacijo in ljudi (npr. obvladovanje odpora proti spremembam, usposabljanje in komuniciranje);

    c. sodeluje z neodvisno kontrolno funkcijo in funkcijo notranje revizije, da bi zagotovil, da so bila tveganja, povezana z izvedbo strategije IKT, opredeljena, ocenjena in učinkovito zmanjšana ter da je okvir upravljanja, sprejet za potrebe izvajanja strategije IKT, učinkovit; in

[5] Višje vodstvo in upravljalni organ, kot sta opredeljena v Direktivi 2013/36/EU z dne 26. junija 2013 v členu 3(7), „upravljalni organ“, in v členu 3(9), „višje vodstvo“.

d. vsebuje postopek načrtovanja in pregleda načrtovanja, ki zagotavlja prožnost za odzivanje na pomembne ugotovljene težave (npr. težave ali zamude pri izvedbi) ali zunanje spremembe (npr. pomembne spremembe v poslovnem okolju, tehnološke težave ali inovacije), da bi zagotovil pravočasno prilagoditev načrta za strateško izvedbo.

2.3 Splošno notranje upravljanje

28. V skladu z naslovom 5 Smernic organa EBA o SREP bi morali pristojni organi oceniti, ali ima institucija primerno in pregledno korporativno strukturo, ki ustreza svojemu namenu in je uvedla primerne ureditve upravljanja. Zlasti v zvezi s sistemi IKT in v skladu s Smernicami organa EBA o notranjem upravljanju bi morala ta ocena vključevati tudi oceno, ali institucija izkazuje:

    a. trdno in pregledno organizacijsko strukturo z jasnimi odgovornostmi glede IKT, vključno z upravljalnim organom in njegovimi odbori, ključne osebe, ki so odgovorne za IKT (npr. glavni informacijski direktor, glavni poslovodja ali oseba z enakovredno vlogo), pa imajo ustrezen neposreden ali posreden dostop do upravljalnega organa, s čimer je zagotovljeno, da se o pomembnih informacijah ali težavah z zvezi z IKT ustrezno poroča, razpravlja in odloča na ravni upravljalnega organa; in

    b. da se upravljalni organ zaveda tveganj, povezanih z IKT, in jih obravnava.

29. V skladu z oddelkom 5.2 Smernic organa EBA o SREP bi morali pristojni organi oceniti, ali je pri politiki in strategiji institucije glede zunanjega izvajanja IKT po potrebi upoštevan učinek zunanjega izvajanja IKT na poslovanje in poslovni model institucije.

2.4 Tveganje, povezano z IKT, v okviru institucije za upravljanje tveganja

30. Pri ocenjevanju upravljanja tveganja v vsej instituciji in notranjih kontrol, kot predvideva naslov 5 Smernic organa EBA o SREP, bi morali pristojni organi upoštevati, ali so z upravljanjem tveganja in okvirom notranjih kontrol sistemi IKT v instituciji ustrezno zaščiteni na način, ki je sorazmeren z velikostjo in dejavnostmi institucije ter njenim profilom tveganja, povezanega z IKT, kot je opredeljeno v naslovu 3. Pristojni organi bi morali predvsem ugotoviti, ali:

    a. nagnjenost k prevzemanju tveganja in ICAAP zajemata tveganja, povezana z IKT, kot del širše kategorije operativnega tveganja, in sicer za potrebe opredelitve strategije za celotno tveganje in določitve notranjega kapitala; in

    b. so tveganja, povezana z IKT, vključena v upravljanje tveganja v vsej instituciji in okvire notranjih kontrol.

31. Pristojni organi bi morali oceno pod točko (a) zgoraj opraviti ob upoštevanju tako pričakovanih kot tudi negativnih scenarijev, npr. scenarijev, ki so vključeni v stresni test za posamezno institucijo ali v nadzorniški stresni test.

32. Zlasti kar zadeva (b), bi morali pristojni organi oceniti, ali sta neodvisna kontrolna funkcija in funkcija notranje revizije, kot je navedeno v odstavkih 104(a), 104(d) in 105(c) Smernic organa EBA o SREP,

ustrezni za zagotavljanje zadostne ravni neodvisnosti med IKT ter funkcijama kontrole in revizije glede na velikost institucije in njen profil tveganja, povezanega z IKT.

2.5 Povzetek ugotovitev

33. Rezultati bi morali biti vključeni v povzetek ugotovitev v skladu z naslovom 5 Smernic organa EBA o SREP in v ustrezni izračun rezultata v skladu z merili, navedenimi v tabeli 3 Smernic organa EBA o SREP.

34. Pri oceni strategije IKT bi bilo treba pri dokončanju zgornje ocene upoštevati naslednje točke:

    a. Če pristojni organi sklenejo, da je okvir upravljanja institucije pomanjkljiv za razvoj in izvedbo njene strategije IKT v skladu z oddelkom 2.2, bi moralo to vplivati na oceno notranjega upravljanja institucije, kot je določeno v točki 87(a) naslova 5 Smernic organa EBA o SREP;

    b. če pristojni organi iz zgornjih ocen iz oddelka 2.2 sklenejo, da bi bili strategija IKT in poslovna strategija bistveno neusklajeni, kar bi lahko bistveno škodljivo vplivalo na dolgoročne poslovne in/ali finančne cilje institucije, njen trajnostni in/ali poslovni model ali njena poslovna področja, ki so bila v odstavku 62(a) Smernic organa EBA o SREP določena za najpomembnejša, bi moralo to vplivati na oceno poslovnega modela iz točk 70(b) in 70(c) naslova 4 Smernic organa EBA o SREP; in

    c. če pristojni organi iz zgornjih ocen iz oddelka 2.2 sklenejo, da institucija morda nima dovolj virov IKT in zmogljivosti za uporabo IKT, da bi izvajala in podpirala pomembne načrtovane strateške spremembe, bi moralo to vplivati na oceno poslovnega modela iz točke 70(b) naslova 4 Smernic organa EBA o SREP.

Naslov 3 – Ocena izpostavljenosti institucij tveganju, povezanemu z IKT, ter njihovih kontrol IKT

3.1 Splošni premisleki

35. Pristojni organi bi morali oceniti, ali je institucija ustrezno opredelila, ocenila in zmanjšala tveganja, povezana z IKT. Postopek bi moral spadati v okvir upravljanja operativnega tveganja in se skladati s pristopom k operativnemu tveganju.

36. Pristojni organi bi morali najprej ugotoviti, katera so pomembna inherentna tveganja, povezana z IKT, ki jim je ali bi jim bila lahko izpostavljena institucija, nato pa oceniti učinkovitost okvira institucije za upravljanje tveganj, povezanih z IKT, ter postopkov in kontrol za zmanjševanje teh tveganj. Rezultat ocene bi moral biti vključen v povzetek ugotovitev, ki se uporabi za izračun rezultata operativnega tveganja v skladu s Smernicami organa EBA o SREP. Če je tveganje, povezano z IKT, označeno za pomembno in mu želijo pristojni organi dodeliti posamezen rezultat, se uporabi tabela 1 za dodelitev rezultata podtveganja v okviru operativnega tveganja.

37. Pri pripravi ocene v skladu s tem naslovom bi morali pristojni organi uporabiti vse razpoložljive vire informacij, kot je navedeno v odstavku 127 naslova 6 Smernic organa EBA o SREP, npr. dejavnosti institucije za upravljanje tveganja, poročanje in rezultati, ter jih vzeti za podlago pri opredelitvi svojih prednostnih nalog pri nadzorni oceni. Pristojni organi bi morali pri pripravi ocene uporabiti tudi druge vire informacij, vključno z naslednjimi, če je to ustrezno:

    a. samoocene tveganja, povezanega z IKT, in kontrol (če so vključene v informacije o ICAAP);
    b. upravljavske informacije v zvezi s tveganjem, povezanim z IKT, ki so predložene upravljalnemu organu institucije, npr. redno poročanje o tveganju, povezanem z IKT, na podlagi incidentov (tudi v zbirki podatkov o operativnih izgubah) in podatki o izpostavljenosti tveganju, povezanemu z IKT, ki jih posreduje funkcija upravljanja tveganja institucije;
    c. ugotovitve notranje in zunanje revizije v zvezi z IKT, ki se sporočijo revizijskemu odboru institucije.

3.2 Opredelitev pomembnih tveganj, povezanih z IKT

38. Pristojni organi bi morali s spodaj navedenimi koraki opredeliti pomembna tveganja, povezana z IKT, ki jim je ali bi jim lahko bila izpostavljena institucija.

3.2.1 Pregled profila tveganja, povezanega z IKT

39. Pri pregledu profila tveganja, povezanega z IKT, bi morali pristojni organi upoštevati vse ustrezne informacije o izpostavljenostih institucije tveganju, povezanemu z IKT, vključno z informacijami iz

odstavka 37 ter ugotovljenimi pomembnimi pomanjkljivostmi ali slabostmi v organizaciji IKT in kontroli na ravni celotne institucije, kot je določeno v naslovu 2 teh smernic, po potrebi pa te informacije tudi sorazmerno pregledati. Kot del tega pregleda bi morali pristojni organi upoštevati:

a. možen vpliv bistvene motnje v sistemih IKT institucije na finančni sistem, bodisi na državni ali na mednarodni ravni;
b. ali za institucijo morda veljajo tveganja glede varnosti IKT ali razpoložljivosti in neprekinjenega delovanja IKT zaradi odvisnosti od interneta, visoke stopnje prevzemanja inovativnih rešitev IKT ali drugih poslovnih distribucijskih kanalov, zaradi katerih je institucija verjetnejša tarča kibernetskih napadov;
c. ali je institucija morda bolj izpostavljena tveganjem glede varnosti IKT, razpoložljivosti in neprekinjenega delovanja IKT, celovitosti podatkov IKT ali sprememb IKT zaradi zapletenosti (npr. kot posledica združitev ali prevzemov) ali zastarelosti svojih sistemov IKT;
d. ali institucija uvaja pomembne spremembe sistemov IKT in/ali funkcije IKT (npr. kot posledica združitev, prevzemov, prodaj ali nadomestitve temeljnih sistemov IKT), ki lahko škodljivo vplivajo na stabilnost ali pravilno delovanje sistemov ter lahko vodijo do pomembnih tveganj glede razpoložljivosti in neprekinjenega delovanja IKT, varnosti IKT, sprememb IKT ali celovitosti podatkov IKT;
e. ali je institucija storitve IKT ali sisteme IKT oddala v zunanje izvajanje v skupini ali zunaj nje, kar bi ji lahko povzročilo pomembna tveganja glede zunanjega izvajanja IKT;
f. ali institucija izvaja agresivne ukrepe za varčevanje pri IKT, kar lahko povzroči zmanjšanje potrebnih naložb v IKT, virov in strokovnega znanja o IT ter poveča izpostavljenost vsem vrstam tveganja, povezanega z IKT, v taksonomiji;
g. ali je institucija zaradi lokacije pomembnih centrov za delovanje/podatke IKT (npr. regije, države) morda izpostavljena naravnim nesrečam (npr. poplavam, potresom), politični nestabilnosti ali sporom z delovno silo in civilnim nemirom, ki lahko povzročijo pomembno povečanje tveganj glede razpoložljivosti in neprekinjenega delovanja IKT ter varnosti IKT.

3.2.2 Pregled kritičnih sistemov in storitev IKT

40. Kot del postopka opredelitve tveganj, povezanih z IKT, ki imajo lahko znaten bonitetni vpliv na institucijo, bi morali pristojni organi pregledati dokumentacijo institucije in oblikovati mnenje o tem, kateri sistemi in storitve IKT so kritični za primerno obratovanje, razpoložljivost, neprekinjeno delovanje in varnost ključnih dejavnosti institucije.

41. V ta namen bi morali pristojni organi pregledati metodologijo in postopke, ki jih uporablja institucija, da bi ugotovila, kateri sistemi in storitve IKT so kritični, pri tem pa bi morali upoštevati, da so nekateri sistemi in storitve IKT za institucijo morda kritični z vidikov neprekinjenega poslovanja in razpoložljivosti, varnosti (npr. preprečevanje goljufij) in/ali zaupnosti (npr. zaupni podatki). Pri izvajanju pregleda pristojni organi upoštevajo, da bi morali kritični sistemi in storitve IKT izpolnjevati najmanj enega od naslednjih pogojev:

a. podpirajo osrednje poslovne operacije in distribucijske kanale (npr. bankomate, spletno in mobilno bančništvo) institucije;

b. podpirajo ključne procese upravljanja in korporativne funkcije, vključno z upravljanjem tveganja (npr. sistemi za upravljanje tveganja in upravljanje denarnih sredstev);

c. zanje veljajo posebne pravne ali regulativne zahteve (če obstajajo), ki določajo poostrene zahteve glede razpoložljivosti, odpornosti, zaupnosti ali varnosti (npr. zakonodaja o varstvu podatkov ali morebitni ciljni čas obnove (RTO, najdaljši čas, v katerem je treba po incidentu obnoviti sistem ali postopek) in ciljna točka obnove (RPO, najdaljši čas, v katerem se lahko v primeru incidenta podatki izgubijo)) za nekatere sistemsko pomembne storitve (kjer in če je to ustrezno);

d. obdelujejo ali shranjujejo zaupne ali občutljive podatke, ki bi lahko ob nepooblaščenem dostopu bistveno vplivali na ugled institucije, njene finančne rezultate ali njeno trdnost in neprekinjeno poslovanje (npr. zbirke občutljivih podatkov strank); in/ali

e. omogočajo temeljne funkcionalnosti, ki so ključne za ustrezno delovanje institucije (npr. telekomunikacijske storitve in storitve povezljivosti ter storitve IKT in kibernetske varnosti).

3.2.3 Opredelitev pomembnih tveganj, povezanih z IKT, za kritične sisteme in storitve IKT

42. Ob upoštevanju opravljenih pregledov profila tveganja, povezanega z IKT, ter zgoraj navedenih kritičnih sistemov in storitev IKT v instituciji bi morali pristojni organi pripraviti mnenje o pomembnih tveganjih, povezanih z IKT, ki imajo lahko po njihovi nadzorniški presoji bistven bonitetni vpliv na kritične sisteme in storitve IKT v instituciji.

43. Pri ocenjevanju morebitnega vpliva tveganj, povezanih z IKT, na kritične sisteme in storitve IKT institucije bi morali pristojni organi upoštevati:

a. finančni vpliv, med drugim vključno z izgubo sredstev ali premoženja, morebitnimi odškodninami strankam, pravnimi stroški in stroški sanacije, pogodbeno odškodnino in izgubljenim prihodkom;

b. možnosti za motnje v poslovanju, med drugim upoštevajoč kritičnost prizadetih finančnih storitev; število strank in/ali podrejenih družb in zaposlenih, ki bi bili lahko prizadeti;

c. možni vpliv na ugled institucije glede na kritičnost prizadete bančne storitve ali operativne dejavnosti (npr. kraja podatkov strank); zunanji profil/prepoznavnost prizadetih sistemov in storitev IKT (npr. sistemi za mobilno ali spletno bančništvo, prodajna mesta, bankomati ali plačilni sistemi);

d. regulativni vpliv, vključno z možnostjo javne graje s strani zakonodajnega organa, globami ali celo spremembo dovoljenj;

e. strateški vpliv na institucijo, na primer če pride do ogroženosti ali kraje strateškega proizvoda ali poslovnih načrtov.

44. Pristojni organi bi morali nato opredeljena tveganja, povezana z IKT, ki veljajo za pomembna, razvrstiti v naslednje kategorije, za katere so dodatni opisi tveganj in primeri navedeni v Prilogi. Pristojni organi bi morali o tveganjih, povezanih z IKT, ki so navedena v Prilogi, razmisliti v okviru ocene iz naslova 3:

a. tveganje glede razpoložljivosti in neprekinjenega delovanja IKT,
b. tveganje glede varnosti IKT,

c. tveganje glede sprememb IKT,
d. tveganje glede celovitosti podatkov IKT,
e. tveganje glede zunanjega izvajanja IKT.

Razvrščanje v kategorije pristojnim organom pomaga ugotoviti, katera tveganja so pomembna (če obstajajo) ter bi jih bilo torej treba pobližje in/ali bolj poglobljeno proučiti v naslednjih ocenjevalnih korakih.

3.3 Ocena kontrol za zmanjševanje pomembnih tveganj, povezanih z IKT

45. Za oceno izpostavljenosti institucije preostalemu tveganju, povezanemu z IKT, bi morali pristojni organi proučiti, kako institucija opredeljuje, spremlja, ocenjuje in zmanjšuje pomembna tveganja, ki so jih pristojni organi opredelili v zgornji oceni.

46. V ta namen bi morali pristojni organi za opredeljena pomembna tveganja, povezana z IKT, pregledati veljavne:

a. politiko upravljanja tveganja, povezanega z IKT, procese in pragove sprejemljivega tveganja;
b. organizacijsko upravljanje in nadzorni okvir;
c. obseg in ugotovitve notranje revizije; in
d. kontrole tveganja, povezanega z IKT, ki se nanašajo posebej na opredeljeno pomembno tveganje, povezano z IKT.

47. Pri oceni bi bilo treba upoštevati rezultat analize upravljanja celotnega tveganja in okvira notranjih kontrol, kot je omenjeno v naslovu 5 Smernic organa EBA o SREP, pa tudi upravljanje in strategijo institucije, kot je navedeno v naslovu 2 teh smernic, saj lahko bistvene pomanjkljivosti, ugotovljene na teh področjih, vplivajo na sposobnost institucije, da upravlja in zmanjšuje svojo izpostavljenost tveganju, povezanemu z IKT. Kjer je to ustrezno, bi morali pristojni organi uporabiti tudi vire informacij iz odstavka 37 teh smernic.

48. Pristojni organi bi morali naslednje ocenjevalne korake izvesti na način, ki je sorazmeren z naravo, obsegom in zapletenostjo dejavnosti institucije ter z uporabo nadzorniškega pregledovanja, ki ustreza njenemu profilu tveganja, povezanega z IKT.

3.3.1 Politika upravljanja tveganja, povezanega z IKT, procesi in pragovi sprejemljivega tveganja

49. Pristojni organi bi morali proučiti, ali je institucija sprejela ustrezne politike upravljanja tveganja, procese in pragove sprejemljivega tveganja za opredeljena pomembna tveganja, povezana z IKT. Lahko so del okvira upravljanja operativnega tveganja ali pa spadajo v ločen dokument. Pri tej oceni bi morali pristojni organi upoštevati, ali:

a. je politika upravljana tveganja formalizirana, jo je odobril upravljalni organ ter vsebuje dovolj smernic o nagnjenosti institucije k prevzemanju tveganja, povezanega z IKT, glavnih

ciljih upravljanja tega tveganja in/ali uporabljenih pragovih sprejemljivega tveganja. O politiki upravljanja tveganja, povezanega z IKT, se obvestijo tudi vsi ustrezni deležniki;

b. veljavna politika zajema vse pomembne elemente za upravljanje opredeljenih pomembnih tveganj, povezanih z IKT;

c. je institucija uvedla proces in osnovne postopke za opredelitev (npr. samoocena tveganja in kontrol, analiza scenarijev tveganja) in spremljanje zadevnih pomembnih tveganj, povezanih z IKT; in

d. je institucija uvedla poročanje o upravljanju tveganja, povezanega z IKT, s katerim se višjemu vodstvu in upravljalnemu organu pravočasno posredujejo informacije ter se jima omogoči, da ocenita in spremljata, ali so načrti in ukrepi institucije za zmanjševanje tveganja, povezanega z IKT, skladni z odobrenimi nagnjenostjo k prevzemanju tveganja in/ali pragovi sprejemljivega tveganja (če je to ustrezno), ter spremljata spremembe pomembnih tveganj, povezanih z IKT.

3.3.2 Organizacijsko upravljanje in nadzorni okvir

50. Pristojni organi bi morali oceniti, kako so veljavne vloge in odgovornosti pri upravljanju tveganja vgrajene in vključene v notranjo organizacijo za upravljanje in nadziranje opredeljenih pomembnih tveganj, povezanih z IKT. V zvezi s tem bi morali pristojni organi oceniti, ali institucija izkazuje:

a. jasne vloge in odgovornosti za opredelitev, oceno, spremljanje in zmanjševanje zadevnih pomembnih tveganj, povezanih z IKT, ter za poročanje o njih in nadzor nad njimi;

b. da so vloge in odgovornosti v zvezi s tveganjem jasno sporočene, dodeljene in vgrajene v vse ustrezne dele (npr. poslovna področja, IT) in procese organizacije, vključno z vlogami in odgovornostmi za zbiranje in združevanje informacij o tveganju ter poročanje o njih višjemu vodstvu in/ali upravljalnemu organu;

c. da se dejavnosti upravljanja tveganja, povezanega z IKT, izvajajo z ustreznimi človeškimi in tehničnimi viri primerne kakovosti. Za ocenjevanje verodostojnosti veljavnih načrtov za zmanjševanje tveganja bi morali pristojni organi oceniti tudi, ali je institucija za njihovo izvedbo dodelila ustrezne finančne proračune in/ali druge potrebne vire;

d. ustrezno nadaljnjo obravnavo in odgovor upravljalnega organa, kar zadeva pomembne ugotovitve neodvisnih kontrolnih funkcij o tveganjih, povezanih z IKT, ob upoštevanju možnega prenosa nekaterih vidikov na odbor, če ta obstaja; in

e. da so izvzetosti iz veljavnih predpisov in politik zabeležene ter vključene v evidentiran pregled in poročanje neodvisne kontrolne funkcije s poudarkom na z njimi povezanih tveganjih.

3.3.3 Obseg in ugotovitve notranje revizije

51. Pristojni organi bi morali ugotoviti, ali je funkcija notranje revizije učinkovita, ko gre za revizijo veljavnega okvira kontrol tveganja, povezanega z IKT, in sicer tako, da proučijo, ali:

a. se revizija okvira kontrol tveganja, povezanega z IKT, izvaja z zahtevano kakovostjo, podrobnostjo in pogostostjo ter sorazmerno z velikostjo, dejavnostmi in profilom tveganja, povezanega z IKT;

b. načrt revizije vključuje revizije kritičnih tveganj, povezanih z IKT, ki jih opredeli institucija;

c. se o pomembnih ugotovitvah revizij IKT, vključno z dogovorjenimi ukrepi, poroča upravljalnemu organu; in

d. ugotovitve revizij IKT, vključno z dogovorjenimi ukrepi, nadalje obravnava višje vodstvo in/ali revizijski odbor, prav tako pa redno pregleduje poročila o napredku.

3.3.4 Kontrole tveganja, povezanega z IKT, ki se nanašajo posebej na opredeljena pomembna tveganja, povezana z IKT

52. Za opredeljena pomembna tveganja, povezana z IKT, bi morali pristojni organi oceniti, ali ima institucija ustrezne kontrole za njihovo obravnavo. Naslednji oddelki vsebujejo neizčrpen seznam posebnih kontrol, ki jih je treba upoštevati pri ocenjevanju pomembnih tveganj, opredeljenih v točki 3.2.3, ki so bila razvrščena v naslednje kategorije tveganj, povezanih z IKT:

a. tveganja glede razpoložljivosti in neprekinjenega delovanja IKT;
b. tveganja glede varnosti IKT;
c. tveganja glede sprememb IKT;
d. tveganja glede celovitosti podatkov IKT;
e. tveganja glede zunanjega izvajanja IKT.

(a) Kontrole za upravljanje pomembnih tveganj glede razpoložljivosti in neprekinjenega delovanja IKT

53. Poleg zahtev iz Smernic organa EBA o SREP (odstavki 279 do 281) bi morali pristojni organi oceniti, ali ima institucija ustrezen okvir za opredelitev, razumevanje, merjenje in zmanjševanje tveganj glede razpoložljivosti in neprekinjenega delovanja IKT.

54. Pri tej oceni bi morali pristojni organi zlasti upoštevati, ali okvir:

a. kritične procese IKT in ustrezne podporne sisteme IKT, ki bi morali biti vključeni v načrte za poslovno odpornost in neprekinjeno poslovanje, opredeljuje s:

i. celovito analizo odvisnosti med kritičnimi poslovnimi procesi in podpornimi sistemi;

ii. določitvijo ciljev obnove za podporne sisteme IKT (te na primer v obliki ciljnega časa obnove in ciljne točke obnove običajno določajo podjetje in/ali predpisi);

iii. ustreznimi kriznimi načrti, ki omogočajo razpoložljivost, neprekinjeno delovanje in obnovo kritičnih sistemov in storitev IKT, da bi motnje v poslovanju institucije omejili na sprejemljiv obseg;

b. ima poslovno odpornost, politike za neprekinjeno delovanje nadzornega okolja ter standarde in operativne kontrole, ki vključujejo:

i. ukrepe za preprečevanje razmer, v katerih bi en sam scenarij, incident ali nesreča vplivala tako na produkcijske sisteme IKT kot tudi na sisteme IKT za obnovo;

ii. postopke varnostnih kopij in obnove sistemov IKT za kritično programsko opremo in podatke, s katerimi je zagotovljeno, da se varnostne kopije shranjujejo na varnem in dovolj oddaljenem mestu, da incident ali nesreča ne more uničiti ali pokvariti kritičnih podatkov;

iii. spremljanje rešitev za pravočasno odkrivanje incidentov z zvezi z razpoložljivostjo ali neprekinjenim delovanjem IKT;

iv. dokumentiran proces obvladovanja in stopnjevanja incidentov, ki zagotavlja tudi smernice o različnih vlogah in odgovornostih v zvezi z obvladovanjem in stopnjevanjem incidentov, članih kriznih odborov in hierarhije dajanja navodil ob izrednih dogodkih;

v. fizične ukrepe tako za zaščito kritične infrastrukture IKT (npr. podatkovnih centrov) institucije pred okoljskimi tveganji (npr. poplavami in drugimi naravnimi nesrečami) kot tudi za zagotavljanje ustreznega obratovalnega okolja za sisteme IKT (npr. klimatske naprave);

vi. procese, vloge in odgovornosti za zagotavljanje, da so tudi sistemi in storitve IKT, oddani v zunanje izvajanje, zajeti v ustrezne rešitve in načrte za poslovno odpornost in neprekinjeno poslovanje;

vii. rešitve za načrtovanje in spremljanje uspešnosti in zmogljivosti IKT za kritične sisteme in storitve IKT z opredeljenimi zahtevami glede razpoložljivosti, da bi pravočasno opazili pomembne omejitve uspešnosti in zmogljivosti;

viii. če je to potrebno in ustrezno, rešitve za zaščito kritičnih internetnih dejavnosti ali storitev (npr. storitve e-bančništva) pred zavrnitvami storitve in drugimi kibernetskimi napadi prek interneta, ki so namenjeni preprečevanju ali motenju dostopa do teh dejavnosti in storitev;

c. preizkuša rešitve za razpoložljivost in neprekinjeno delovanje IKT v primeru različnih realističnih scenarijev, vključno s kibernetskimi napadi, preizkusi nadomestnega načina delovanja in preizkusi varnostnih kopij kritične programske opreme in podatkov, ki:

i. so načrtovani, formalizirani in dokumentirani, rezultati preizkusov pa se uporabijo za izboljšanje učinkovitosti rešitev za razpoložljivost in neprekinjeno delovanje IKT;

ii. vključujejo deležnike in funkcije znotraj organizacije, kot je vodstvo poslovnega področja, vključno s skupinami za neprekinjeno poslovanje, odzivanje na incidente in odzivanje na krize, ter ustrezne zunanje deležnike v ekosistemu;

iii. zagotavljajo ustrezno sodelovanje z upravljalnim organom in višjim vodstvom (npr. kot del skupine za krizno upravljanje), ki sta tudi obveščena o rezultatih preizkusov.

(b) Kontrole za upravljanje pomembnih tveganj glede varnosti IKT

55. Pristojni organi bi morali oceniti, ali ima institucija učinkovit okvir za opredelitev, razumevanje, merjenje in zmanjševanje tveganj glede varnosti IKT. Pri tej oceni bi morali pristojni organi zlasti preveriti, ali okvir upošteva:

a. jasno opredeljene vloge in odgovornosti glede:
   i. oseb in/ali odborov, ki so pristojni in/ali odgovorni za vsakodnevno upravljanje varnosti IKT ter pripravo splošnih politik za varnost IKT s poudarkom na potrebi po njihovi neodvisnosti;
   ii. zasnove, izvedbe, upravljanja in spremljanja varnostnih kontrol IKT;
   iii. zaščite kritičnih sistemov in storitev IKT, tako da se sprejmejo na primer proces ocenjevanja ranljivosti, upravljanje programskih popravkov, zaščita na končni točki (npr. v primeru zlonamernega virusa) ter orodja za zaznavanje in preprečevanje vdorov;
   iv. spremljanja, razvrščanja in obravnave zunanjih ali notranjih incidentov v zvezi z varnostjo IKT, vključno z odzivanjem na incidente ter ponovnim zagonom in obnovitvijo sistemov in storitev IKT;
   v. rednih in proaktivnih ocen nevarnosti za vzdrževanje ustreznih varnostnih kontrol;

b. politiko za varnost IKT, ki upošteva in po potrebi spoštuje mednarodno priznane standarde varnost in varnostna načela IKT (npr. načelo najmanjših pravic – omejitev dostopa na najnižjo raven, ki še omogoča običajno delovanje, pri upravljanju pravic dostopa, in načelo obrambe v globino – večplastni varnostni mehanizmi, ki izboljšajo varnost sistema kot celote, pri načrtovanju varnostne arhitekture);

c. proces za opredelitev sistemov in storitev IKT ter sorazmernih varnostnih zahtev za IKT, ki odražajo tveganje goljufij in/ali možne nepravilne uporabe in/ali zlorabe zaupnih podatkov, ter dokumentirana pričakovanja glede varnosti, ki jih je treba upoštevati pri teh opredeljenih sistemih, storitvah in podatkih IKT ter so usklajena s pragom sprejemljivega tveganja institucije, poleg tega pa se spremlja njihovo pravilno izvajanje;

d. dokumentiran proces obvladovanja in stopnjevanja varnostnih incidentov, ki zagotavlja smernice o različnih vlogah in odgovornostih v zvezi z obvladovanjem in stopnjevanjem incidentov, članih kriznih odborov in hierarhije dajanja navodil ob izrednih varnostnih dogodkih;

e. beleženje dejavnosti uporabnikov in skrbnikov, ki omogoča učinkovito spremljanje ter pravočasno zaznavanje nepooblaščenih dejavnosti in odzivanje nanje; namenjeno je izvajanju forenzičnih preiskav varnostnih incidentov ali pomoči pri takih raziskavah. Institucija bi morala sprejeti politiko beleženja, v kateri so opredeljeni ustrezne vrste evidenc, ki jih je treba voditi, in obdobje shranjevanja takih evidenc;

f. kampanje in pobude za ozaveščanje in obveščanje, s katerimi se vse ravni institucije obvestijo o varni uporabi in zaščiti sistemov IKT ter glavnih tveganjih glede varnosti IKT (in drugih tveganjih), ki se jih je treba zavedati, zlasti kar zadeva obstoječe in razvijajoče se kibernetske nevarnosti (npr. računalniške viruse, možne notranje ali zunanje zlorabe ali napade, kibernetske napade) ter njihovo vlogo pri zmanjševanju kršitev varnosti;

g. ustrezne fizične varnostne ukrepe (npr. videokamere, protivlomni alarm, varnostna vrata) za preprečevanje nepooblaščenega fizičnega dostopa do kritičnih in občutljivih sistemov IKT (npr. podatkovnih centrov);

h. ukrepe za zaščito sistemov IKT pred napadi z interneta (npr. kibernetskimi napadi) ali drugih zunanjih omrežij (npr. tradicionalnih telekomunikacijskih povezav ali povezav z zanesljivimi partnerji). Pristojni organi bi morali preveriti, ali okvir institucije upošteva:

   i. proces in rešitve za vzdrževanje popolnega in posodobljenega popisa in pregleda vseh navzven usmerjenih priključnih točk omrežij (npr. spletišča, internetne aplikacije, brezžična omrežja, dostop na daljavo), prek katerih bi lahko tretja oseba vdrla v notranje sisteme IKT;

   ii. strogo upravljane in nadzorovane varnostne ukrepe (npr. požarne zidove, posredniške strežnike, posredovalnike elektronske pošte, protivirusne skenerje in skenerje vsebine) za zaščito vhodnega in izhodnega omrežnega prometa (npr. elektronske pošte) ter navzven usmerjenih priključnih točk omrežij, prek katerih bi lahko tretja oseba vdrla v notranje sisteme IKT;

   iii. procese in rešitve za zaščito spletišč in aplikacij, ki jih je mogoče neposredno napasti z interneta in/ali od zunaj ter jih uporabiti kot vhodno točko za dostop do notranjih sistemov IKT. Ti procesi in rešitve na splošno obsegajo mešanico priznanih praks varnega razvoja, praks krepitve in skeniranja sistemov IKT za ranljivosti in/ali uvedbo dodatnih varnostnih rešitev, kot so na primer požarni sistemi v aplikacijah in/ali sistemi za zaznavanje in/ali preprečevanje vdorov;

   iv. redno preizkušanje prodora skozi varnostne ukrepe, da bi ocenili učinkovitost izvedenih kibernetskih in notranjih ukrepov in procesov za varnost IKT. Preizkuse bi morali izvajati zaposleni in/ali zunanji izvedenci s potrebnim strokovnim znanjem, dokumentirane rezultate in sklepe pa sporočiti višjemu vodstvu in/ali upravljalnemu organu. Če je to potrebno in ustrezno, bi morala institucija iz preizkusov ugotoviti, kje mora dodatno izboljšati varnostne kontrole in procese in/ali pridobiti boljša zagotovila o njihovi učinkovitosti.

(c) Kontrole za upravljanje pomembnih tveganj glede sprememb IKT

56. Pristojni organi bi morali oceniti, ali ima institucija učinkovit okvir za opredelitev, razumevanje, merjenje in zmanjševanje tveganj glede sprememb IKT, ki je sorazmeren z naravo, obsegom in zapletenostjo dejavnosti institucije ter njenim profilom tveganja, povezanega z IKT. Okvir institucije bi moral zajemati tveganja, povezana z razvojem, preizkušanjem in odobritvijo sprememb sistemov IKT, vključno z razvojem ali spremembo programske opreme, preden so prenesene v produkcijsko okolje, zagotavljati pa bi moral tudi ustrezno upravljanje življenjskega cikla IKT. Pri tej oceni bi morali pristojni organi zlasti preveriti, ali okvir upošteva:

a. dokumentirane procese za upravljanje in nadziranje sprememb sistemov IKT (npr. upravljanje konfiguracije in popravkov) in podatkov IKT (npr. rešitve za hrošče ali popravki podatkov), ki zagotavljajo ustrezno upravljanje tveganj, povezanih z IKT, v primeru pomembnih sprememb IKT, ki lahko bistveno vplivajo na profil tveganja institucije ali njeno izpostavljenost tveganju;

b. specifikacije o zahtevanem ločevanju dolžnosti v različnih fazah izvedenih procesov sprememb IKT (npr. zasnova in razvoj rešitev, preizkušanje in odobritev nove programske opreme in/ali sprememb, prenos in izvedba v produkcijskem okolju ter rešitve za hrošče) s poudarkom na rešitvah in ločevanju dolžnosti za upravljanje in nadziranje sprememb produkcijskih sistemov in podatkov IKT, ki jih izvede osebje IKT (npr. razvijalci, skrbniki sistemov IKT, skrbniki zbirk podatkov) ali druge osebe (npr. poslovni uporabniki, ponudniki storitev);

c. testna okolja, ki so dovolj podobna produkcijskim okoljem;

d. popis obstoječih aplikacij in sistemov IKT v produkcijskem okolju, pa tudi v testnem in razvojnem okolju, da je mogoče zahtevane spremembe (npr. posodobitve ali nadgradnje različic, popravke sistemov, spremembe konfiguracije) ustrezno upravljati, izvajati in spremljati za vse zadevne sisteme IKT;

e. proces za spremljanje in upravljanje življenjskega cikla uporabljenih sistemov IKT, ki zagotavlja, da ti sistemi še naprej izpolnjujejo in podpirajo dejanske poslovne zahteve in zahteve upravljanja tveganja ter da imajo uporabljene rešitve in sistemi IKT še vedno podporo prodajalcev, spremljati pa jih morajo tudi ustrezni postopki za življenjski cikel razvoja programske opreme;

f. sistem za nadzor različic izvorne kode in ustrezne postopke za preprečevanje nepooblaščenih sprememb izvorne kode programske opreme, ki se razvija znotraj institucije;

g. proces za preverjanje varnosti in ranljivosti novih ali pomembno spremenjenih sistemov IKT in programske opreme, preden se ti prenesejo v produkcijsko okolje in izpostavijo možnim kibernetskim napadom;

h. proces in rešitve za preprečevanje nepooblaščenega ali nenamernega razkritja zaupnih podatkov, ko se sistemi IKT nadomestijo, arhivirajo, zavržejo ali uničijo;

i. procese neodvisnega pregleda in potrjevanja za zmanjšanje tveganja človeških napak pri izvajanju sprememb sistemov IKT, ki imajo lahko pomemben škodljiv vpliv na razpoložljivost, neprekinjeno poslovanje ali varnost institucije (npr. pomembne spremembe konfiguracije požarnega zidu, spremembe požarnih zidov).

(d) Kontrole za upravljanje pomembnih tveganj glede celovitosti podatkov IKT

57. Pristojni organi bi morali oceniti, ali ima institucija učinkovit okvir za opredelitev, razumevanje, merjenje in zmanjševanje tveganj glede celovitosti podatkov IKT, ki je sorazmeren z naravo, obsegom in zapletenostjo dejavnosti institucije ter njenim profilom tveganja, povezanega z IKT. Okvir institucije bi moral upoštevati tveganja, povezana z ohranitvijo celovitosti podatkov, ki se shranjujejo in obdelujejo v sistemih IKT. Pri tej oceni bi morali pristojni organi zlasti preveriti, ali okvir upošteva:

a. politiko, ki opredeljuje vloge in odgovornosti pri upravljanju celovitosti podatkov v sistemih IKT (npr. podatkovni arhitekt, odgovorne osebe za podatke[6], skrbniki podatkov[7], lastniki/nadzorniki

[6] Odgovorna oseba za podatke je odgovorna za obdelavo in uporabo podatkov.
[7] Skrbnik podatkov je odgovoren za varno skrbništvo, prevoz in shranjevanje podatkov.

podatkov[8]) ter vključuje smernice o podatkih, ki so kritični z vidika celovitosti podatkov in bi bilo treba zanje uvesti posebne kontrole IKT (npr. avtomatizirane kontrole za potrjevanje vnosov, kontrole prenosa podatkov, uskladitve itd.) ali preglede (npr. preverjanje združljivosti s podatkovno arhitekturo) v različnih fazah življenjskega cikla podatkov IKT;

b. dokumentirano podatkovno arhitekturo, podatkovni model in/ali slovar, ki je potrjen pri ustreznih poslovnih in računalniških deležnikih, namenjen pa je podpiranju potrebne skladnosti podatkov v vseh sistemih IKT ter zagotavljanju, da so podatkovna arhitektura, podatkovni model in/ali slovar stalno usklajeni s poslovnimi potrebami in potrebami upravljanja tveganja;

c. politiko o dovoljeni uporabi računalništva končnega uporabnika in zanašanju nanj, zlasti kar zadeva opredelitev, registracijo in dokumentacijo pomembnih računalniških rešitev končnega uporabnika (npr. pri obdelavi pomembnih podatkov) ter pričakovane varnostne stopnje za preprečevanje nepooblaščenih sprememb tako orodja kot tudi v njem shranjenih podatkov;

d. dokumentirane procese za obravnavo izjem, ki so namenjeni reševanju prepoznanih težav s celovitostjo podatkov IKT v skladu z njihovo kritičnostjo in občutljivostjo.

58. V primeru nadziranih institucij, ki spadajo v področje uporabe načel BCBS 239 glede učinkovitega združevanja podatkov o tveganjih in poročanja o tveganjih[9], bi morali pristojni organi pregledati analizo zmogljivosti institucije za poročanje o tveganjih in združevanje podatkov v primerjavi z načeli in pripravljeno dokumentacijo o tem, pri tem pa upoštevati časovni okvir za izvedbo in prehodne ureditve v teh načelih.

(e) Kontrole za upravljanje pomembnih tveganj glede zunanjega izvajanja IKT

59. Pristojni organi bi morali oceniti, ali strategija institucije za zunanje izvajanje v skladu z zahtevami smernic odbora SEBS o zunanjem izvajanju (2006) in zahtevo iz odstavka 85(d) Smernic organa EBA o SREP ustrezno velja za zunanje izvajanje IKT, vključno z oddajanjem storitev IKT v zunanje izvajanje subjektu znotraj skupine. Pri ocenjevanju tveganj glede zunanjega izvajanja IKT bi morali pristojni organi upoštevati, da so lahko ta tveganja zajeta tudi v oceno inherentnih operativnih tveganj iz odstavka 240(j) Smernic organa EBA o SREP, da bi preprečili podvajanje dela ali dvojno štetje.

60. Pristojni organi bi morali zlasti oceniti, ali ima institucija učinkovit okvir za opredelitev, razumevanje, merjenje in zmanjševanje tveganj glede zunanjega izvajanja IKT, zlasti pa kontrole in nadzorno okolje za zmanjševanje tveganj glede pomembnih storitev IKT, oddanih v zunanje izvajanje, ki so sorazmerni z velikostjo institucije, njenimi dejavnostmi in profilom tveganj, povezanih z IKT, ter vključujejo:

a. oceno učinka zunanjega izvajanja IKT na upravljanje tveganja v instituciji v zvezi z uporabo ponudnikov storitev (npr. ponudnikov storitev v oblaku) in njihovih storitev v procesu javnega naročanja, ki je dokumentirana in jo višje vodstvo ali upravljalni organ upošteva pri odločanju, ali

[8] Nadzornik podatkov je odgovoren za upravljanje in primernost podatkovnih elementov – tako vsebine kot tudi metapodatkov.

[9] Baselski odbor za bančni nadzor, Načela učinkovitega združevanja podatkov o tveganjih in poročanja o tveganjih, januar 2013, dostopno na spletu: http://www.bis.org/publ/bcbs239.pdf.

naj storitve odda v zunanje izvajanje ali ne. Institucija bi morala pregledati politike upravljanja tveganja, povezanega z IKT, ter kontrole IKT in nadzorno okolje ponudnika storitev, da bi se prepričala, ali ustrezajo njenim ciljem notranjega upravljanja tveganja in nagnjenosti k prevzemanju tveganja. Pregled bi bilo treba v pogodbenem obdobju zunanjega izvajanja redno posodabljati, pri tem pa upoštevati značilnosti storitev, oddanih v zunanje izvajanje;

b. spremljanje tveganj, povezanih z IKT, za storitve, oddane v zunanje izvajanje, v pogodbenem obdobju zunanjega izvajanja v okviru upravljanja tveganja institucije, pri čemer se ugotovitve upoštevajo pri poročanju institucije o upravljanju tveganj, povezanih z IKT (npr. poročanje o neprekinjenem poslovanju, poročanje o varnosti);

c. spremljanje in primerjavo prejetih ravni storitve s pogodbeno dogovorjenimi ravnmi storitve, ki bi morali biti del pogodbe o zunanjem izvajanju ali sporazuma o ravni storitve; in

d. ustrezno osebje, vire in pristojnosti za spremljanje in upravljanje tveganj, povezanih z IKT, ki izhajajo iz storitev, oddanih v zunanje izvajanje.

3.4 Povzetek ugotovitev in izračun rezultatov

61. Z zgoraj opisanim postopkom bi si morali pristojni organi oblikovati mnenje o tveganju institucije, povezanem z IKT. To mnenje bi moralo izražati povzetek ugotovitev, ki jih pristojni organi upoštevajo pri izračunu rezultata operativnega tveganja iz tabele 6 Smernic organa EBA o SREP. Pri mnenju o pomembnih tveganjih, povezanih z IKT, bi morali pristojni organi upoštevati naslednja merila za oceno operativnega tveganja:

a. Merila glede tveganja

i. Profil tveganja in izpostavljenosti institucije;
ii. opredeljeni kritični sistemi in storitve IKT; in
iii. pomembnost tveganja, povezanega z IKT, ko gre za kritične sisteme IKT.

b. Merila glede upravljanja in kontrol

i. Ali sta politika in strategija institucije za upravljanje tveganja, povezanega z IKT, usklajeni z njeno splošno strategijo in nagnjenostjo k prevzemanju tveganja;
ii. ali je organizacijski okvir za upravljanje tveganja, povezanega z IKT, zanesljiv ter ima jasne odgovornosti in jasno ločene naloge med prevzemniki tveganja ter funkcijama upravljanja in kontrole;
iii. ali so sistemi za merjenje in spremljanje tveganja, povezanega z IKT, ter poročanje o njem ustrezni; in
iv. ali so okviri kontrol za tveganje, povezano z IKT, učinkoviti.

62. Če pristojni organi tveganje, povezano z IKT, štejejo za pomembno ter se pristojni organ odloči, da bo rezultat za to tveganje izračunal kot podkategorijo operativnega tveganja, so v spodnji tabeli (tabeli 1) navedena merila za izračun rezultata tveganja, povezanega z IKT.

Tabela 1: Nadzorniška merila za izračun rezultata tveganja, povezanega z IKT

Rezultat tveganja	Nadzorniško mnenje	Merila glede inherentnih tveganj	Merila glede ustreznega upravljanja in kontrol
1	Glede na raven tveganja pri delovanju ter upravljanje in kontrolo ni bilo ugotovljeno nobeno zaznavno tveganje za znaten bonitetni vpliv na institucijo.	• Viri informacij, ki se upoštevajo v skladu z odstavkom 37, niso razkrili znatnih izpostavljenosti tveganju, povezanemu z IKT. • Narava profila tveganja, povezanega z IKT, skupaj s pregledom kritičnih sistemov IKT ter pomembnih tveganj, povezanih s sistemi in storitvami IKT, ni razkrila pomembnih tveganj, povezanih z IKT.	• Politika in strategija institucije glede tveganja, povezanega z IKT, sta sorazmerni z njeno splošno strategijo in nagnjenostjo k prevzemanju tveganja. • Organizacijski okvir za tveganje, povezano z IKT, je zanesljiv ter ima jasne odgovornosti in jasno ločene naloge med prevzemniki tveganja ter funkcijama upravljanja in kontrole. • Sistemi za merjenje in spremljanje tveganja, povezanega z IKT, ter poročanje o njem so ustrezni. • Okvir kontrol za tveganje, povezano z IKT, je učinkovit.
2	Glede na raven tveganja pri delovanju ter upravljanje in kontrolo je tveganje za znaten bonitetni vpliv na institucijo nizko.	• Viri informacij, ki se upoštevajo v skladu z odstavkom 37, niso razkrili znatnih izpostavljenosti tveganju, povezanem z IKT. • Narava profila tveganja, povezanega z IKT, skupaj s pregledom kritičnih sistemov IKT ter pomembnih tveganj, povezanih s sistemi in storitvami IKT, je razkrila omejeno izpostavljenost tveganju, povezanemu z IKT (npr. ne več kot 2 od 5 vnaprej določenih kategorij tveganja, povezanega z IKT).	
3	Glede na raven tveganja pri delovanju ter upravljanje in kontrolo je inherentno tveganje za znaten bonitetni vpliv na institucijo srednje.	• Viri informacij, ki se upoštevajo v skladu z odstavkom 37, so razkrili znake možnih znatnih izpostavljenosti tveganju, povezanem z IKT. • Narava profila tveganja, povezanega z IKT, skupaj s pregledom kritičnih sistemov IKT ter pomembnih tveganj, povezanih s sistemi in storitvami IKT, je razkrila povečano izpostavljenost tveganju, povezanemu z IKT (npr. 3 ali več od 5 vnaprej določenih kategorij tveganja, povezanega z IKT).	
4	Glede na raven	• Viri informacij, ki se upoštevajo v	

	tveganja pri delovanju ter upravljanje in kontrolo je inherentno tveganje za znaten bonitetni vpliv na institucijo visoko.	skladu z odstavkom 37, so zagotovili več znakov znatnih izpostavljenosti tveganju, povezanemu z IKT. • Narava profila tveganja, povezanega z IKT, skupaj s pregledom kritičnih sistemov IKT ter pomembnih tveganj, povezanih s sistemi in storitvami IKT, je razkrila visoko izpostavljenost tveganju, povezanemu z IKT (npr. 4 ali 5 od 5 vnaprej določenih kategorij tveganja, povezanega z IKT).	

Priloga – Taksonomija tveganja, povezanega z IKT

5 kategorij tveganja, povezanega z IKT, z neizčrpnim seznamom tveganj, povezanih z IKT, ki imajo možen vpliv visoke resnosti in/ali operativni vpliv, vpliv na ugled ali finančni vpliv

Kategorije tveganja, povezanega z IKT	Tveganja, povezana z IKT (neizčrpen seznam)[10]	Opis tveganja	Primeri
Tveganja glede razpoložljivosti in neprekinjenega delovanja IKT	Neustrezno upravljanje zmogljivosti	Pomanjkanje virov (npr. strojne opreme, programske opreme, osebja, ponudnikov storitev) lahko povzroči nezmožnost prilagajanja obsega storitve poslovnim potrebam, prekinitev delovanja sistemov, poslabšanje storitve in/ali operativne napake.	• Primanjkljaj zmogljivosti lahko vpliva na stopnje prenosa ter razpoložljivost omrežja (interneta) za storitve, kot je spletno bančništvo. • Pomanjkanje osebja (notranjega ali tretjih oseb) lahko povzroči prekinitve sistemov in/ali operativne napake.
	Izpad sistemov IKT	Izguba razpoložljivosti zaradi okvar strojne opreme.	• Okvara/napaka shranjevanja (trdi diski), strežnikov ali druge opreme IKT, ki nastane npr. zaradi pomanjkljivega vzdrževanja.
		Izguba razpoložljivosti zaradi okvar programske opreme in hroščev.	• Neskončna zanka v uporabniški programski opremi preprečuje izvedbo transakcije. • Izpadi zaradi nadaljnje uporabe zastarelih sistemov in rešitev IKT, ki ne izpolnjujejo več sodobnih zahtev glede razpoložljivosti in odpornosti in/ali jih prodajalci ne podpirajo več.
	Neustrezno načrtovanje neprekinjenega delovanja in obnovitve IKT po nesreči	Odpoved načrtovane razpoložljivosti IKT in/ali rešitev za neprekinjeno delovanje IKT in/ali obnovitve IKT po nesreči (npr. nadomestni podatkovni center za obnovitev), ko so aktivirane v odziv na nesrečo.	• Zaradi razlik v konfiguraciji primarnega in sekundarnega podatkovnega centra se lahko zgodi, da nadomestni podatkovni center ne more zagotoviti načrtovanega neprekinjenega delovanja storitve.

[10] Tveganja, povezana z IKT, so navedena v kategoriji tveganja, na katero imajo največji vpliv, vendar lahko vplivajo tudi na druge kategorije tveganja.

Kategorije tveganja, povezanega z IKT	Tveganja, povezana z IKT (neizčrpen seznam)[10]	Opis tveganja	Primeri
	Moteči ali uničujoči kibernetski napadi	Napadi z različnimi nameni (npr. aktivizem, izsiljevanje), ki povzročijo preobremenitev sistemov in omrežja, zakonitim uporabnikom pa preprečijo dostop do spletnih računalniških storitev.	• Napadi za porazdeljeno zavrnitev storitve se izvajajo z množico računalniških sistemov na internetu, ki jih nadzoruje heker in internetnim storitvam (npr. za e-bančništvo) pošiljajo veliko število navidezno upravičenih storitvenih zahtevkov.
Tveganja glede varnosti IKT	Kibernetski napadi in drugi zunanji napadi na podlagi IKT	Napadi, izvedeni z interneta ali zunanjih omrežij za različne namene (npr. goljufijo, vohunjenje, aktivizem/sabotažo, kibernetski terorizem) z uporabo najrazličnejših pristopov (npr. socialnega inženiringa, poskusov vdora z izkoriščenjem ranljivosti, uporabo zlonamerne programske opreme), s katerimi se prevzame nadzor nad notranjimi sistemi IKT.	Različne vrste napadov: • Organizirana trajna grožnja (APT) prevzema nadzora nad notranjimi sistemi ali kraje informacij (npr. informacij v zvezi s krajo identitete, informacij o kreditnih karticah). • Zlonamerna programska oprema (npr. izsiljevalska programska oprema), ki podatke šifrira z namenom izsiljevanja. • Okužba notranjih sistemov IKT s trojanskimi konji za izvajanje prikritih zlonamernih sistemskih dejavnosti. • Izkoriščanje ranljivosti sistema IKT in/ali (spletnih) aplikacij (npr. SQL-vrinjenje itd.) za pridobivanje dostopa do notranjega sistema IKT.
		Goljufive plačilne transakcije, ki jih izvedejo hekerji, tako da zaobidejo varnostne ukrepe storitev e-bančništva in plačilnih storitev ali vdrejo vanje in/ali napadejo in izkoristijo varnostne ranljivosti notranjih plačilnih sistemov institucije.	• Napadi storitev e-bančništva ali plačilnih storitev z namenom izvajanja nepooblaščenih prenosov. • Ustvarjanje in pošiljanje goljufivih plačilnih transakcij iz notranjih plačilnih sistemov institucije (npr. goljufiva sporočila SWIFT).
		Goljufive transakcije z vrednostnimi papirji, ki jih izvedejo hekerji, tako da zaobidejo varnostne ukrepe storitev e-bančništva, ki zagotavljajo tudi dostop do računov strank za vrednostne papirje, ali vdrejo vanje.	• Napadi z napihovanjem vrednosti in prodajo, v katerih napadalci pridobijo dostop do e-bančnih računov strank za vrednostne papirje ter oddajo goljufiva naročila za kupovanje ali prodajo, da bi vplivali na tržno ceno in/ali se okoristili s predhodnimi pozicijami vrednostnih papirjev.

Kategorije tveganja, povezanega z IKT	Tveganja, povezana z IKT (neizčrpen seznam)[10]	Opis tveganja	Primeri
		Napadi na komunikacijske povezave in pogovore vseh vrst ali sisteme IKT z namenom zbiranja informacij in/ali izvajanja goljufij.	• Prisluškovanje nezaščitenemu prenosu podatkov za overitev v navadnem besedilu ali prestrezanje takega prenosa.
	Neustrezna notranja varnost IKT	Pridobivanje nepooblaščenega dostopa do kritičnih sistemov IKT od znotraj za različne namene (npr. goljufija, izvajanje in prikrivanje dejavnosti prevarantskih trgovcev, kraja podatkov, aktivizem/sabotaža) z različnimi pristopi (npr. zloraba in/ali stopnjevanje privilegijev, kraja identitete, socialni inženiring, izkoriščanje ranljivosti v sistemih IKT, uporaba zlonamerne programske opreme).	• Nameščanje beležnikov tipkanja za krajo uporabniških imen in gesel za pridobivanje nepooblaščenega dostopa do zaupnih podatkov in/ali izvajanje goljufij. • Razbijanje/ugibanje šibkih gesel za pridobivanje nezakonitih ali povečanih dostopnih pravic. • Sistemski skrbnik za goljufijo uporabi operacijske sisteme ali pripomočke zbirk podatkov (za neposredne spremembe zbirk podatkov).
		Nepooblaščene manipulacije IKT zaradi neustreznih procesov in praks upravljanja dostopa do IKT.	• Opustitev onemogočenja ali izbrisa nepotrebnih računov – na primer računov zaposlenih, ki so zamenjali položaj in/ali zapustili institucijo, vključno z gosti ali dobavitelji, ki dostopa ne potrebujejo več – kar omogoča nepooblaščen dostop do sistemov IKT. • Dodeljevanje čezmernih pravic in ugodnosti dostopa, kar dopušča nepooblaščene dostope in/ali omogoča prikrivanje prevarantskih dejavnosti.
		Varnostne grožnje zaradi pomanjkljivega ozaveščanja na področju varnosti, ko zaposleni ne razumejo ali ne upoštevajo varnostnih politik in procesov IKT ali jih zanemarijo.	• Zaposleni, ki so zavedeni v pomoč pri napadu (npr. socialni inženiring). • Slabe prakse glede podatkov za dostop: izmenjava gesel, uporaba gesel, ki jih je preprosto uganiti, uporaba istega gesla za številne različne namene itd. • Shranjevanje nešifriranih zaupnih podatkov na prenosnih računalnikih in prenosnih rešitvah za shranjevanje podatkov (npr. USB-ključih), ki jih je

Kategorije tveganja, povezanega z IKT	Tveganja, povezana z IKT (neizčrpen seznam)[10]	Opis tveganja	Primeri
			mogoče izgubiti ali ukrasti.
		Nepooblaščeno shranjevanje ali prenos zaupnih informacij zunaj institucije.	• Osebe, ki kradejo ali namenoma razkrivajo ali iz institucije tihotapijo zaupne informacije ter jih delijo z nepooblaščenimi osebami ali javnostjo.
	Neustrezna fizična varnost IKT	Zloraba ali kraja sredstev IKT s fizičnim dostopom, ki povzroči škodo, povzroči izgubo sredstev ali podatkov ali omogoči druge nevarnosti.	• Fizičen vlom v pisarne in/ali podatkovne centre, da bi ukradli opremo IKT (npr. namizne računalnike, prenosne računalnike, rešitve za shranjevanje) in/ali prekopirali podatke s fizičnim dostopom do sistemov IKT.
		Namerne ali naključne poškodbe fizičnih sredstev IKT, ki nastanejo zaradi terorizma, nesreč ali nesrečnega/napačnega ravnanja osebja institucije in/ali tretjih oseb (dobaviteljev, serviserjev).	• Fizični terorizem (tj. teroristične bombe) ali sabotaža sredstev IKT. • Uničenje podatkovnega centra zaradi ognja, puščanja vode ali drugih dejavnikov.
		Neustrezna fizična zaščita pred naravnimi nesrečami, zaradi katere se v naravnih nesrečah delno ali popolno uničijo sistemi IKT/podatkovni centri.	• Potresi, izjemna vročina, viharji, snežna neurja, poplave, požar, strele.
Tveganja glede sprememb IKT	Neustrezne kontrole sprememb sistema IKT in razvoja IKT	Incidenti, nastali zaradi neopaženih napak ali ranljivosti, ki so posledica spremembe (npr. nepredvideni učinki spremembe ali slabo upravljana sprememba zaradi pomanjkljivega testiranja ali neustreznih praks upravljanja sprememb), npr. na programski opremi, sistemih IKT in podatkih.	• Sprostitev neustrezno testirane programske opreme ali sprememb konfiguracije v produkcijsko okolje, kar ima nepričakovane škodljive učinke na podatke (npr. okvara, izbris) in/ali delovanje sistema IKT (npr. odpoved, poslabšanje delovanja). • Nenadzorovane spremembe sistemov IKT ali podatkov v produkcijskem okolju. • Sprostitev slabo zavarovanih sistemov IKT in internetnih aplikacij v produkcijsko okolje, kar hekerjem omogoči, da napadejo zagotovljene internetne storitve in/ali prodrejo v notranje sisteme IKT. • Nenadzorovane spremembe izvorne kode notranje razvite programske opreme.

Kategorije tveganja, povezanega z IKT	Tveganja, povezana z IKT (neizčrpen seznam)[10]	Opis tveganja	Primeri
			• Nezadostno testiranje zaradi pomanjkanja testnih okolij.
	Neustrezna arhitektura IKT	Zaradi slabega upravljanja arhitekture IKT pri načrtovanju, vzpostavljanju in vzdrževanju sistemov IKT (npr. programska oprema, strojna oprema, podatki) lahko sčasoma nastanejo zapleteni, zahtevni in neprilagodljivi sistemi IKT, ki so dragi za upravljanje, niso več dovolj usklajeni s poslovnimi potrebami ter ne izpolnjujejo dejanskih zahteve glede upravljanja tveganja.	• Neustrezno upravljanje sprememb sistemov IKT, programske opreme in/ali podatkov v daljšem obdobju, zaradi česar nastanejo zapleteni in heterogeni sistemi in arhitekture IKT, ki jih je težko upravljati, kar ima številne škodljive učinke na poslovanje in upravljanje tveganja (npr. pomanjkljiva prožnost in prilagodljivost, incidenti in okvare IKT, visoki stroški delovanja, oslabela varnost in odpornost IKT, zmanjšana kakovost podatkov in slabše zmogljivosti poročanja). • Prekomerno prilagajanje in širitev paketov tržne programske opreme z notranje razvito programsko opremo, zaradi česar ni mogoče uporabljati poznejših izdaj in nadgradenj tržne programske opreme, obstaja pa tudi tveganje, da je prodajalec ne bo več podpiral.
	Neustrezno upravljanje življenjskega cikla in popravkov	Opustitev vzdrževanja ustreznega popisa vseh sredstev IKT v podporo dobrih praks upravljanja življenjskega cikla in popravkov ter v povezavi z njimi. Zaradi tega nastanejo neustrezno popravljeni (in zato ranljivejši) in zastareli sistemi IKT, ki morda ne podpirajo poslovnih potreb in potreb upravljanja tveganja.	• Nepopravljeni in zastareli sistemi IKT, ki imajo lahko škodljive učinke na poslovanje in upravljanje tveganja (npr. pomanjkljiva prožnost in prilagodljivost, izpadi IKT, oslabela varnost in odpornost IKT).
Tveganja glede celovitosti podatkov IKT	Neuspešna obdelava podatkov IKT ali ravnanje z njimi	Napake ali okvare v sistemu, komuniciranju in/ali aplikacijah ali napačno izveden postopek pridobivanja, prenosa in nalaganja podatkov (ETL) lahko povzroči okvaro ali izgubo podatkov.	• Napaka v računalniškem sistemu pri paketni obdelavi, ki povzroči napačno stanje na bančnih računih strank. • Napačno izvedene poizvedbe. • Izguba podatkov zaradi napake pri podvajanju podatkov (varnostne kopije).

Kategorije tveganja, povezanega z IKT	Tveganja, povezana z IKT (neizčrpen seznam)[10]	Opis tveganja	Primeri
	Slabo zasnovane kontrole potrjevanja podatkov v sistemih IKT	Napake v zvezi z manjkajočimi ali neučinkovitimi kontrolami avtomatiziranega vnosa podatkov in sprejetja (npr. za uporabljene podatke tretjih oseb) ter kontrolami prenosa, obdelave in izpisa podatkov v sistemih IKT (npr. kontrole veljavnosti vnosa, uskladitve podatkov).	• Neustrezno ali neveljavno oblikovanje/potrjevanje vnosov podatkov v aplikacijah in/ali uporabniških vmesnikih. • Pomanjkanje kontrol uskladitve podatkov za pridobljene izpise. • Pomanjkanje kontrol za izvedene postopke pridobivanja podatkov (npr. poizvedbe v zbirkah podatkov), zaradi česar pride do napačnih podatkov. • Uporaba pomanjkljivih zunanjih podatkov.
	Slabo nadzorovane spremembe podatkov v produkcijskih sistemih IKT.	Napake v podatkih zaradi pomanjkanja kontrol pravilnosti in upravičenosti manipulacij podatkov, izvedenih v produkcijskih sistemih IKT.	• Razvijalci ali skrbniki zbirk podatkov na nenadzorovan način neposredno dostopajo do podatkov v produkcijskih sistemih IKT in jih spreminjajo, npr. v primeru incidenta IKT.
	Slabo zasnovana in/ali upravljana podatkovna arhitektura, podatkovni tokovi, podatkovni modeli ali podatkovni slovarji	Zaradi slabo zasnovane in/ali upravljane podatkovne arhitekture, podatkovnih tokov, podatkovnih modelov ali podatkovnih slovarjev lahko nastane več različic istih podatkov v sistemih IKT, ki niso več skladni zaradi različno uporabljenih podatkovnih modelov ali opredelitev podatkov, in/ali razlike v osnovnem procesu proizvajanja in spreminjanja podatkov.	• Obstoj različnih zbirk podatkov strank za posamezen proizvod ali poslovno enoto z različnimi opredelitvami podatkov in podatkovnimi polji, zaradi česar so podatki strank neusklajeni ter jih je težko primerjati in vključiti na ravni celotne finančne institucije ali skupine.
Tveganja glede zunanjega izvajanja IKT	Neustrezna odpornost storitev tretje osebe ali drugega	Kritične storitve IKT, telekomunikacijske storitve in pripomočki, oddani v zunanje izvajanje, niso na razpolago. Izguba ali okvara kritičnih/občutljivih podatkov,	• Temeljne storitve zaradi odpovedi ponudnikovih sistemov IKT ali aplikacij (oddanih v zunanje izvajanje) niso na razpolago. • Motnje telekomunikacijskih povezav.

Kategorije tveganja, povezanega z IKT	Tveganja, povezana z IKT (neizčrpen seznam)[10]	Opis tveganja	Primeri
	subjekta v skupini	zaupanih ponudniku storitve.	• Prekinitev električnega napajanja.
	Neustrezno upravljanje zunanjega izvajanja	Resno poslabšanje ali odpoved storitve zaradi neučinkovite pripravljenosti ali nadzornih postopkov ponudnika storitev, izbranega za zunanje izvajanje. Neučinkovito upravljanje zunanjega izvajanja lahko povzroči pomanjkanje ustreznih veščin in sposobnosti, da bi v celoti opredelili, ocenili, zmanjšali in spremljali tveganja IKT, pa tudi omejitev operativnih zmogljivosti institucij.	• Slabi postopki za obravnavo incidentov, pogodbeni nadzorni mehanizmi in jamstva, vključeni v pogodbo s ponudnikom storitev, ki povečujejo ključno glavno odvisnost od tretjih oseb in prodajalcev. • Neustrezne kontrole upravljanja sprememb, povezane z okoljem IKT ponudnika storitev, lahko povzročijo resno poslabšanje ali odpoved storitve.
	Neustrezna varnost tretje osebe ali drugega subjekta v skupini	Vdor v sisteme IKT tretjih oseb, ki so ponudniki storitev, z neposrednim vplivom na storitve, oddane v zunanje oddajanje, ali kritične/zaupne podatke, shranjene pri ponudniku storitev. Osebje ponudnika storitev pridobi nepooblaščen dostop do kritičnih/zaupnih podatkov, shranjenih pri ponudniku storitev.	• Zločinci ali teroristi vdrejo v sisteme IKT ponudnikov storitev, da bi pridobili dostop do sistemov IKT institucij ali dosegli/uničili kritične ali občutljive podatke, shranjene pri ponudniku storitev. • Zlonamerne osebe znotraj ponudnika storitev skušajo ukrasti in prodati občutljive podatke.