Smernice

EBA/GL/2019/04

28. november 2019

Smernice EBA o upravljanju tveganj, povezanih z IKT in varnostjo

Obveznosti glede skladnosti in poročanja

Vloga teh smernic

1. Ta 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 spoštovanje smernic.

2. V smernicah je navedeno stališče organa EBA o ustreznih nadzornih praksah v okviru Evropskega sistema finančnega nadzora oziroma o tem, kako naj se pravo Evropske unije uporablja na zadevnem področju. Pristojni organi iz člena 4(2) Uredbe (EU) št. 1093/2010, na katere se smernice nanašajo, naj jih upoštevajo tako, da jih ustrezno vključijo v svoje prakse (npr. s spremembo svojega pravnega okvira ali svojih nadzornih postopkov), vključno z določili smernic, ki so namenjene predvsem institucijam.

Zahteve glede poročanja

3. Pristojni organi morajo v skladu s členom 16(3) Uredbe (EU) št. 1093/2010 do ([dd. mm. llll]) organ EBA uradno obvestiti, ali ravnajo ali nameravajo ravnati v skladu s temi smernicami, ali pa navedejo razloge, zakaj jih ne upoštevajo ali jih ne nameravajo upoštevati. Če organ EBA uradnega obvestila pristojnih organov do navedenega roka ne bo prejel, bo štel, da smernic ne upoštevajo. Uradna obvestila je treba poslati na obrazcu, ki je na voljo na spletišču organa EBA, na elektronski naslov compliance@eba.europa.eu z navedbo sklica „EBA/GL/2019/04“. 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 spletišču 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).

Predmet urejanja, področje uporabe in opredelitev pojmov

Predmet urejanja

5. Te smernice temeljijo na določbah člena 74 Direktive 2013/36/EU (CRD) v zvezi z notranjim upravljanjem in izhajajo iz pooblastila za izdajo smernic iz člena 95(3) Direktive (EU) 2015/2366 (PSD2).

6. Te smernice določajo ukrepe za obvladovanje tveganja, ki jih morajo finančne institucije (kot so opredeljene v odstavku 9 v nadaljevanju) sprejeti v skladu s členom 74 CRD za obvladovanje svojih tveganj, povezanih z informacijsko in komunikacijsko tehnologijo (IKT) ter varnostjo, za vse dejavnosti, in ki jih morajo ponudniki plačilnih storitev (kot so opredeljeni v odstavku 9 v nadaljevanju) sprejeti v skladu s členom 95(1) PSD2 za obvladovanje operativnih in varnostnih tveganj (predvidena kot „tveganja, povezana z IKT in varnostjo“), povezanih s plačilnimi storitvami, ki jih opravljajo. Smernice vključujejo zahteve za informacijsko varnost, vključno s kibernetsko varnostjo, če so informacije shranjene v sistemih IKT.

Področje uporabe

7. Te smernice se uporabljajo v zvezi z upravljanjem tveganj, povezanih z IKT in varnostjo, v finančnih institucijah (kot so opredeljene v odstavku 9 v nadaljevanju). Za namene teh smernic izraz „tveganja, povezana z IKT in varnostjo“ pomeni operativna in varnostna tveganja iz člena 95 PSD2 za zagotavljanje plačilnih storitev.

8. Za ponudnike plačilnih storitev (kot so opredeljeni v odstavku 9 v nadaljevanju) se te smernice uporabljajo za njihovo opravljanje plačilnih storitev v skladu s področjem uporabe in pooblastilom iz člena 95 PSD2. Za institucije (kot so opredeljene v odstavku 9 v nadaljevanju) se te smernice uporabljajo za vse dejavnosti, ki jih opravljajo.

Naslovniki

9. Te smernice so namenjene finančnim institucijam, ki za namene teh smernic pomenijo (1) ponudnike plačilnih storitev, kot so opredeljeni v členu 4(11) PSD2, in (2) institucije, tj. kreditne institucije in investicijska podjetja, kot so opredeljeni v točki 3 člena 4(1) Uredbe (EU) št. 575/2013. Namenjene so tudi pristojnim organom, kot so opredeljeni v točki 40 člena 4(1) Uredbe (EU) št. 575/2013, vključno z Evropsko centralno banko v zvezi z zadevami, ki se nanašajo na naloge, prenesene nanjo v skladu z Uredbo (EU) št. 1024/2013, in pristojnim organom v skladu s PSD2, kot so navedeni v členu 4(2)(i) Uredbe (EU) št. 1093/2010.

Opredelitve pojmov

10. Če ni določeno drugače, imajo izrazi v teh smernicah enak pomen kot izrazi, uporabljeni in opredeljeni v Direktivi 2013/36/EU (CRD), Uredbi (EU) št. 575/2013 (CRR) in Direktivi (EU) 2015/2366 (PSD2). Za namene teh smernic se uporabljajo tudi naslednje opredelitve pojmov:

Tveganje, povezano z IKT in varnostjo	Tveganje izgube zaradi kršitve zaupnosti, nezagotavljanja celovitosti sistemov in podatkov, neustreznosti ali nerazpoložljivosti sistemov in podatkov ali nezmožnosti, da se zaradi sprememb okolja ali poslovnih zahtev v razumnem času in z razumnimi stroški spremeni tudi informacijska tehnologija (tj. agilnost)[2]. To vključuje varnostna tveganja, ki so posledica neustreznih ali neuspešnih notranjih procesov ali zunanjih dogodkov, vključno s kibernetskimi napadi ali neustreznim fizičnim varovanjem.
Upravljalni organ	(a) Za kreditne institucije in investicijska podjetja ima ta izraz enak pomen kot opredelitev v točki (7) člena 3(1) Direktive 2013/36/EU. (b) Za plačilne institucije ali institucije za izdajo elektronskega denarja ta izraz pomeni direktorje ali osebe, odgovorne za upravljanje plačilnih institucij in institucij za izdajo elektronskega denarja, ter, kadar je ustrezno, osebe, odgovorne za vodenje poslov plačilnih institucij in institucij za izdajo elektronskega denarja v zvezi s plačilnimi storitvami. (c) Za ponudnike plačilnih storitev iz člena 1(1)(c), (e) in (f) Direktive (EU) 2015/2366 ima ta izraz pomen, ki mu ga dodeljuje zakonodaja EU ali nacionalna zakonodaja, ki se uporablja.
Operativni ali varnostni incident	Enkratni dogodek ali niz povezanih dogodkov, ki jih finančna institucija ne načrtuje in ki ima ali bo verjetno imel negativen učinek na celovitost, razpoložljivost, zaupnost in/ali avtentičnost storitev.
Višje vodstvo	(a) Za kreditne institucije in investicijska podjetja ima ta izraz enak pomen kot opredelitev v točki (9) člena 3(1) Direktive 2013/36/EU. (b) Za plačilne institucije in institucije za izdajo elektronskega denarja ta izraz pomeni fizične osebe, ki v instituciji opravljajo izvršilne funkcije, so pristojne za vsakodnevno upravljanje institucije in v zvezi s tem tudi odgovorne upravljalnemu organu.

[2] Opredelitev iz Smernic organa EBA o skupnih postopkih in metodologijah za proces nadzorniškega pregledovanja in ovrednotenja z dne 19. decembra 2014 (EBA/GL/2014/13), kakor so bile spremenjene s smernicami EBA/GL/2018/03.

	(c) Za ponudnike plačilnih storitev iz člena 1(1)(c), (e) in (f) Direktive (EU) 2015/2366 ima ta izraz pomen, ki mu ga dodeljuje zakonodaja EU ali veljavna nacionalna zakonodaja, ki se uporablja.
Nagnjenost k prevzemanju tveganja	Skupna raven in vrste tveganj, ki so jih ponudniki plačilnih storitev in institucije v skladu s svojim poslovnim modelom pripravljeni prevzeti v okviru svoje sposobnosti prevzemanja tveganj, da dosežejo svoje strateške cilje.
Revizijska funkcija	(a) Za kreditne institucije in investicijska podjetja revizijska funkcija pomeni, kot je navedeno v oddelku 22 Smernic organa EBA o notranjem upravljanju (EBA/GL/2017/11). (b) Pri ponudnikih plačilnih storitev, ki niso kreditne institucije, mora biti revizijska funkcija neodvisna v okviru ponudnika plačilnih storitev ali od ponudnika plačilnih storitev ter je lahko funkcija notranje in/ali zunanje revizije.
Projekti IKT	Kateri koli projekt ali njegov del, pri katerem se sistemi in storitve IKT spremenijo, nadomestijo, opustijo ali vzpostavijo. Projekti IKT so lahko del širših programov IKT ali poslovnega preoblikovanja.
Tretja oseba	Organizacija, ki je s subjektom vzpostavila poslovne odnose ali sklenila pogodbe za zagotavljanje proizvoda ali storitve[3].
Informacijsko sredstvo	Zbirka oprijemljivih ali neoprijemljivih informacij, ki jih je treba zavarovati.
Sredstvo IKT	Sredstvo, ki je lahko programska ali strojna oprema prisotno v poslovnem okolju.
Sistemi IKT[4]	IKT, vključene v mehanizem ali povezovalno omrežje, ki podpirajo delovanje finančne institucije.
Storitve IKT[5]	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 spremljanja in storitve podpore odločanja in poslovanja.

[3] Opredelitev iz dokumenta skupine G7 o temeljnih elementih za obvladovanje kibernetskih tveganj v odnosu do tretjih oseb v finančnem sektorju.
[4] Opredelitev iz Smernic o oceni tveganja, povezanega z IKT, v skladu s procesom nadzorniškega pregledovanja in vrednotenja (SREP) (EBA/GL/2017/05).
[5] Glej prejšnjo opombo.

Izvajanje

Datum začetka uporabe

11. Te smernice se začnejo uporabljati 30. junija 2020.

Razveljavitev

12. S temi smernicami bodo Smernice o varnostnih ukrepih za operativna in varnostna tveganja (EBA/GL/2017/17), izdane leta 2017, razveljavljene na datum začetka uporabe teh smernic.

Smernice o obvladovanju tveganj, povezanih z IKT in varnostjo

1.1. Sorazmernost

1. Vse finančne institucije bi morale zagotavljati skladnost z določbami teh smernic na način, ki je sorazmeren z njihovo velikostjo, in upošteva njihovo notranjo organizacijo ter vrsto, obseg, kompleksnost in tveganost storitev in proizvodov, ki jih zagotavljajo ali nameravajo zagotavljati finančne institucije.

1.2. Ureditev upravljanja in strategija

1.2.1. Ureditev upravljanja

2. Upravljalni organ bi moral zagotoviti, da imajo finančne institucije vzpostavljen ustrezen okvir notranjega upravljanja in notranjih kontrol za tveganja, povezana z IKT in varnostjo. Upravljalni organ bi moral jasno opredeliti vloge in odgovornosti za funkcije IKT, upravljanje tveganja informacijske varnosti in zagotavljanja neprekinjenega poslovanja, vključno z vlogami in odgovornostmi upravljalnega organa in njegovih odborov.
3. Upravljalni organ bi moral zagotoviti dovolj ustrezno usposobljenega osebja v finančnih institucijah, za stalno podporo operativnih potreb na področju IKT, stalnega procesa upravljanja tveganj, povezanih z IKT in varnostjo, ter za zagotavljanje izvajanja njihove strategije IKT. Ob tem bi moral zagotoviti, da je dodeljeni proračun ustrezen za izpolnitev zgoraj navedenega. Poleg tega bi morale finančne institucije zagotoviti, da vsi člani osebja, vključno z nosilci ključnih funkcij, enkrat letno ali po potrebi pogosteje opravijo ustrezno usposabljanje o tveganjih, povezanih z IKT in varnostjo, vključno z informacijsko varnostjo (glej tudi oddelek 1.4.7).

4. Upravljalni organ je v celoti odgovoren za opredelitev, odobritev in nadzor nad izvajanjem strategije IKT finančnih institucij v okviru njihove splošne poslovne strategije ter za vzpostavitev učinkovitega okvira upravljanja tveganj, povezanih z IKT in varnostjo.

1.2.2. Strategija

5. Strategija IKT bi morala biti usklajena s splošno poslovno strategijo finančnih institucij in bi morala opredeljevati:

   a) kako bi se IKT finančnih institucij moral razvijati za učinkovito podporo in udeležbo v njihovi poslovni strategiji, vključno z razvojem organizacijske strukture, spremembami sistema IKT in ključnimi odvisnostmi od tretjih oseb;
   b) načrtovano strategijo in razvoj arhitekture IKT, vključno z odvisnostmi od tretjih oseb;
   c) jasne cilje informacijske varnosti, osredotočene na sisteme, storitve, osebje in procese IKT.

6. Finančne institucije bi morale določiti sklope akcijskih načrtov, ki vsebujejo predvidene ukrepe za doseganje cilja strategije IKT. Z njimi bi moralo biti seznanjeno vse zadevno osebje (tudi pogodbeni izvajalci in tretje osebe v vlogi ponudnikov, kjer so ti vključeni in je to ustrezno). Akcijski načrti bi morali biti redno pregledovani, da se tako zagotovi njihova ustreznost in primernost. Finančne institucije bi morale vzpostaviti tudi postopke za spremljanje in merjenje učinkovitosti izvajanja svoje strategije IKT.

1.2.3. Uporaba tretjih oseb v vlogi ponudnikov

7. Finančne institucije bi morale ne glede na Smernice organa EBA o zunanjem izvajanju (EBA/GL/2019/02) in člen 19 PSD2 zagotoviti učinkovitost ukrepov za zmanjšanje tveganja, kot so opredeljeni v njihovem okviru upravljanja tveganja, vključno z ukrepi iz teh smernic, če operativne funkcije plačilnih storitev ter/ali storitev in sistemov IKT katere koli dejavnosti izvajajo zunanji izvajalci, vključno s subjekti v skupini, ali kadar se uporabljajo tretje osebe.

8. Finančne institucije bi morale, da se zagotovi neprekinjenost zagotavljanja storitev IKT in delovanja sistemov IKT, poskrbeti, da pogodbe in sporazumi o ravni storitev (tako v primeru običajnih razmer kot v primeru motenih storitev – glej tudi oddelek 1.7.2), sklenjenimi s ponudniki (zunanjimi izvajalci, subjekti v skupini ali tretjimi osebami v vlogi ponudnikov), vključujejo:

   a) ustrezne in sorazmerne cilje in ukrepe, povezane z informacijsko varnostjo, vključno z zahtevami, kot so minimalne zahteve glede kibernetske varnosti, specifikacije življenjskega cikla podatkov finančnih institucij, katere koli zahteve glede šifriranja podatkov, varnosti omrežij in procesom varnostne spremljave ter lokacije podatkovnih centrov;
   b) postopke za obravnavo operativnih in varnostnih incidentov, vključno s stopnjevanjem in poročanjem.

9. Finančne institucije bi morale spremljati raven skladnosti teh ponudnikov z varnostnimi cilji, ukrepi in cilji uspešnosti zadevne finančne institucije ter v zvezi s tem pridobiti ustrezna zagotovila.

1.3. Okvir upravljanja tveganj, povezanih z IKT in varnostjo

1.3.1. Organizacija in cilji

10. Finančne institucije bi morale prepoznavati ter upravljati svoja tveganja, povezana z IKT in varnostjo. Funkcija(-e) IKT, odgovorna(-e) za sisteme, procese in varnostne operacije IKT bi morala(-e) imeti vzpostavljene ustrezne procese in kontrole, s katerimi zagotavlja(-jo), da se vsa tveganja prepoznavajo, analizirajo, merijo, spremljajo, upravljajo, sporočajo in ohranjajo v okviru meja nagnjenosti finančne institucije k prevzemanju tveganja ter da so projekti in sistemi, ki jih zagotavljajo, in dejavnosti, ki jih opravljajo, v skladu z zunanjimi in notranjimi zahtevami.

11. Finančne institucije bi morale odgovornost za upravljanje in nadzorovanje tveganj, povezanih z IKT in varnostjo, dodeliti funkciji notranjih kontrol, pri čemer se upoštevajo zahteve iz oddelka 19 Smernic organa EBA o notranjem upravljanju (EBA/GL/2017/11). Poleg tega bi morale zagotoviti neodvisnost in nepristranskost te funkcije notranjih kontrol tako, da jo ustrezno ločijo od procesov operacij IKT. Ta funkcija notranjih kontrol bi morala biti odgovorna neposredno upravljalnemu organu ter pristojna za spremljavo in nadzor nad spoštovanjem okvira upravljanja tveganj, povezanih z IKT in varnostjo. Zagotoviti bi morala, da se tveganja, povezana z IKT in varnostjo, prepoznavajo, merijo, upravljajo, spremljajo in sporočajo. Finančne institucije bi morale zagotoviti, da ta funkcija notranjih kontrol ni odgovorna za nobeno notranjo revizijo.

Funkcija notranje revizije bi morala na podlagi pristopa, ki temelji na oceni tveganj, sposobna opraviti neodvisni pregled in dati nepristransko zagotovilo glede skladnosti vseh dejavnosti, povezanih z IKT in varnostjo, ter enot finančne institucije s politikami in postopki finančne institucije in z zunanjimi zahtevami, pri čemer se upoštevajo zahteve iz oddelka 22 Smernic organa EBA o notranjem upravljanju (EBA/GL/2017/11).

12. Finančne institucije bi morale opredeliti in dodeliti ključne vloge in odgovornosti ter ustrezne linije poročanja za zagotovitev učinkovitega okvira upravljanja tveganj, povezanih z IKT in varnostjo. Ta okvir bi moral biti v celoti vključen in usklajen s splošnim procesom upravljanja tveganj finančnih institucij.

13. Okvir upravljanja tveganj, povezanih z IKT in varnostjo, bi moral vključevati postopke za:

a) določitev nagnjenosti k prevzemanju tveganj, povezanih z IKT in varnostjo, v skladu z nagnjenostjo finančne institucije k prevzemanju tveganja;
b) opredelitev in oceno tveganj, povezanih z IKT in varnostjo, ki jim je izpostavljena finančna institucija;
c) opredelitev ukrepov, vključno s kontrolami, za zmanjšanje tveganj, povezanih z IKT in varnostjo;

d) spremljanje učinkovitosti teh ukrepov in števila prijavljenih incidentov, pri ponudnikih plačilnih storitev vključno s številom prijavljenih incidentov v skladu s členom 96 PSD2, ki vplivajo na dejavnosti, povezane z IKT, ter sprejetje korektivnih ukrepov kjer je to potrebno;
e) poročanje upravljalnemu organu o tveganjih, povezanih z IKT in varnostjo, in kontrolah;
f) prepoznavo in oceno, ali obstajajo tveganja, povezana z IKT in varnostjo, ki so posledica katere koli večje spremembe sistema IKT ali storitev, procesov ali postopkov IKT, in/ali katerega koli pomembnejšega operativnega ali varnostnega incidenta.

14. Finančne institucije bi morale zagotoviti, da je okvir upravljanja tveganj, povezanih z IKT in varnostjo, dokumentiran in da se nenehno izboljšuje na podlagi spoznanj, pridobljenih med njegovim izvajanjem in spremljanjem. Upravljalni organ bi moral okvir upravljanja tveganj, povezanih z IKT in varnostjo, odobriti in pregledati vsaj enkrat letno.

1.3.2. Prepoznava funkcij, procesov in sredstev

15. Finančne institucije bi morale vzpostaviti in vzdrževati posodobljen popis prepoznanih poslovnih funkcij, vlog in podpornih procesov, da lahko prepoznajo njihovo pomembnost ter soodvisnosti, ki se nanašajo na tveganja, povezana z IKT in varnostjo.

16. Poleg tega bi morale finančne institucije prepoznati, vzpostaviti in vzdrževati posodobljen popis prepoznanih informacijskih sredstev, ki podpirajo njihove poslovne funkcije in podporne procese, kot so sistemi IKT, osebje, pogodbeni izvajalci, tretje osebe ter odvisnosti od drugih notranjih in zunanjih sistemov in procesov, da lahko upravljajo vsaj z informacijskimi sredstvi, ki podpirajo njihove kritične poslovne funkcije in procese.

1.3.3. Razvrščanje in ocena tveganja

17. Finančne funkcije bi morale razvrstiti prepoznane poslovne funkcije, podporne procese in informacijska sredstva iz odstavkov 15 in 16 z vidika kritičnosti.

18. Finančne institucije bi morale za opredelitev kritičnosti prepoznanih poslovnih funkcij, podpornih procesov in informacijskih sredstev upoštevati vsaj zahteve glede zaupnosti, celovitosti in razpoložljivosti. Pristojnost in odgovornost za informacijska sredstva bi morala biti jasno opredeljena.

19. Finančne institucije bi morale v okviru ocene tveganja pregledati ustreznost razvrstitve informacijskih sredstev in zadevne dokumentacije.

20. Finančne institucije bi morale prepoznavati tveganja, povezana z IKT in varnostjo, ki vplivajo na prepoznane in razvrščene poslovne funkcije, podporne procese in informacijska sredstva, glede na njihovo kritičnost. Ta ocena tveganja bi morala biti izvedena in dokumentirana vsaj enkrat letno ali po potrebi pogosteje. Tovrstne ocene tveganja bi morale biti opravljene tudi ob vsaki večji spremembi infrastrukture, procesov ali postopkov, ki vplivajo na poslovne funkcije, podporne procese ali informacijska sredstva, posledično pa bi morala biti posodobljena trenutna ocena tveganja finančnih institucij.

21. Finančne institucije bi morale zagotoviti stalno spremljanje groženj in ranljivosti, pomembnih za njihove poslovne procese, podporne funkcije in informacijska sredstva, ter redno pregledovati scenarije tveganja, ki vplivajo nanje.

1.3.4. Obvladovanje tveganja

22. Finančne institucije bi morale na podlagi ocen tveganja določiti, kateri ukrepi so potrebni za obvladovanje prepoznanih tveganj, povezanih z IKT in varnostjo, na sprejemljivo raven, in ali so potrebne spremembe vzpostavljenih poslovnih procesov, kontrolnih ukrepov sistemov in storitev IKT. Finančna institucija bi morala upoštevati čas, potreben za izvedbo teh sprememb, in čas za sprejetje ustreznih začasnih ukrepov za zmanjšanje tveganj, povezanih z IKT in varnostjo, da ostane v okviru nagnjenosti finančne institucije k prevzemanju tveganj, povezanih z IKT in varnostjo.

23. Finančne institucije bi morale opredeliti in izvajati ukrepe za obvladovanje prepoznanih tveganj, povezanih z IKT in varnostjo, ter za varovanje informacijskih sredstev v skladu s svojo razvrstitvijo.

1.3.5. Poročanje

24. Finančne institucije bi morale o rezultatih ocene tveganja jasno in pravočasno poročati upravljalnemu organu. Tovrstno poročanje ne posega v obveznost ponudnikov plačilnih storitev, da pristojnim organom zagotovijo posodobljeno in celovito oceno tveganja v skladu s členom 95(2) Direktive (EU) 2015/2366.

1.3.6. Revizija

25. Ureditev upravljanja finančne institucije, njene sisteme in procese v zvezi s tveganji, povezanimi z IKT in varnostjo, bi morali redno pregledovati usposobljeni revizorji z ustreznim znanjem in izkušnjami s področja IKT in varnostnih tveganj ter plačil (pri ponudnikih plačilnih storitev), da lahko upravljalnemu organu predložijo neodvisno zagotovilo o njihovi učinkovitosti. Revizorji bi morali biti neodvisni v okviru finančne institucije ali od finančne institucije. Pogostost in osredotočenost takih revizij naj bosta sorazmerni z zadevnimi tveganji, povezanimi z IKT in varnostjo.

26. Upravljalni organ finančne institucije bi moral odobriti revizijski načrt, vključno z vsemi revizijami IKT in njihovimi bistvenimi spremembami. Revizijski načrt in njegovo izvajanje, vključno s pogostostjo revizij, bi moral odražati inherentna tveganja, povezana z IKT in varnostjo, v finančni instituciji, biti z njimi sorazmeren in redno posodabljan.

27. Vzpostavljen bi moral biti formalni proces naknadnega pregledovanja vključno z določbami za pravočasno preverjanje in odpravo pomanjkljivosti izhajajočih iz kritičnih IKT revizijskih ugotovitev.

1.4. Informacijska varnost

1.4.1. Politika informacijske varnosti

28. Finančne institucije bi morale pripraviti in dokumentirati politiko informacijske varnosti, v kateri bi morala biti na visoki ravni opredeljena načela in pravila za varstvo zaupnosti, celovitosti in razpoložljivosti podatkov ter informacij finančnih institucij in njihovih strank. Za ponudnike

plačilnih storitev se ta politika opredeli v dokumentu o varnostni strategiji, ki se sprejme v skladu s členom 5(1)(j) Direktive (EU) 2015/2366. Ta politika informacijske varnosti bi morala biti usklajena s cilji informacijske varnosti finančne institucije in temelječa na zadevnih rezultatih procesa ocenjevanja tveganja. To politiko bi moral odobriti upravljalni organ.

29. Politika bi morala vključevati opis glavnih vlog in odgovornosti na področju upravljanja informacijske varnosti, v njej bi morale biti določene zahteve za osebje in pogodbene izvajalce, procese in tehnologijo v zvezi z informacijsko varnostjo, pri čemer se upošteva, da imajo osebje in pogodbeni izvajalci na vseh ravneh odgovornosti pri zagotavljanju informacijske varnosti finančnih institucij. Poleg tega bi politika morala zagotavljati zaupnost, celovitost in razpoložljivost kritičnih logičnih in fizičnih sredstev, virov in občutljivih podatkov v mirovanju, prenosu ali uporabi. S politiko informacijske varnosti bi moralo biti seznanjeno celotno osebje in pogodbeni izvajalci finančne institucije.

30. Finančne institucije bi morale na podlagi politike informacijske varnosti vzpostaviti in izvajati varnostne ukrepe za obvladovanje tveganj, povezanih z IKT in varnostjo, ki so jim izpostavljene. Ti ukrepi bi morali vključevati:

    a) organizacijo in ureditev upravljanja v skladu z odstavkoma 10 in 11;
    b) logično varovanje (oddelek 1.4.2);
    c) fizično varovanje (oddelek 1.4.3);
    d) varnost operacij IKT (oddelek 1.4.4);
    e) spremljanje varnosti (oddelek 1.4.5);
    f) preglede, oceno in testiranje informacijske varnosti (oddelek 1.4.6);
    g) usposabljanje in ozaveščanje o informacijski varnosti (oddelek 1.4.7).

1.4.2. Logično varovanje

31. Finančne institucije bi morale opredeliti, dokumentirati in izvajati postopke logičnih kontrol dostopa (upravljanje identitete in dostopa). Ti postopki bi morali biti vzpostavljeni, izvrševani, spremljani in redno pregledovani. Postopki bi morali vključevati tudi kontrole za odkrivanje nepravilnosti pri spremljanju. Ti postopki bi morali vključevati vsaj naslednje elemente, pri čemer izraz „uporabnik“ vključuje tudi tehnične uporabnike:

    (a) **Potrebo po seznanjenosti, najmanjši obseg pooblastil in razmejitev nalog:** finančne institucije bi morale upravljati s pooblastili za dostop do informacijskih sredstev in njihovih podpornih sistemov na podlagi potrebe po seznanjenosti, vključno z oddaljenim dostopom. Uporabnikom bi moral biti dodeljen najmanjši obseg pooblastil za dostop, ki še omogoča opravljanje njihovih nalog (načelo najmanjšega obsega pooblastil), da se prepreči neupravičen dostop do velikega sklopa podatkov ali, da se prepreči dodelitev kombinacije pooblastil za dostop, ki bi se lahko uporabila za izogibanje kontrolam (načelo razmejitve nalog);

    (b) **Odgovornost uporabnikov:** finančne institucije bi morale čim bolj omejiti uporabo generičnih in skupnih uporabniških računov ter omogočiti, da se lahko prepozna uporabnike, ki so izvedli dejanja v sistemih IKT;

(c) **Pooblastilo privilegiranega dostopa:** finančne institucije bi morale izvajati dosleden nadzor nad privilegiranim dostopom do sistemov, tako da strogo omejijo in skrbno nadzorujejo račune višjim obsegom pooblastil za dostop do sistemov (npr. račune sistemskih skrbnikov). Za zagotovitev varne komunikacije in zmanjšanje tveganja bi oddaljeni skrbniški dostop do ključnih sistemov IKT morali biti odobren samo na podlagi potrebe po seznanjenosti in ob uporabi rešitev z močno avtentikacijo;

(d) **Evidentiranje dejavnosti uporabnikov:** beležene in spremljane bi morale biti vsaj vse dejavnosti uporabnikov z višjim nivojem pooblastil. Dnevniki dostopov bi morali biti zavarovani pred nedovoljenim spreminjanjem in izbrisom, ter hranjeni za obdobje, ki je sorazmerno s kritičnostjo prepoznanih poslovnih funkcij, podpornih procesov in informacijskih sredstev v skladu z oddelkom 1.3.3, brez poseganja v zahteve za hrambo, ki jih določata zakonodaja EU in nacionalna zakonodaja. Finančna institucija bi morala te informacije uporabiti za lažjo prepoznavo in preiskovanje nepravilnosti, ugotovljenih pri zagotavljanju storitev;

(e) **Upravljanje dostopa:** dostopna pooblastila bi morala biti pravočasno dodeljena, preklicana ali spremenjena, v skladu z vnaprej določenimi delovnimi postopki, ki vključujejo poslovnega lastnika informacij, v zvezi s katerimi se ureja dostop (lastnik informacijskih sredstev). Ob prenehanju zaposlitve bi morala biti pooblastila za dostop takoj preklicana;

(f) **Ponovna potrditev dostopa:** pooblastila za dostop bi morala biti redno pregledovana, da se prepreči prekomeren nivo uporabniških pooblastil in, da so uporabniška pooblastila preklicana, ko niso več potrebna;

(g) **Načini avtentikacije:** finančne institucije bi morale izvajati načine avtentikacije, ki so dovolj zanesljive, da lahko učinkovito zagotavljajo skladnost s politikami in postopki kontrol dostopa. Načini avtentikacije bi morali biti sorazmerni s kritičnostjo IKT sistemov, informacij ali procesa, ki je predmet dostopa. To naj vključuje vsaj kompleksna gesla ali načine močnejše avtentikacije (npr. dvofaktorska avtentikacija), ki temeljijo na zadevnem tveganju.

32. Elektronski dostop aplikacij do podatkov in sistemov IKT bi moral biti omejen na najmanjši obseg nujno potreben za opravljanje zadevne storitve.

1.4.3. Fizično varovanje

33. Finančne institucije bi morale opredeliti, dokumentirati in izvajati ukrepe fizičnega varovanja za zaščito svojih prostorov, podatkovnih centrov in občutljivih območij pred nepooblaščenim dostopom in okoljskimi nevarnostmi.

34. Fizični dostop do sistemov IKT bi moral biti dovoljen samo pooblaščenim posameznikom. Pooblastilo bi moralo biti dodeljeno v skladu s posameznikovimi nalogami in odgovornostmi ter omejeno na posameznike, ki so ustrezno usposobljeni in nadzorovani. Fizični dostop bi moral biti redno pregledovan, da se zagotovi preklic pooblastila za dostop takoj, ko to ni več potrebno.

35. Ustrezni ukrepi za zaščito pred okoljskimi nevarnostmi naj bodo sorazmerni s pomenom stavb in kritičnostjo operacij ali sistemov IKT v teh stavbah.

1.4.4. Varnost operacij IKT

36. Finančne institucije bi morale izvajati postopke, s katerimi se preprečijo varnostne težave v sistemih in storitvah IKT, ter čim bolj zmanjšajo njihov vpliv na zagotavljanje storitev IKT. Ti postopki bi morali vključevati naslednje ukrepe:

    a) prepoznavo morebitnih ranljivosti, ki bi morale biti ovrednotene in odpravljene z zagotavljanjem posodobljene programske in strojne opreme, vključno s programsko opremo, ki jo finančne institucije zagotavljajo svojim notranjim in zunanjim uporabnikom, ter z nameščanjem kritičnih varnostnih popravkov ali vzpostavitvijo nadomestnih kontrol;
    b) vzpostavitev varnih osnovnih konfiguracij za vse omrežne komponente;
    c) vzpostavitev segmentacije omrežja, sistemov za preprečitev izgube podatkov in šifriranja omrežnega prometa (v skladu z razvrstitvijo podatkov);
    d) vzpostavitev zaščite končnih točk, vključno s strežniki, delovnimi postajami in mobilnimi napravami; finančne institucije bi morale preveriti, ali končne točke izpolnjujejo standarde, ki so jih opredelile, preden jim odobrijo dostop do svojega omrežja;
    e) zagotavljanje razpoložljivosti mehanizmov za preverjanje celovitosti programske in strojne opreme ter podatkov;
    f) šifriranje podatkov v mirovanju in v prenosu (v skladu z razvrstitvijo podatkov).

37. Poleg tega bi morale finančne institucije redno ugotavljati, ali spremembe v obstoječem operativnem okolju vplivajo na vzpostavljene varnostne ukrepe in ali zahtevajo sprejetje dodatnih ukrepov za obvladovanje povezanih tveganj. Te spremembe bi morale biti del njihovega formalnega postopka za upravljanje sprememb in bi morale zagotavljati ustrezno načrtovanje, testiranje, dokumentiranje, odobritev in uvedbo sprememb.

1.4.5. Stalno spremljanje varnosti

38. Finančne institucije bi morale vzpostaviti in izvajati politike in postopke za odkrivanje nepravilnosti, ki lahko vplivajo na informacijsko varnost finančnih institucij, ter se na take dogodke ustrezno odzivati. Kot del stalnega spremljanja bi morale finančne institucije vzpostaviti ustrezne in učinkovite zmogljivosti za odkrivanje in poročanje o fizičnih ali logičnih vdorih ter kršitvah zaupnosti, celovitosti in razpoložljivosti informacijskih sredstev. Postopki stalnega spremljanja in proces zaznave bi morali pokrivati:

    a) ustrezne notranje in zunanje dejavnike, vključno s poslovnimi funkcijami in upravnimi funkcijami IKT;
    b) transakcije za odkrivanje zlorabe dostopa s strani tretjih oseb ali drugih subjektov in notranje zlorabe dostopa;
    c) morebitne notranje in zunanje grožnje.

39. Finančne institucije bi morale vzpostaviti in izvajati procese ter organizacijske strukture za prepoznavo in stalno spremljanje varnostnih groženj, ki bi lahko pomembno vplivale na njihovo zmožnost zagotavljanja storitev. Finančne institucije bi morale, za primerno zavedanje varnostnih tveganj, aktivno spremljati tehnološki razvoj. Finančne institucije bi

morale uvesti primerne ukrepe za odkrivanje, na primer za prepoznavo morebitnega uhajanja informacij, zlonamerne programske kode in drugih varnostnih groženj, javno znanih ranljivosti programske in strojne opreme ter preverjati razpoložljivost novih varnostnih posodobitev.

40. Spremljanje varnosti bi moralo finančni instituciji tudi pomagati razumeti naravo operativnih ali varnostnih incidentov za ugotavljanje trendov in zagotavljanje podpore organizaciji pri preiskavah.

1.4.6. Pregledi, ocena in testiranje informacijske varnosti

41. Finančne institucije bi morale izvajati raznovrstne preglede, ocene in teste informacijske varnosti za zagotavljanje učinkovite prepoznave ranljivosti v svojih sistemih in storitvah IKT. Opravijo lahko na primer analizo vrzeli glede na standarde informacijske varnosti, preglede skladnosti, notranje in zunanje revizije informacijskih sistemov ali preglede fizične varnosti. Institucija bi morala upoštevati tudi dobro prakso, kot so pregled izvorni kode, ocene ranljivosti, penetracijska testiranja in izvedbe vaj z rdečo ekipo[6].

42. Finančne institucije bi morale vzpostaviti in uvesti okvir za testiranje informacijske varnosti, ki potrjuje robustnost in učinkovitost svojih ukrepov za informacijsko varnost, ter zagotavlja upoštevanje groženj in ranljivosti, prepoznanih na podlagi stalnega spremljanja groženj ter proces ocenjevanja tveganj, povezanih z IKT in varnostjo.

43. Okvir testiranja informacijske varnosti bi moral zagotavljati, da testiranja:

    a) opravijo neodvisni usposobljeni preizkuševalci z ustreznim znanjem in izkušnjami pri testiranju ukrepov na področju informacijske varnosti, ob tem pa niso vključeni v pripravo teh ukrepov;
    b) vključujejo preglede ranljivosti in penetracijska testiranja (vključno s penetracijskim testiranjem na podlagi analize groženj[7], kjer je potrebno in primerno), sorazmerna z stopnjo tveganja, prepoznano pri poslovnih procesih in sistemih.

44. Finančne institucije bi morala izvajati stalna in ponavljajoča se testiranja varnostnih ukrepov. Ta testiranja bi se morala za vse ključne sisteme IKT (odstavek 17) opraviti vsaj enkrat letno, za ponudnike plačilnih storitev pa bi morali biti del celovite ocene varnostnih tveganj, povezanih s plačilnimi storitvami, ki jih opravljajo, v skladu s členom 95(2) PSD2. Nekritični sistemi bi morali biti na podlagi pristopa, ki temelji na oceni tveganj, redno testirani, najmanj pa na vsaka tri leta.

45. Finančne institucije bi morale zagotoviti, da se testiranja varnostnih ukrepov opravijo pri spremembah infrastrukture, procesov ali postopkov in pri izvedbi sprememb zaradi večjih operativnih ali varnostnih incidentov ali zaradi izdaje novih ali pomembno spremenjenih kritičnih aplikacij, dostopnih preko interneta.

[6] angl. red team exercises (ethical hacking)
[7] angl. threat-led penetration testing (TLPT)

46. Finančne institucije bi morale stalno spremljati in vrednotiti rezultate varnostnih testiranj ter pri kritičnih sistemih IKT ustrezno in brez nepotrebnega odlašanja posodobiti svoje varnostne ukrepe.

47. Za ponudnike plačilnih storitev bi moral okvir testiranja vključevati tudi varnostne ukrepe za (1) plačilne terminale in naprave, ki se uporabljajo za opravljanje plačilnih storitev, (2) plačilne terminale in naprave, ki se uporabljajo za avtentikacijo uporabnikov plačilnih storitev, ter (3) naprave in programsko opremo, ki jih ponudnik plačilnih storitev zagotovi uporabniku plačilnih storitev zaradi generiranja/prejema avtentikacijske kode.

48. Na podlagi zaznanih varnostnih groženj in izvedenih sprememb bi se pri izvedbi testiranja moralo vključiti scenarije morebitnih napadov, ki vključujejo relevantne in znane potencialne napade.

1.4.7. Usposabljanje in ozaveščanje o informacijski varnosti

49. Finančne institucije bi morale določiti program usposabljanja, vključno z rednimi programi ozaveščanja o varnosti, za vse osebje in izvajalce za zagotovitev njihove usposobljenosti za opravljanje nalog in odgovornosti v skladu z zadevnimi varnostnimi politikami in postopki za zmanjšanje človeških napak, kraj, goljufij, zlorab ali izgub ter za obravnavanje tveganj, povezanih z informacijsko varnostjo. Zagotoviti bi morale tudi, da programi usposabljanja zagotavljajo usposabljanje za vse člane osebja in pogodbene izvajalce vsaj enkrat letno.

1.5. Upravljanje operacij IKT

50. Finančne institucije bi morale upravljati operacije IKT na podlagi dokumentiranih in vzpostavljenih procesov in postopkov (ki pri ponudnikih plačilnih storitev vključujejo dokument o varnostni strategiji v skladu s členom 5(1)(j) PSD2), ki jih odobri upravljalni organ. Ta sklop dokumentov bi moral opredeliti, kako finančne institucije upravljajo, spremljajo in nadzorujejo svoje sisteme in storitve IKT, vključno z dokumentiranjem kritičnih operacij IKT, ter bi moral finančnim institucijam omogočati vzdrževanje posodobljenega inventarja sredstev IKT..

51. Finančne institucije bi morale zagotoviti, da je zmogljivost njihovih operacij IKT usklajena z njihovimi poslovnimi zahtevami. Finančne institucije bi morale vzdrževati in, kjer je to mogoče, izboljševati učinkovitost svojih operacij IKT, kar vključuje, vendar ni omejeno na, proučevanje možnosti za zmanjšanje morebitnih napak, ki izhajajo iz ročne izvedbe nalog.

52. Finančne institucije bi morale izvajati postopke evidentiranja in spremljanja kritičnih operacij IKT za zagotovitev možnosti zaznave, analize in odprave napak.

53. Finančne institucije bi morale vzdrževati posodobljen inventar sredstev IKT (vključno s sistemi IKT, omrežnimi napravami, podatkovnimi zbirkami itd.). V inventarju sredstev IKT bi se morala hraniti konfiguracija sredstev IKT ter povezave in soodvisnosti med različnimi sredstvi IKT, da se omogočita ustrezna konfiguracija in upravljanje sprememb.

54. Inventar sredstev IKT bi moral biti dovolj podroben, da omogoča takojšnjo prepoznavo sredstva IKT, njegove lokacije, varnostne razvrstitve in lastništva. Soodvisnosti med sredstvi bi morale

biti dokumentirane za pomoč pri odzivu na varnostne in operativne incidente, vključno s kibernetskimi napadi.

55. Finančne institucije bi morale spremljati in upravljati življenjski cikel sredstev IKT za zagotovitev, da ta še naprej izpolnjujejo in podpirajo poslovne zahteve in zahteve v zvezi z upravljanjem tveganj. Finančne institucije bi morale stalno spremljati ali so njihova IKT sredstva podprta s strani njihovih zunanjih ali notranjih dobaviteljev in razvijalcev ter ali so na podlagi dokumentiranih postopkov nameščeni vsi ustrezni popravki in posodobitve. Tveganja, ki izhajajo iz zastarelih ali nepodprtih sredstev IKT, bi morala biti ocenjena in obvladovana.

56. Finančne institucije bi morale uvesti proces načrtovanja zmogljivosti in kapacitet ter njihovega spremljanja, da lahko pravočasno preprečijo ter zaznajo in se odzovejo na težave povezane z nezadostno zmogljivostjo sistemov IKT in primanjkljajem kapacitet IKT.

57. Finančne institucije bi morale opredeliti in izvajati postopke za varnostno kopiranje podatkov in sistemov IKT ter postopke za obnovo podatkov, da se v primeru potreb zagotovi zmožnost njihove povrnitve. Obseg in pogostost varnostnega kopiranja bi morala biti določena v skladu z zahtevami za okrevanje poslovanja ter kritičnostjo podatkov in sistemov IKT, ovrednotena pa bi morala v skladu z izvedeno oceno tveganj. Postopki varnostnega kopiranja in obnove podatkov bi se morali redno testirati.

58. Finančne institucije bi morale zagotoviti, da se varnostne kopije podatkov in sistemov IKT varno hranijo ter da so dovolj oddaljene od primarne lokacije, da niso izpostavljene istim tveganjem.

1.5.1 Upravljanje incidentov in problemov IKT

59. Finančne institucije bi morale vzpostaviti in izvajati proces upravljanja incidentov in problemov, ki finančni instituciji omogoča za stalno spremljanje ter evidentiranje operativnih in varnostnih IKT incidentov ter za pravočasno nadaljevanje s poslovanjem in ponovno vzpostavitev kritičnih poslovnih funkcij in procesov, po nastopu motenj v poslovanju. Finančne institucije bi morale določiti ustrezna merila in pragove za razvrstitev dogodkov med operativne ali varnostne incidente v skladu z oddelkom „Opredelitve pojmov“ teh smernic ter zgodnje opozorilne znake, ki bi se morali uporabljati kot opozorila, ki omogočajo zgodnje odkrivanje teh incidentov. Taka merila in pragovi za ponudnike plačilnih storitev ne posegajo v razvrstitev večjih incidentov v skladu s členom 96 PSD2 in Smernicami o poročanju o večjih incidentih v skladu s PSD2 (EBA/GL/2017/10).

60. Finančne institucije bi morale za zmanjšanje učinka neželenih dogodkov in zagotovitev pravočasnega okrevanja, vzpostaviti ustrezne procese in organizacijske strukture za dosledno in celostno spremljanje, obravnavanje in nadaljnje spremljanje operativnih in varnostnih incidentov, ob tem pa poskrbeti še, da so temeljni vzroki prepoznani in odpravljeni, da se preprečijo ponovitve incidentov. Postopek upravljanja incidentov in odpravljanja težav bi moral določati:

    a) postopke za prepoznavo, spremljanje, evidentiranje in prednostno razvrščanje incidentov na podlagi kritičnosti za poslovanje;

b) vloge in odgovornosti za različne scenarije incidentov (npr. napake, nepravilno delovanje, kibernetski napadi);
c) postopke upravljanja problemov za prepoznavo, analizo in reševanje temeljnih vzrokov v ozadju enega ali več incidentov – finančna institucija bi morala analizirati operativne ali varnostne incidente, za katere je verjetno, da bodo nanjo vplivali in so bili prepoznani ali so se zgodili v organizaciji in/ali zunaj nje, ter prouči ključna spoznanja, pridobljena na podlagi teh analiz, in ustrezno posodobi varnostne ukrepe;
d) učinkovite načrte notranje komunikacije, vključno s postopkoma za priglasitev incidentov in stopnjevanje, kar vključuje tudi pritožbe strank v zvezi z varnostjo, za zagotovitev, da:
    i) se o incidentih z morebitnim velikim neželenim učinkom na ključne sisteme in storitve IKT poroča pristojnemu višjemu vodstvu in višjemu vodstvu za IKT,
    ii) se upravljalni organ pri pomembnih incidentih na ad hoc podlagi obvesti vsaj o vplivu, odzivu in dodatnih kontrolah, opredeljenih zaradi incidentov;
e) postopke odziva na incidente, da se zmanjšajo učinki incidentov in se zagotovi, da pravočasno in varno ponovno operativnost storitev;
f) specifične načrte zunanje komunikacije za kritične poslovne funkcije in procese z namenom:
    i) sodelovanje z relevantnimi deležniki za učinkovit odziv in okrevanje po incidentu,
    ii) ustrezno pravočasno obveščanje zunanjih deležnikov (npr. strank, drugih tržnih udeležencev, nadzornega organa), ki upošteva veljavno regulativo.

1.6. Upravljanje projektov in sprememb IKT

1.6.1. Upravljanje projektov IKT

61. Finančna institucija bi morala izvajati program in/ali proces upravljanja projektov, ki opredeljuje vloge, odgovornosti in pristojnosti za učinkovito podporo izvajanju strategije IKT.

62. Finančna institucija bi morala ustrezno spremljati in obvladovati tveganja, ki izhajajo iz portfelja projektov IKT (upravljanje programov), pri čemer bi morala upoštevati tudi tveganja, ki lahko izhajajo iz soodvisnosti med različnimi projekti in odvisnosti več projektov od istih virov in/ali strokovnega znanja.

63. Finančna institucija bi morala vzpostaviti in izvajati politiko upravljanja projektov, ki vključuje vsaj:

a) projektne cilje;
b) vloge in odgovornosti;
c) oceno projektnega tveganja;
d) načrt, časovni okvir in korake projekta;
e) ključne mejnike;
f) zahteve v zvezi z upravljanjem sprememb.

64. Politika upravljanja projektov IKT bi morala zagotavljati, da informacijsko varnostne zahteve analizira in odobri funkcija, ki je neodvisna od razvojne funkcije.

65. Finančna institucija bi morala zagotoviti, da so v projektni skupini zastopana vsa področja, na katera vpliva projekt IKT, ter da ima projektna skupina znanje, potrebno za zagotovitev varne in uspešne izvedbe projekta.

66. O določitvi in izvajanju projektov IKT ter z njimi povezanimi tveganji bi moralo biti poročano upravljalnemu organu posamično ali skupno, glede na pomembnost in velikost projektov IKT, ter v odvisnosti od relevantnih okoliščin ali redno ali na ad hoc podlagi. Finančne institucije bi morale projektno tveganje vključevati v svoj okvir upravljanja tveganj.

1.6.2. Nakup in razvoj sistemov IKT

67. Finančne institucije bi morale razviti in uvesti proces vodenja nakupa, razvoja in vzdrževanja sistemov IKT. Ta postopek bi moral biti oblikovan na podlagi pristopa, ki temelji na oceni tveganj.

68. Finančna institucija bi morala zagotoviti, da so pred nakupom ali razvojem sistemov IKT jasno opredeljene funkcionalne in nefunkcionalne zahteve (vključno z zahtevami glede informacijske varnosti) ter da jih odobri pristojno poslovodstvo.

69. Finančna institucija bi morala zagotoviti, da so vzpostavljeni ukrepi za obvladovanje tveganja nenamernih sprememb ali namerne zlorabe sistemov IKT med razvojem in uvedbo v produkcijsko okolje.

70. Finančne institucije bi morale imeti vzpostavljeno metodologijo za testiranje in odobritev sistemov IKT pred njihovo prvo uporabo. Ta metodologija naj upošteva kritičnost poslovnih procesov in sredstev. S testiranjem naj se zagotovi, da novi sistemi IKT delujejo, kot je bilo predvideno. Uporabljena bi morala biti testna okolja, ki primerno odslikavajo produkcijsko okolje.

71. Finančne institucije bi morale testirati sisteme IKT, storitve IKT in ukrepe za informacijsko varnost z namenom prepoznave morebitnih varnostnih pomanjkljivosti, kršitev in incidentov.

72. Finančna institucija bi morala vzpostaviti ločena okolja IKT za zagotovitev ustrezne razmejitve nalog in zmanjšanje vpliva nepreverjenih sprememb na produkcijske sisteme. Pri tem bi morala zlasti zagotoviti razmejitev produkcijskega okolja od razvojnega, testnega in drugih neprodukcijskih okolij. Zagotovi bi morala tudi celovitost in zaupnost produkcijskih podatkov v neprodukcijskih okoljih. Dostop do produkcijskih podatkov mora biti omejen na pooblaščene uporabnike.

73. Finančne institucije bi morale izvajati ukrepe za zaščito celovitosti izvorne kode sistemov IKT, ki jih razvijajo samostojno. Poleg tega bi morale izčrpno dokumentirati razvoj, vpeljavo, upravljanje in/ali konfiguracijo sistemov IKT, da zmanjšajo nepotrebno odvisnost od področnih strokovnjakov. Dokumentacija sistema IKT bi morala, kjer je to primerno, vsebovati vsaj uporabniško dokumentacijo, tehnično dokumentacijo sistema in operativne postopke.

74. Postopki finančne institucije za nakup in razvoj sistemov IKT bi morali biti uporabljeni tudi za sisteme IKT, ki jih razvijejo ali upravljajo končni uporabniki poslovne funkcije zunaj organizacije IKT (npr. za računalniške aplikacije končnih uporabnikov), in sicer na podlagi pristopa, ki temelji na oceni tveganja. Finančna institucija bi morala voditi register takšnih aplikacij, ki podpirajo kritične poslovne funkcije ali procese.

1.6.3. Upravljanje sprememb IKT

75. Finančne institucije bi morale vzpostaviti in izvajati postopek upravljanja sprememb IKT in s tem zagotoviti, da se vse spremembe sistemov IKT nadzorovano evidentirajo, testirajo, ocenjujejo, odobrijo, uvedejo in preverijo. Finančne institucije bi morale zagotoviti, da spremembe v izrednih razmerah (tj. spremembe, ki jih je treba uvesti čim prej) sledijo postopkom, ki zagotavljajo ustrezne zaščitne ukrepe.

76. Finančne institucije bi morale določiti, ali spremembe v obstoječem operativnem okolju vplivajo na vzpostavljene varnostne ukrepe in ali je potrebno zaradi njih sprejeti dodatne ukrepe za obvladovanje prisotnih tveganj. Te spremembe bi morale biti bodo skladne s formalnim postopkom upravljanja sprememb v finančnih institucijah.

1.7. Upravljanje neprekinjenega poslovanja

77. Finančne institucije bi morale vzpostaviti trden proces upravljanja neprekinjenega poslovanja, s čimer bi maksimalno povečale zmožnost zagotavljanja neprekinjenega poslovanja in omejile izgubo v primeru resne motnje poslovanja v skladu s členom 85(2) Direktive 2013/36/EU in naslovom VI Smernic organa EBA o notranjem upravljanju (EBA/GL/2017/11).

1.7.1. Analiza vpliva na poslovanje

78. Finančne institucije bi morale v okviru trdnega upravljanja neprekinjenega poslovanja izvesti analizo vpliva na poslovanje[8] preko analize svoje izpostavljenosti resnim motnjam v poslovanju ter kvantitativno in kvalitativno oceno njihovih morebitnih vplivov (vključno z vplivom na zaupnost, celovitost in razpoložljivost) na podlagi notranjih in/ali zunanjih podatkov (npr. podatkov tretjih oseb v vlogi ponudnikov, pomembnih za poslovni proces, ali javno dostopnih podatkov, ki so lahko pomembni za analizo vpliva na poslovanje) in analizo scenarijev. Analiza vpliva na poslovanje bi morala upoštevati tudi kritičnost opredeljenih in razvrščenih poslovnih funkcij, podpornih procesov, tretjih oseb v vlogi ponudnikov, in informacijskih sredstev ter njihove soodvisnosti v skladu z oddelkom 1.3.3.

79. Finančne institucije bi morale zagotoviti, da so njihovi sistemi in storitve IKT zasnovani in usklajeni z analizo vpliva na poslovanje, npr. ob upoštevanju redundance nekaterih kritičnih komponent za preprečitev motenj, ki bi jih povzročili dogodki v katerih bi bile prizadete navedene komponente.

[8] angl. business impact analysis (BIA)

1.7.2. Načrtovanje neprekinjenega poslovanja

80. Finančne institucije bi morale na podlagi analize vpliva na poslovanje (BIA) pripraviti načrte za zagotovitev neprekinjenega poslovanja (načrti neprekinjenega poslovanja, BCP), ki bi morali biti dokumentirani in odobreni s strani njihovih upravljalnih organov. Načrti bi morali upoštevati zlasti tveganja, ki bi lahko pomenila neželen vpliv na sisteme in storitve IKT. Načrti bi morali podpirati cilje pri zaščiti in, kjer je to potrebno, ponovne vzpostavitve zaupnosti, celovitosti in razpoložljivosti poslovnih funkcij, podpornih procesov in informacijskih sredstev. Finančne institucije bi se morale pri pripravi teh načrtov ustrezno uskladiti z notranjimi in zunanjimi deležniki.

81. Finančne institucije bi morale oblikovati načrte neprekinjenega poslovanja s katerimi lahko zagotovijo ustrezen odziv v primerih morebitnih izpadov in motenj poslovanja ter zmožnost okrevanja ključnih poslovnih aktivnosti skladno s ciljnim časom okrevanja[9] (maksimalni čas v katerem mora sistem ali proces okrevati po incidentu) in ciljnim stanjem okrevanja [10] (maksimalni obseg časa v katerem je ob incidentu sprejemljiva izguba podatkov). V primerih resnih motenj poslovanja, ki sprožijo izvajanje posebnih načrtov neprekinjenega poslovanja, bi morale finančne inštitucije določiti vrstni red izvajanja ukrepov za ponovno vzpostavitev poslovanja na osnovi ocene tveganj, ki lahko temelji na ocenah tveganj iz oddelka 1.3.3. Pri ponudnikih plačilnih storitev to lahko na primer vključuje prednostno vzpostavitev obdelave kritičnih transakcij ob hkratnem izvajanju drugih ukrepov za ponovno vzpostavitev poslovanja.

82. Finančna institucija bi morala v načrtu neprekinjenega poslovanja upoštevati različne scenarije, ki jim je lahko izpostavljena, tudi skrajne, a možne, vključno s scenarijem kibernetskega napada, ter oceniti morebitni vpliv, ki ga lahko imajo taki scenariji. Na podlagi teh scenarijev bi finančna inštitucija morala opisati, kako zagotavlja neprekinjenost delovanja sistemov in storitev IKT ter informacijsko varnost.

1.7.3. Načrti odziva in okrevanja

83. Finančne institucije bi morale na podlagi analize vpliva na poslovanje (odstavek 78) in možnih scenarijev (odstavek 82) razviti načrte odziva in okrevanja. Ti načrti bi morali določati kateri pogoji lahko sprožijo aktivacijo teh načrtov in kateri ukrepi bi morali biti sprejeti za zagotovitev razpoložljivosti, neprekinjenosti in okrevanja vsaj njihovih kritičnih sistemov in storitev IKT.. Načrti odziva in okrevanja poslovanja bi morali dosegati cilje okrevanja poslovanja finančnih institucij.

84. V načrtih odziva in okrevanja bi se morale upoštevati možnosti kratkoročnega in dolgoročnega okrevanja. Načrti bi morali biti:

    a) osredotočeni na okrevanje delovanja ključnih poslovnih funkcij, podpornih procesov, informacijskih sredstev in njihovih soodvisnosti za preprečitev neželenih učinkov na delovanje finančnih institucij in na finančni sistem, vključujoč plačilne sisteme in

[9] angl. recovery time objective (RTO)
[10] angl. recovery point objective (RPO)

uporabnike plačilnih storitev, ter na zagotavljanje izvedbe še neobdelanih plačilnih transakcij;

b) dokumentirani in razpoložljivi poslovnim in podpornim enotam ter lahko dostopni v nujnem primeru;

c) posodobljeni v skladu s spoznanji, pridobljenimi iz incidentov in testiranj, novo prepoznanimi tveganji in grožnjami ter spremenjenimi cilji okrevanja in prioritetami.

85. V načrtih bi morale biti upoštevane tudi alternativne možnosti, kadar okrevanje morda kratkoročno ni izvedljivo zaradi stroškov, tveganj, logistike ali nepredvidenih okoliščin.

86. Poleg tega bi morala finančna institucija v okviru načrtov odziva in okrevanja upoštevati in izvajati ukrepe za neprekinjenost poslovanja za obvladovanje izpada delovanja tistih tretjih oseb v vlogi ponudnikov, ki so ključni za neprekinjenost njenih storitev IKT (v skladu z določbami Smernic EBA o zunanjem izvajanju (EBA/GL/2019/02) glede načrtov neprekinjenega poslovanja).

1.7.4. Testiranje načrtov

87. Finančne institucije bi morale redno testirati načrte neprekinjenega poslovanja. Zlasti bi morale zagotoviti, da se načrti neprekinjenega poslovanja njihovih kritičnih poslovnih funkcij, podpornih procesov, informacijskih sredstev in njihovih soodvisnosti (vključno s tistimi, ki jih zagotavljajo tretji ponudniki, kjer je to primerno) vsaj enkrat letno testirajo v skladu z odstavkom 89.

88. Načrti neprekinjenega poslovanja bi se morali posodabljati vsaj enkrat letno na podlagi rezultatov testiranj, podatkov o aktualnih grožnjah in spoznanj, pridobljenih iz predhodnih dogodkov. Morebitne spremembe ciljev okrevanja (vključno s ciljnim časom okrevanja in ciljnim stanjem okrevanja) ter/ali spremembe poslovnih funkcij, podpornih procesov in informacijskih sredstev, bi se morale, kjer je relevantno, upoštevati kot podlaga za posodobitev načrtov neprekinjenega poslovanja.

89. Finančne institucije bi morale s testiranjem svojih načrtov neprekinjenega poslovanja dokazati, da lahko zagotavljajo pogoje za svoj obstoj do ponovne vzpostavitve kritičnih dejavnosti. Zlasti bi morale:

a) vključiti testiranje ustreznega sklopa resnih, vendar možnih scenarijev, vključno s scenariji, ki so bili upoštevani pri razvoju načrtov neprekinjenega poslovanja (vključno s testiranjem storitev tretjih oseb v vlogi ponudnikov); to naj vključuje prenos ključnih poslovnih funkcij, podpornih procesov in informacijskih sredstev v okolje za okrevanje po katastrofi s katerim lahko dokažejo zmožnost delovanja v dovolj dolgem časovnem obdobju, da je to reprezentativno, in da se nato lahko ponovno vzpostavi običajno delovanje;

b) teste zasnovati tako, da se preverijo predpostavke, na katerih temeljijo načrti neprekinjenega poslovanja, vključno z ureditvami upravljanja in načrti kriznega komuniciranja; ter

c) vključevati postopke za preverjanje zmožnosti njihovega osebja in pogodbenih izvajalcev, sistemov in storitev IKT za ustrezno odzivanje na scenarije iz odstavka 89(a).

90. Rezultati testiranj bi morali biti dokumentirani, vsaka pomanjkljivost, prepoznana na podlagi testov, pa bi se morala analizirati, obravnavati in poročati upravljalnemu organu.

1.7.5. Krizno komuniciranje

91. Finančne institucije bi morale v primeru motnje poslovanja, v nujnih primerih in med izvajanjem načrtov neprekinjenosti poslovanja zagotoviti, da imajo vzpostavljene učinkovite ukrepe kriznega komuniciranja za primerno in pravočasno obveščanje vseh zadevnih notranjih in zunanjih deležnikov, vključno s pristojnimi organi, če se to zahteva v skladu z nacionalnimi predpisi, in relevantnimi ponudniki (zunanjimi izvajalci, osebe znotraj skupine ali tretje osebe, ki nastopajo kot ponudniki storitev).

1.8. Upravljanje odnosov z uporabniki plačilnih storitev

92. Ponudniki plačilnih storitev bi morali vzpostaviti in izvajati postopke za boljšo ozaveščenost uporabnikov plačilnih storitev o varnostnih tveganjih, povezanih s plačilnimi storitvami, in sicer z usmerjanjem in zagotavljanjem pomoči.

93. Pomoč in svetovanje, ki je na voljo uporabnikom plačilnih storitev, bi moralo biti posodabljano glede na nove grožnje in ranljivosti, o spremembah pa bi uporabnike plačilnih storitev bilo potrebno obvestiti.

94. Ponudniki plačilnih storitev bi morali, če to dopušča funkcionalnost produkta, uporabnikom plačilnih storitev dovoliti, da onemogočijo določene plačilne funkcionalnosti, ki jih ponudnik plačilnih storitev zagotavlja uporabniku plačilnih storitev.

95. Če se je ponudnik plačilnih storitev v skladu s členom 68(1) Direktive (EU) 2015/2366 s plačnikom dogovoril o omejitvah porabe za plačilne transakcije, izvedene prek določenih plačilnih instrumentov, bi moral ponudnik plačilnih storitev plačniku zagotoviti možnost, da prilagodi te omejitve do najvišje dogovorjene meje.

96. Ponudniki plačilnih storitev bi morali uporabnikom plačilnih storitev zagotoviti možnost, da prejmejo opozorilo o začetih in/ali neuspelih poskusih izvedbe plačilnih transakcij ter jim s tem omogočijo, da lahko zaznajo goljufivo ali zlonamerno uporabo njihovih računov.

97. Ponudniki plačilnih storitev bi morali uporabnike plačilnih storitev sproti obveščati o posodobitvah in varnostnih postopkih, ki vplivajo nanje pri dostopu do plačilnih storitev.

98. Ponudniki plačilnih storitev bi morali uporabnikom plačilnih storitev zagotoviti pomoč v zvezi z vsemi vprašanji, zahtevami za podporo in obvestili o nepravilnostih ali težavami, ki se nanašajo na varnostne zadeve v zvezi s plačilnimi storitvami. Uporabnike plačilnih storitev bi morali ustrezno obvestiti o tem, kako lahko dobijo tako pomoč.