Linji gwida

EBA/GL/2019/04

28 ta' Novembru 2019

Linji Gwida tal-EBA dwar l-ICT u l-ġestjoni tar-riskju tas-sigurtà

Obbligi ta' konformità u ta' rapportar

Status ta' dawn il-linji gwida

1. Dan id-dokument jinkludi linji gwida maħruġin skont l-Artikolu 16 tar-Regolament (UE) Nru 1093/2010 [1]. F'konformità mal-Artikolu 16(3) tar-Regolament (UE) Nru 1093/2010, l-awtoritajiet kompetenti u l-istituzzjonijiet finanzjarji jridu jagħmlu kull sforz biex jikkonformaw mal-linji gwida.

2. Il-linji gwida jistabbilixxu l-fehma tal-EBA dwar prattiki superviżorji xierqa fis-Sistema Ewropea ta' Superviżjoni Finanzjarja jew dwar kif il-liġi tal-Unjoni Ewropea għandha tiġi applikata f'qasam partikolari. L-awtoritajiet kompetenti kif definiti fl-Artikolu 4(2) tar-Regolament (UE) Nru 1093/2010 u li għalihom japplikaw il-linji gwida għandhom jikkonformaw billi jinkorporawhom fil-prattiki tagħhom kif xieraq (eż. billi jemendaw il-qafas legali tagħhom jew il-proċessi superviżorji tagħhom), inkluż fejn il-linji gwida huma diretti primarjament lejn l-istituzzjonijiet.

Rekwiżiti ta' rapportar

3. Skont l-Artikolu 16(3) tar-Regolament (UE) Nru 1093/2010, l-awtoritajiet kompetenti jridu jinnotifikaw lill-EBA, sa ([jj.xx.ssss]), dwar jekk jikkonformawx jew jekk humiex biħsiebhom jikkonformaw ma' dawn il-linji gwida, jew inkella jagħtu r-raġunijiet tagħhom għan-nuqqas ta' konformità. Fin-nuqqas ta' kwalunkwe notifika sa din l-iskadenza, l-awtoritajiet kompetenti jitqiesu bħala mhux konformi mill-EBA. In-notifiki għandhom jintbagħtu billi tiġi sottomessa l-formola disponibbli fuq is-sit web tal-EBA lil compliance@eba.europa.eu bir-referenza "EBA/GL/2019/04". In-notifiki għandhom jiġu sottomessi minn persuni b'awtorità xierqa li jirrappurtaw il-konformità f'isem l-awtoritajiet kompetenti tagħhom. Kwalunkwe bidla fl-istatus ta' konformità trid tiġi rrapportata wkoll lill-EBA.

4. In-notifiki jiġu ppubblikati fuq is-sit web tal-EBA, f'konformità mal-Artikolu 16(3).

[1] Regolament (UE) Nru 1093/2010 tal-Parlament Ewropew u tal-Kunsill tal-24 ta' Novembru 2010 li jistabbilixxi Awtorità Superviżorja Ewropea (Awtorità Bankarja Ewropea) u li jemenda d-Deċiżjoni Nru 716/2009/KE u jħassar id-Deċiżjoni tal-Kummissjoni 2009/78/KE (ĠU L 331, 15.12.2010, p. 12).

Suġġett, kamp ta' applikazzjoni u definizzjonijiet

Suġġett

5. Dawn il-linji gwida jibnu fuq id-dispożizzjonijiet tal-Artikolu 74 tad-Direttiva 2013/36/UE (CRD) rigward il-governanza interna, u huma derivati mill-mandat li jinħarġu linji gwida fl-Artikolu 95(3) tad-Direttiva (UE) 2015/2366 (PSD2).

6. Dawn il-linji gwida jispeċifikaw il-miżuri ta' ġestjoni tar-riskju li l-istituzzjonijiet finanzjarji (kif definit fil-paragrafu 9 hawn taħt) iridu jieħdu f'konformità mal-Artikolu 74 tas-CRD biex jiġġestixxu r-riskji tal-ICT u tas-sigurtà tagħhom għall-attivitajiet kollha u li l-fornituri ta' servizzi ta' pagament (PSPs kif definit fil-paragrafu 9 hawn taħt) iridu jieħdu, f'konformità mal-Artikolu 95(1) tal-PSD2, biex jiġġestixxu r-riskji operazzjonali u ta' sigurtà (maħsuba bħala "riskji tal-ICT u tas-sigurtà") relatati mas-servizzi ta' pagament li jipprovdu. Il-linji gwida jinkludu rekwiżiti għas-sigurtà tal-informazzjoni, inkluża ċ-ċibersigurtà, sa fejn l-informazzjoni tinżamm fuq sistemi tal-ICT.

Kamp ta' applikazzjoni

7. Dawn il-linji gwida japplikaw fir-rigward tal-ġestjoni tar-riskji tal-ICT u tas-sigurtà fi ħdan l-istituzzjonijiet finanzjarji (kif definiti fil-paragrafu 9). Għall-finijiet ta' dawn il-linji gwida, it-terminu riskji tal-ICT u tas-sigurtà jindirizza r-riskji operazzjonali u ta' sigurtà tal-Artikolu 95 tal-PSD2 għall-forniment ta' servizzi ta' pagament.

8. Għal PSPs (kif definiti fil-paragrafu 9), dawn il-linji gwida japplikaw għall-forniment tagħhom ta' servizzi ta' pagament, f'konformità mal-kamp ta' applikazzjoni u l-mandat tal-Artikolu 95 tal-PSD2. Għall-istituzzjonijiet (kif definiti fil-paragrafu 9), dawn il-linji gwida japplikaw għall-attivitajiet kollha li jipprovdu.

Destinatarji

9. Dawn il-linji gwida huma indirizzati lill-istituzzjonijiet finanzjarji, li għall-finijiet ta' dawn il-linji gwida tirreferi għal (1) PSPs kif definiti fl-Artikolu 4(11) tal-PSD2, u (2) għal istituzzjonijiet, jiġifieri istituzzjonijiet ta' kreditu u ditti ta' investiment kif definiti fil-punt 3 tal-Artikolu 4(1) tar-Regolament (UE) Nru 575/2013. Dawn il-linji gwida japplikaw ukoll għall-awtoritajiet kompetenti kif definit fil-punt 40 tal-Artikolu 4(1) tar-Regolament (UE) Nru 575/2013, inkluż il-Bank Ċentrali Ewropew fir-rigward ta' kwistjonijiet relatati mal-kompiti konferiti lilu bir-Regolament (UE) Nru 1024/2013, u għall-awtoritajiet kompetenti skont il-PSD2, kif imsemmija fil-punt (i) tal-Artikolu 4(2) tar-Regolament (UE) 1093/2010.

Definizzjonijiet

10. Sakemm ma jkunx speċifikat mod ieħor, it-termini użati u definiti f'2013/36/UE (CRD), fir-Regolament (UE) Nru 575/2013 (CRR) u fid-Direttiva (UE) 2015/2366 (PSD2) għandhom l-istess tifsira fil-linji gwida. Barra minn hekk, għall-finijiet ta' dawn il-linji gwida, japplikaw id-definizzjonijiet li ġejjin:

Riskju tal-ICT u tas-sigurtà	Riskju ta' telf minħabba l-ksur tal-kunfidenzjalità, in-nuqqas ta' integrità ta' sistemi u *data*, l-inadegwatezza jew in-nuqqas ta' disponibbiltà ta' sistemi u *data*, jew in-nuqqas ta' kapaċità għall-bdil tat-teknoloġija tal-informazzjoni (IT) fi żmien raġonevoli u bi spejjeż raġonevoli meta r-rekwiżiti tal-ambjent jew tan-negozju jinbidlu (jiġifieri l-aġilità) [2]. Dan jinkludi riskji tas-sigurtà li jirriżultaw minn proċessi interni inadegwati jew li fallew jew avvenimenti esterni, inklużi attakki ċibernetiċi jew sigurtà fiżika inadegwata.
Korp ta' ġestjoni	(a) Għall-istituzzjonijiet tal-kreditu u ditti ta' investiment, dan it-terminu għandu l-istess tifsira bħad-definizzjoni fil-punt (7) tal-Artikolu 3(1) tad-Direttiva 2013/36/UE. (b) Għall-istituzzjonijiet ta' pagament jew istituzzjonijiet ta' flus elettroniċi, dan it-terminu jfisser diretturi jew persuni responsabbli mill-ġestjoni tal-istituzzjonijiet ta' pagament u istituzzjonijiet ta' flus elettroniċi, u fejn rilevanti, persuni responsabbli mill-ġestjoni tal-attivitajiet tas-servizzi ta' pagament tal-istituzzjonijiet ta' pagament u istituzzjonijiet ta' flus elettroniċi. (c) Għall-PSPs imsemmija fil-punti (c), (e) u (f) tal-Artikolu 1(1) tad-Direttiva (UE) 2015/2366, dan it-terminu għandu t-tifsira mogħtija lilu mil-liġi tal-UE jew dik nazzjonali applikabbli.
Inċident operazzjonali jew tas-sigurtà	Avveniment wieħed jew serje ta' avvenimenti marbutin mhux ippjanati mill-istituzzjoni finanzjarja li għandhom jew li probabbilment se jkollhom impatt negattiv fuq l-integrità, id-disponibbiltà, il-kunfidenzjalità u/jew l-awtentiċità tas-servizzi.
Maniġment superjuri	(a) Għall-istituzzjonijiet ta' kreditu u ditti ta' investiment, dan it-terminu għandu l-istess tifsira bħad-definizzjoni fil-punt (9) tal-Artikolu 3(1) tad-Direttiva 2013/36/UE. (b) Għall-istituzzjonijiet ta' pagament u l-istituzzjonijiet ta' flus elettroniċi, dan it-terminu jfisser persuni fiżiċi li jeżerċitaw funzjonijiet eżekuttivi fi ħdan istituzzjoni u li jkunu responsabbli mill-ġestjoni ta' kuljum tal-istituzzjoni, u marbuta li jagħtu rendikont ta' dan lill-korp ta' ġestjoni.

[2] Definizzjoni mil-Linji Gwida tal-EBA dwar il-proċeduri u l-metodoloġiji komuni għall-proċess ta' rieżami u evalwazzjoni superviżorji tad-19 ta' Diċembru 2014 (EBA/GL/2014/13), emendati mill-EBA/GL/2018/03.

	(c) Għall-PSPs imsemmija fil-punti (c), (e) u (f) tal-Artikolu 1(1) tad-Direttiva (UE) 2015/2366, dan it-terminu għandu t-tifsira mogħtija lilu mil-liġi tal-UE jew dik nazzjonali applikabbli.
Predispożizzjoni għar-riskju	Il-livell aggregat u t-tipi ta' riskju li l-PSPs u l-istituzzjonijiet huma lesti jassumu fil-kapaċità ta' riskju tagħhom, f'konformità mal-mudell kummerċjali tagħhom, biex jilħqu l-objettivi strateġiċi tagħhom.
Il-funzjoni ta' awditjar	(a) Għall-istituzzjonijiet ta' kreditu u d-ditti ta' investiment, il-funzjoni ta' awditjar hija kif imsemmija fit-Taqsima 22 tal-linji gwida tal-EBA dwar il-governanza interna (EBA/GL/2017/11). (b) Għal PSPs li mhumiex istituzzjonijiet ta' kreditu, il-funzjoni ta' awditjar trid tkun indipendenti fi ħdan jew mill-PSP u tista' tkun funzjoni ta' awditjar intern u/jew estern.
Proġetti tal-ICT	Kwalunkwe proġett, jew parti minnu, fejn is-sistemi u s-servizzi tal-ICT jinbidlu, jiġu sostitwiti, jitwarrbu jew jiġu implimentati. Il-proġetti tal-ICT jistgħu jkunu parti minn programmi usa' tal-ICT jew tat-trasformazzjoni tan-negozju.
Parti terza	Organizzazzjoni li tkun daħlet f'relazzjonijiet kummerċjali jew kuntratti ma' entità biex tipprovdi prodott jew servizz[3].
Assi ta' informazzjoni	Ġabra ta' informazzjoni, tanġibbli jew mhux tanġibbli, li tajjeb li tiġi protetta.
Assi tal-ICT	Assi jew ta' softwer jew ħardwer li tinstab fl-ambjent tan-negozju.
Sistemi tal-ICT[4]	L-istabbiliment tal-ICT bħala parti minn mekkaniżmu jew netwerk ta' interkonnessjoni li jappoġġa l-operazzjonijiet ta' istituzzjoni finanzjarja.
Servizzi tal-ICT[5]	Is-servizzi pprovduti minn sistemi tal-ICT lil utent intern jew estern wieħed jew aktar. L-eżempji jinkludu d-dħul tad-*data*, il-ħżin tad-*data*, servizzi ta' pproċessar u ta' rapportar tad-*data*, iżda anki s-servizzi ta' appoġġ għall-monitoraġġ, għan-negozju u għad-deċiżjonijiet.

[3] Definizzjoni mill-elementi fundamentali tal-G7 għall-ġestjoni tar-riskji ċibernetiċi minn parti terza fis-settur finanzjarju.
[4] Definizzjoni mil-Linji Gwida dwar il-Valutazzjoni tar-Riskju tal-ICT taħt il-proċess ta' Eevižjoni u Evalwazzjoni Superviżorji (SREP) (EBA/GL/2017/05).
[5] ibid.

Implimentazzjoni

Data ta' applikazzjoni

11. Dawn il-linji gwida jibdew japplikaw mit-30 ta' Ġunju 2020.

Tħassir

12. Il-Linji Gwida dwar il-miżuri ta' sigurtà għar-riskji operazzjonali u ta' sigurtà (EBA/GL/2017/17) maħruġa fl-2017 se jitħassru b'dawn il-linji gwida fid-data li fiha dawn il-linji gwida jsiru applikabbli.

Linji Gwida dwar l-ICT u l-ġestjoni tar-riskju tas-sigurtà

1.1. Proporzjonalità

1. L-istituzzjonijiet finanzjarji kollha għandhom jikkonformaw mad-dispożizzjonijiet stabbiliti f'dawn il-linji gwida b'tali mod li jkun proporzjonat ma', u jqis, id-daqs tal-istituzzjonijiet finanzjarji, l-organizzazzjoni interna tagħhom, u n-natura, il-kamp ta' applikazzjoni, il-kumplessità u l-livell ta' riskju tas-servizzi u l-prodotti li l-istituzzjonijiet finanzjarji jipprovdu jew biħsiebhom jipprovdu.

1.2. Governanza u strateġija

1.2.1. Governanza

2. Il-korp ta' ġestjoni għandu jiżgura li l-istituzzjonijiet finanzjarji jkollhom fis-seħħ qafas ta' governanza interna u ta' kontroll intern adegwat għar-riskji tal-ICT u tas-sigurtà tagħhom. Il-korp ta' ġestjoni għandu jistabbilixxi rwoli u responsabbiltajiet ċari għall-funzjonijiet tal-ICT, il-ġestjoni tar-riskji tas-sigurtà tal-informazzjoni, u l-kontinwità tan-negozju, inklużi dawk għall-korp ta' ġestjoni u l-kumitati tiegħu.

3. Il-korp ta' ġestjoni għandu jiżgura li l-kwantità u l-ħiliet tal-persunal tal-istituzzjonijiet finanzjarji jkunu adegwati biex jappoġġaw il-ħtiġijiet operazzjonali tal-ICT tagħhom u l-proċessi ta' ġestjoni tar-riskji tal-ICT u tas-sigurtà tagħhom fuq bażi kontinwa u biex tiġi żgurata l-implimentazzjoni tal-istrateġija tal-ICT tagħhom. Il-korp ta' ġestjoni għandu jiżgura li l-baġit allokat ikun xieraq biex jikseb dan t'hawn fuq. Barra minn hekk, l-istituzzjonijiet finanzjarji għandhom jiżguraw li l-membri kollha tal-persunal, inklużi d-detenturi ta' funzjonijiet ewlenin, jirċievu taħriġ xieraq dwar ir-riskji ta' sigurtà u tal-ICT, inkluż dwar is-sigurtà tal-informazzjoni, fuq bażi annwali, jew aktar spiss jekk ikun meħtieġ (ara wkoll it-Taqsima 1.4.7).

4. Il-korp ta' ġestjoni għandu responsabbiltà ġenerali mill-istabbiliment, l-approvazzjoni u s-sorveljanza tal-implimentazzjoni tal-istrateġija tal-ICT tal-istituzzjonijiet finanzjarji bħala parti mill-istrateġija ġenerali tan-negozju tagħhom kif ukoll għall-istabbiliment ta' qafas ta' ġestjoni tar-riskji effettiv għar-riskji tal-ICT u tas-sigurtà.

1.2.2. Strateġija

5. L-istrateġija tal-ICT għandha tkun allinjata mal-istrateġija ġenerali tan-negozju tal-istituzzjonijiet finanzjarji u għandha tiddefinixxi:

   a) kif l-ICT tal-istituzzjonijiet finanzjarji għandha tevolvi biex tappoġġa u tipparteċipa fl-istrateġija tan-negozju tagħhom, inkluži l-evoluzzjoni tal-istruttura organizzattiva, il-bidliet fis-sistema tal-ICT u dipendenzi ewlenin ma' partijiet terzi;
   b) l-istrateġija ppjanata u l-evoluzzjoni tal-istruttura tal-ICT, inkluži dipendenzi ta' partijiet terzi;
   c) objettivi ċari dwar is-sigurtà tal-informazzjoni, li jiffukaw fuq sistemi tal-ICT u servizzi tal-ICT, persunal u proċessi.

6. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu settijiet ta' pjanijiet ta' azzjoni li jkun fihom miżuri li għandhom jittieħdu biex jintlaħaq l-għan tal-istrateġija tal-ICT. Dawn għandhom jiġu kkomunikati lill-persunal rilevanti kollu (inkluži l-kuntratturi u l-forniturі terzi fejn applikabbli u rilevanti). Il-pjanijiet ta' azzjoni għandhom jiġu rieżaminati perjodikament biex tiġi żgurata r-rilevanza u l-adegwatezza tagħhom. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu wkoll proċessi biex jimmonitorjaw u jkejlu l-effettività tal-implimentazzjoni tal-istrateġija tal-ICT tagħhom.

1.2.3. Użu ta' forniturі terzi

7. Mingħajr preġudizzju għal-Linji Gwida tal-EBA dwar l-esternalizzazzjoni tal-arranġamenti (EBA/GL/2019/02) u l-Artikolu 19 tal-PSD2, l-istituzzjonijiet finanzjarji għandhom jiżguraw l-effettività tal-miżuri ta' mitigazzjoni tar-riskju kif definiti mill-qafas ta' ġestjoni tar-riskju tagħhom, inkluži l-miżuri stabbiliti f'dawn il-linji gwida, meta l-funzjonijiet operazzjonali tas-servizzi ta' pagament u/jew tas-servizzi tal-ICT u tas-sistemi tal-ICT ta' kwalunkwe attività jiġu esternalizzati, inkluż lil entitajiet fi grupp, jew meta jintużaw partijiet terzi.

8. Sabiex tiġi żgurata l-kontinwità tas-servizzi tal-ICT u tas-sistemi tal-ICT, l-istituzzjonijiet finanzjarji għandhom jiżguraw li l-kuntratti u l-ftehimiet fil-livell tas-servizz (kemm għal ċirkostanzi normali kif ukoll fil-każ ta' tħarbit fis-servizz — ara wkoll it-Taqsima 1.7.2) mal-forniturі (forniturі tal-esternalizzazzjoni, entitajiet fi grupp, jew forniturі terzi) jinkludu dawn li ġejjin:

   a) objettivi u miżuri xierqa u proporzjonati relatati mas-sigurtà tal-informazzjoni, inkluži rekwiżiti bħar-rekwiżiti minimi taċ-ċibersigurtà; l-ispeċifikazzjonijiet taċ-ċiklu tal-ħajja tad-*data* tal-istituzzjoni finanzjarja; kwalunkwe rekwiżit rigward il-kriptaġġ tad-*data*, is-sigurtà tan-netwerk u l-proċessi tal-monitoraġġ tas-sigurtà, u l-post fejn jinsabu ċ-ċentri tad-*data*;

b) proċeduri ta' ġestjoni ta' inċidenti operazzjonali u ta' sigurtà, inklużi eskalazzjoni u rapportar.

9. L-istituzzjonijiet finanzjarji għandhom jimmonitorjaw u jfittxu l-assigurazzjoni dwar il-livell ta' konformità ta' dawn il-forniturі mal-objettivi, il-miżuri u l-miri ta' prestazzjoni ta' sigurtà tal-istituzzjoni finanzjarja.

1.3. Qafas tal-ġestjoni tar-riskji tal-ICT u tas-sigurtà

1.3.1. Organizzazzjoni u objettivi

10. L-istituzzjonijiet finanzjarji għandhom jidentifikaw u jiġġestixxu r-riskji tal-ICT u tas-sigurtà tagħhom. Il-funzjoni(jiet) tal-ICT li jkunu responsabbli mis-sistemi tal-ICT, il-proċessi u l-operazzjonijiet tas-sigurtà għandu jkollhom proċessi u kontrolli xierqa fis-seħħ biex jiżguraw li r-riskji kollha jiġu identifikati, analizzati, imkejla, immonitorjati, ġestiti, irrappurtati u miżmuma fi ħdan il-limiti tal-predispożizzjoni għar-riskju tal-istituzzjoni finanzjarja u li l-proġetti u s-sistemi li jwettqu u l-attivitajiet li jwettqu jkunu f'konformità mar-rekwiżiti esterni u interni.

11. L-istituzzjonijiet finanzjarji għandhom jassenjaw ir-responsabbiltà mill-ġestjoni u s-sorveljanza tar-riskji tal-ICT u tas-sigurtà għal funzjoni ta' kontroll, filwaqt li jaderixxu mar-rekwiżiti tat-Taqsima 19 tal-Linji Gwida tal-EBA dwar il-governanza interna (EBA/GL/2017/11). L-istituzzjonijiet finanzjarji għandhom jiżguraw l-indipendenza u l-oġġettività ta' din il-funzjoni ta' kontroll billi tiġi segregata b'mod xieraq mill-proċessi tal-operazzjonijiet tal-ICT. Din il-funzjoni ta' kontroll għandha tirrapporta direttament għand il-korp ta' ġestjoni u tkun responsabbli mill-monitoraġġ u l-kontroll tal-aderenza mal-qafas ta' ġestjoni tar-riskji tal-ICT u tas-sigurtà. Għandha tiżgura li r-riskji tal-ICT u tas-sigurtà jiġu identifikati, imkejla, ivvalutati, ġestiti, immonitorjati u rrapportati. L-istituzzjonijiet finanzjarji għandhom jiżguraw li din il-funzjoni ta' kontroll ma tkun responsabbli mill-ebda awditjar intern.

    Il-funzjoni ta' awditjar intern għandha, skont approċċ ibbażat fuq ir-riskju, ikollha l-kapaċità li twettaq rieżami b'mod indipendenti u tipprovdi assigurazzjoni oġġettiva tal-konformità tal-attivitajiet u l-unitajiet kollha tal-ICT u dawk relatati mas-sigurtà ta' istituzzjoni finanzjarja mal-politiki u l-proċeduri tal-istituzzjoni finanzjarja u mar-rekwiżiti esterni, filwaqt li taderixxi mar-rekwiżiti tat-Taqsima 22 tal-Linji Gwida tal-EBA dwar il-governanza interna (EBA/GL/2017/11).

12. L-istituzzjonijiet finanzjarji għandhom jiddefinixxu u jassenjaw rwoli u responsabbiltajiet ewlenin, u linji ta' rapportar rilevanti, sabiex il-qafas ta' ġestjoni tar-riskji tal-ICT u tas-sigurtà jkun effettiv. Dan il-qafas għandu jkun integrat b'mod sħiħ fil-proċessi ġenerali tal-ġestjoni tar-riskju tal-istituzzjonijiet finanzjarji, u jkun allinjat magħhom.

13. Il-qafas tal-ġestjoni tar-riskji tal-ICT u tas-sigurtà għandu jinkludi proċessi fis-seħħ biex:

    a) jiddetermina l-predispożizzjoni għar-riskju għal riskji tal-ICT u tas-sigurtà, skont il-predispożizzjoni għar-riskju tal-istituzzjoni finanzjarja;
    b) jidentifika u jivvaluta r-riskji tal-ICT u tas-sigurtà li għalihom tkun esposta istituzzjoni finanzjarja;

c) jiddefinixxi miżuri ta' mitigazzjoni, inklużi kontrolli, biex jiġu mitigati r-riskji tal-ICT u tas-sigurtà;
d) jissorvelja l-effettività ta' dawn il-miżuri kif ukoll l-għadd ta' inċidenti rrappurtati, inkluż għal PSPs, l-inċidenti rrappurtati skont l-Artikolu 96 tal-PSD2 li jaffettwaw l-attivitajiet relatati mal-ICT, u fejn meħtieġ jieħu azzjoni biex jikkoreġi l-miżuri;
e) jirrapporta lill-korp ta' ġestjoni dwar ir-riskji tal-ICT u tas-sigurtà, u l-kontrolli;
f) jidentifika u jivvaluta jekk hemmx xi riskju tal-ICT u tas-sigurtà li jirriżulta minn kwalunkwe bidla kbira fis-sistema tal-ICT jew fis-servizzi, il-proċessi jew il-proċeduri tal-ICT, u/jew wara kwalunkwe inċident operazzjonali jew ta' sigurtà sinifikanti.

14. L-istituzzjonijiet finanzjarji għandhom jiżguraw li l-qafas tal-ġestjoni tar-riskji tal-ICT u tas-sigurtà jiġi ddokumentat, u jittejjeb kontinwament, abbażi tat-"tagħlimiet miksuba" matul l-implimentazzjoni u l-monitoraġġ tiegħu. Il-qafas tal-ġestjoni tar-riskji tal-ICT u tas-sigurtà għandu jiġi approvat u rieżaminat, tal-inqas darba fis-sena, mill-korp ta' ġestjoni.

1.3.2. Identifikazzjoni ta' funzjonijiet, proċessi u assi

15. L-istituzzjonijiet finanzjarji għandhom jidentifikaw, jistabbilixxu u jżommu mmappjar aġġornat tal-funzjonijiet kummerċjali, ir-rwoli u l-proċessi ta' appoġġ tagħhom biex jidentifikaw l-importanza ta' kull waħda minnhom u tal-interdipendenzi tagħhom relatati mar-riskji tal-ICT u tas-sigurtà.

16. Barra minn hekk, l-istituzzjonijiet finanzjarji għandhom jidentifikaw, jistabbilixxu u jżommu mmappjar aġġornat tal-assi ta' informazzjoni li jappoġġaw il-funzjonijiet kummerċjali u l-proċessi ta' appoġġ tagħhom, bħalma huma s-sistemi tal-ICT, il-persunal, il-kuntratturi, il-partijiet terzi u d-dipendenzi fuq sistemi u proċessi interni u esterni oħrajn, sabiex ikunu jistgħu, tal-inqas, jimmaniġġaw l-assi ta' informazzjoni li jappoġġaw il-funzjonijiet u l-proċessi kritiċi tan-negozju tagħhom.

1.3.3. Klassifikazzjoni u valutazzjoni tar-riskju

17. L-istituzzjonijiet finanzjarji għandhom jikklassifikaw il-funzjonijiet kummerċjali, il-proċessi ta' appoġġ u l-assi ta' informazzjoni msemmija fil-paragrafi 15 u 16 f'termini ta' kemm huma kritiċi.

18. Sabiex jiddefinixxu kemm huma kritiċi dawn il-funzjonijiet kummerċjali, il-proċessi ta' appoġġ u l-assi ta' informazzjoni identifikati, l-istituzzjonijiet finanzjarji għandhom mill-inqas jikkunsidraw ir-rekwiżiti ta' kunfidenzjalità, integrità u disponibbiltà. Għandu jkun hemm responsabbiltà assenjati b'mod ċar għall-assi ta' informazzjoni.

19. L-istituzzjonijiet finanzjarji għandhom jirrieżaminaw l-adegwatezza tal-klassifikazzjoni tal-assi ta' informazzjoni u d-dokumentazzjoni rilevanti, meta ssir il-valutazzjoni tar-riskju.

20. L-istituzzjonijiet finanzjarji għandhom jidentifikaw ir-riskji tal-ICT u tas-sigurtà li jkollhom impatt fuq il-funzjonijiet kummerċjali identifikati u kklassifikati, fuq il-proċessi ta' appoġġ u fuq l-assi ta' informazzjoni, skont kemm huma kritiċi. Jekk ikun meħtieġ, din il-valutazzjoni tar-riskju għandha ssir u tiġi ddokumentata kull sena jew f'intervalli iqsar. Tali valutazzjonijiet tar-riskju għandhom jitwettqu wkoll fuq kwalunkwe bidliet kbar fl-infrastruttura, fil-proċessi jew fil-

proċeduri li jaffettwaw il-funzjonijiet kummerċjali, il-proċessi ta' appoġġ jew l-assi ta' informazzjoni, u konsegwentement il-valutazzjoni tar-riskju attwali tal-istituzzjonijiet finanzjarji għandha tiġi aġġornata.

21. L-istituzzjonijiet finanzjarji għandhom jiżguraw li jimmonitorjaw kontinwament it-theddid u l-vulnerabbiltajiet rilevanti għall-proċessi tan-negozju tagħhom, il-funzjonijiet ta' appoġġ u l-assi ta' informazzjoni u għandhom jirrieżaminaw b'mod regolari x-xenarji tar-riskju li jkollhom impatt fuqhom.

1.3.4. Mitigazzjoni tar-riskju

22. Abbażi tal-valutazzjonijiet tar-riskju, l-istituzzjonijiet finanzjarji għandhom jiddeterminaw liema miżuri huma meħtieġa biex ir-riskji tal-ICT u tas-sigurtà identifikati jitnaqqsu għal livelli aċċettabbli u jekk humiex meħtieġa bidliet fil-proċessi tan-negozju, il-miżuri ta' kontroll, is-sistemi tal-ICT u s-servizzi tal-ICT eżistenti. Istituzzjoni finanzjarja għandha tikkunsidra ż-żmien meħtieġ biex jiġu implimentati dawn il-bidliet u ż-żmien biex jittieħdu miżuri ta' mitigazzjoni interim xierqa biex jiġu minimizzati r-riskji tal-ICT u tas-sigurtà biex jibqgħu fi ħdan il-predispożizzjoni għar-riskju tal-ICT u tas-sigurtà tal-istituzzjoni finanzjarja.

23. L-istituzzjonijiet finanzjarji għandhom jiddefinixxu u jimplimentaw miżuri biex jimmitigaw ir-riskji tal-ICT u tas-sigurtà identifikati u biex jipproteġu l-assi ta' informazzjoni skont il-klassifikazzjoni tagħhom.

1.3.5. Rapportar

24. L-istituzzjonijiet finanzjarji għandhom jirrapportaw ir-riżultati tal-valutazzjoni tar-riskju lill-korp ta' ġestjoni b'mod ċar u f'waqtu. Rapportar bħal dan huwa mingħajr preġudizzju għall-obbligu li l-PSPs jipprovdu lill-awtoritajiet kompetenti b'valutazzjoni tar-riskju aġġornata u komprensiva, kif stabbilit fl-Artikolu 95(2) tad-Direttiva (UE) 2015/2366.

1.3.6. Awditu

25. Il-governanza, is-sistemi u l-proċessi ta' istituzzjoni finanzjarja għar-riskji tagħha tal-ICT u tas-sigurtà għandhom jiġu vverifikati minn żmien għal żmien minn awdituri b'għarfien, ħiliet u għarfien espert suffiċjenti f'riskji tal-ICT u tas-sigurtà u f'pagamenti (għall-PSPs) biex jipprovdu assigurazzjoni indipendenti tal-effettività tagħhom lill-korp ta' ġestjoni. L-awdituri għandhom ikunu indipendenti fi ħdan jew mill-istituzzjoni finanzjarja. Il-frekwenza u l-attenzjoni ta' tali awditu għandhom ikunu proporzjonati mar-riskji rilevanti tal-ICT u tas-sigurtà.

26. Korp ta' ġestjoni ta' istituzzjoni finanzjarja għandu japprova l-pjan ta' awditu, inkluż kwalunkwe awditu tal-ICT u kwalunkwe modifika materjali tagħhom. Il-pjan ta' awditu u l-eżekuzzjoni tiegħu, inkluża l-frekwenza tal-awditu, għandhom jirriflettu u jkunu proporzjonati mar-riskji inerenti għall-ICT u s-sigurtà fl-istituzzjoni finanzjarja u għandhom jiġu aġġornati regolarment.

27. Għandu jiġi stabbilit proċess ta' segwitu formali li jinkludi dispożizzjonijiet għall-verifika f'waqtha u r-rimedju tas-sejbiet tal-awditu tal-ICT.

1.4. Sigurtà tal-informazzjoni

1.4.1. Politika tas-sigurtà tal-informazzjoni

28. L-istituzzjonijiet finanzjarji għandhom jiżviluppaw u jiddokumentaw politika dwar is-sigurtà tal-informazzjoni li għandha tiddefinixxi l-prinċipji ta' livell għoli u r-regoli li jipproteġu l-kunfidenzjalità, l-integrità u d-disponibbiltà tad-*data* u l-informazzjoni tal-istituzzjonijiet u tal-klijenti tagħhom. Fil-każ tal-PSPs, din il-politika tiġi identifikata fid-dokument tal-politika tas-sigurtà li għandu jiġi adottat skont l-Artikolu 5(1)(j) tad-Direttiva (UE) 2015/2366. Il-politika dwar is-sigurtà tal-informazzjoni għandha tkun konformi mal-objettivi tas-sigurtà tal-informazzjoni tal-istituzzjoni finanzjarja u bbażata fuq ir-riżultati rilevanti tal-proċess tal-valutazzjoni tar-riskju. Il-politika għandha tiġi approvata mill-korp ta' ġestjoni.

29. Il-politika għandha tinkludi deskrizzjoni tar-rwoli u r-responsabbiltajiet ewlenin tal-ġestjoni tas-sigurtà tal-informazzjoni, u għandha tistabbilixxi r-rekwiżiti għall-persunal u l-kuntratturi, il-proċessi u t-teknoloġija fir-rigward tas-sigurtà tal-informazzjoni, filwaqt li tirrikonoxxi li l-persunal u l-kuntratturi fil-livelli kollha għandhom responsabbiltajiet biex jiżguraw is-sigurtà tal-informazzjoni tal-istituzzjonijiet finanzjarji. Il-politika għandha tiżgura l-kunfidenzjalità, l-integrità u d-disponibbiltà tal-assi fiżiċi u loġiċi kritiċi, ir-riżorsi u d-*data* sensittiva ta' istituzzjoni finanzjarja kemm jekk dawn mhux qed jintużaw, jekk qegħdin fi tranżitu jew qed jintużaw. Il-politika tas-sigurtà tal-informazzjoni għandha tiġi kkomunikata lill-persunal u l-kuntratturi kollha tal-istituzzjoni finanzjarja.

30. Abbażi tal-politika dwar is-sigurtà tal-informazzjoni, l-istituzzjonijiet finanzjarji għandhom jistabbilixxu u jimplimentaw miżuri ta' sigurtà biex inaqqsu r-riskji tal-ICT u tas-sigurtà li huma esposti għalihom. Dawn il-miżuri għandhom jinkludu:

    a) organizzazzjoni u governanza skont il-paragrafi 10 u 11;
    b) sigurtà loġika (Taqsima 1.4.2);
    c) sigurtà fiżika (Taqsima 1.4.3);
    d) sigurtà tal-operazzjonijiet tal-ICT (Taqsima 1.4.4);
    e) monitoraġġ tas-sigurtà (Taqsima 1.4.5);
    f) rieżamijiet, valutazzjoni u ttestjar tas-sigurtà tal-informazzjoni (Taqsima 1.4.6);
    g) taħriġ u sensibilizzazzjoni dwar is-sigurtà tal-informazzjoni (Taqsima 1.4.7).

1.4.2. Sigurtà loġika

31. L-istituzzjonijiet finanzjarji għandhom jiddefinixxu, jiddokumentaw u jimplimentaw proċeduri għall-kontroll tal-aċċess loġiku (ġestjoni tal-identità u tal-aċċess). Dawn il-proċeduri għandhom jiġu implimentati, infurzati, immonitorjati u rieżaminati perjodikament. Il-proċeduri għandhom jinkludu wkoll kontrolli għall-monitoraġġ ta' anomaliji. Dawn il-proċeduri għandhom, bħala minimu, jimplimentaw l-elementi li ġejjin, fejn it-terminu "utent" jinkludi wkoll utenti tekniċi:

    (a) **Il-ħtieġa ta' tagħrif, l-inqas privileġġ u s-segregazzjoni tad-dmirijiet:** l-istituzzjonijiet finanzjarji għandhom jiġġestixxu d-drittijiet ta' aċċess għall-assi ta' informazzjoni u s-sistemi ta' appoġġ tagħhom fuq bażi ta' "ħtieġa ta' tagħrif", inkluż għal aċċess mill-

bogħod. L-utenti għandhom jingħataw drittijiet minimi ta' aċċess li huma strettament meħtieġa biex iwettqu dmirijiethom (prinċipju ta' "l-inqas privileġġ"), jiġifieri biex jiġi evitat aċċess mhux ġustifikat għal sett kbir ta' *data* jew biex tiġi evitata l-allokazzjoni ta' kombinazzjonijiet ta' drittijiet ta' aċċess li jistgħu jintużaw biex jiġu evitati l-kontrolli (il-prinċipju ta' "segregazzjoni tad-dmirijiet").

(b) **Responsabbiltà tal-utenti:** l-istituzzjonijiet finanzjarji għandhom jillimitaw, kemm jista' jkun, l-użu ta' kontijiet ġeneriċi u kondiviżi tal-utenti u jiżguraw li l-utenti jkunu jistgħu jiġu identifikati għall-azzjonijiet imwettqa fis-sistemi tal-ICT.

(c) **Drittijiet privileġġati ta' aċċess:** l-istituzzjonijiet finanzjarji għandhom jimplimentaw kontrolli b'saħħithom fuq l-aċċess għas-sistema privileġġata billi jillimitaw strettament u jissorveljaw mill-qrib il-kontijiet b'intitolamenti ta' aċċess għas-sistema għolja (eż. kontijiet ta' amministratur). Sabiex tiġi żgurata komunikazzjoni sigura u jitnaqqas ir-riskju, l-aċċess amministrattiv mill-bogħod għal sistemi tal-ICT kritiċi għandu jingħata biss abbażi ta' ħtieġa ta' tagħrif u meta jintużaw soluzzjonijiet ta' awtentikazzjoni b'saħħithom.

(d) **Reġistrazzjoni tal-attivitajiet tal-utenti:** bħala minimu, l-attivitajiet kollha minn utenti privileġġati għandhom jiġu rreġistrati u mmonitorjati. Ir-reġistri ta' aċċess għandhom jinżammu siguri biex jiġi evitat modifika jew tħassir mhux awtorizzat u jinżammu għal perjodu li jikkorrispondi ma' kemm huma kritiċi dawn il-funzjonijiet ta' negozju, il-proċessi ta' appoġġ u l-assi ta' informazzjoni identifikati, f'konformità mat-Taqsima 1.3.3, mingħajr preġudizzju għar-rekwiżiti ta' żamma stipulati fil-liġi nazzjonali u tal-UE. Istituzzjoni finanzjarja għandha tuża din l-informazzjoni biex tiffaċilita l-identifikazzjoni u l-investigazzjoni ta' attivitajiet anomali li jkunu ġew identifikati fil-forniment tas-servizzi ta' pagament.

(e) **Ġestjoni tal-aċċess:** għandhom jingħataw, jiġu rtirati jew jiġu modifikati f'waqthom drittijiet ta' aċċess, skont flussi tax-xogħol għall-approvazzjoni predefiniti li jinvolvu sid in-negozju tal-informazzjoni li jkun hemm aċċess għaliha (sid tal-assi tal-informazzjoni). Fil-każ ta' terminazzjoni ta' impjieg, id-drittijiet ta' aċċess għandhom jiġu rtirati minnufih.

(f) **Ċertifikazzjoni mill-ġdid tal-aċċess:** id-drittijiet ta' aċċess għandhom jiġu rieżaminati perjodikament biex ikun żgurat li l-utenti ma jkollhomx privileġġi eċċessivi u li d-drittijiet ta' aċċess jiġu rtirati meta ma jkunux meħtieġa aktar.

(g) **Metodi ta' awtentikazzjoni:** l-istituzzjonijiet finanzjarji għandhom jinfurzaw metodi ta' awtentikazzjoni li huma robusti biżżejjed biex jiżguraw b'mod adegwat u effettiv li jkun hemm konformità mal-politiki u l-proċeduri ta' kontroll tal-aċċess. Il-metodi ta' awtentikazzjoni għandhom ikunu proporzjonati ma' kemm huma kritiċi s-sistemi tal-ICT, l-informazzjoni jew il-proċess li jkun hemm aċċess għalihom. Dan għandu, bħala minimu, jinkludi passwords kumplessi jew metodi ta' awtentikazzjoni aktar b'saħħithom (bħal awtentikazzjoni b'żewġ fatturi), skont ir-riskju rilevanti.

32. L-aċċess elettroniku permezz ta' applikazzjonijiet għad-*data* u s-sistemi tal-ICT għandu jkun limitat għal minimu meħtieġ għall-forniment tas-servizz rilevanti.

1.4.3. Sigurtà fiżika

33. Il-miżuri tas-sigurtà fiżika tal-istituzzjonijiet finanzjarji għandhom jiġu definiti, dokumentati u implimentati biex jipproteġu l-bini, iċ-ċentri tad-*data* u ż-żoni sensittivi tagħhom minn aċċess mhux awtorizzat u minn perikli ambjentali.

34. L-individwi awtorizzati biss għandu jkollhom permess biex jaċċessaw b'mod fiżiku s-sistemi tal-ICT. L-awtorizzazzjoni għandha tkun assenjata f'konformità mal-kompiti u r-responsabbiltajiet tal-individwu, u tkun limitata għal individwi li jiġu mħarrġa u mmonitorjati kif xieraq. L-aċċess fiżiku għandu jiġi rieżaminat regolarment biex ikun żgurat li d-drittijiet ta' aċċess bla bżonn jiġu rrevokati meta ma jkunux meħtieġa.

35. Miżuri adegwati għall-protezzjoni minn perikli ambjentali għandhom ikunu proporzjonati mal-importanza tal-bini u ma' kemm huma kritiċi l-operazzjonijiet jew tas-sistemi tal-ICT li jinsabu f'dan il-bini.

1.4.4. Sigurtà tal-operazzjonijiet tal-ICT

36. L-istituzzjonijiet finanzjarji għandhom jimplimentaw proċeduri biex jipprevjenu l-okkorrenza ta' kwistjonijiet ta' sigurtà fis-sistemi tal-ICT u fis-servizzi tal-ICT u għandhom jimminimizzaw l-impatt tagħhom fuq l-għoti tas-servizz tal-ICT. Dawn il-proċeduri għandhom jinkludu l-miżuri li ġejjin:

    a) l-identifikazzjoni tal-vulnerabbiltajiet potenzjali, li għandhom jiġu evalwati u rrimedjati billi jiġi żgurat li s-softwer u l-firmwer huma aġġornati, inkluż is-softwer ipprovdut mill-istituzzjonijiet finanzjarji lill-utenti interni u esterni tagħhom, billi jiġu żviluppati patches ta' sigurtà kritiċi jew billi jiġu implimentati kontrolli ta' kumpens;
    b) l-implimentazzjoni ta' linji bażi siguri tal-konfigurazzjoni tal-komponenti tan-netwerk kollha;
    c) l-implimentazzjoni ta' segmentazzjoni tan-netwerk, sistemi ta' prevenzjoni ta' telf ta' *data* u l-kriptaġġ tat-traffiku tan-netwerk (skont il-klassifikazzjoni tad-*data*);
    d) l-implimentazzjoni ta' ħarsien tal-punti ta' tmiem inklużi servers, workstations u tagħmir mobbli; l-istituzzjonijiet finanzjarji għandhom jevalwaw jekk il-punti ta' tmiem jissodisfawx l-istandards ta' sigurtà definiti minnhom qabel ma jingħataw aċċess għan-netwerk korporattiv;
    e) l-iżgurar li jkun hemm fis-seħħ mekkaniżmi li jivverifikaw l-integrità tas-softwer, il-firmwer u d-*data*;
    f) il-kriptaġġ tad-*data* wieqfa u fi tranżitu (skont il-klassifikazzjoni tad-*data*).

37. Barra minn hekk, fuq bażi kontinwa, l-istituzzjonijiet finanzjarji għandhom jiddeterminaw jekk il-bidliet fl-ambjent operattiv eżistenti jinfluwenzawx il-miżuri ta' sigurtà eżistenti jew jirrikjedux l-adozzjoni ta' miżuri addizzjonali għall-mitigazzjoni xierqa tar-riskji relatati. Dawn il-bidliet għandhom ikunu parti mill-proċess ta' ġestjoni tat-tibdil formali tal-istituzzjonijiet finanzjarji, li għandu jiżgura li l-bidliet jiġu ppjanati, ittestjati, iddokumentati, awtorizzati u implimentati kif xieraq.

1.4.5. Monitoraġġ tas-sigurtà

38. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu u jimplimentaw politiki u proċeduri biex jidentifikaw attivitajiet anomali li jista' jkollhom impatt fuq is-sigurtà tal-informazzjoni tal-istituzzjonijiet finanzjarji u li jirrispondu b'mod xieraq għal dawn l-avvenimenti. Bħala parti minn dan il-monitoraġġ kontinwu, l-istituzzjonijiet finanzjarji għandhom jimplimentaw kapaċitajiet xierqa u effettivi għall-identifikazzjoni u r-rapportar ta' intrużjoni fiżika jew loġika kif ukoll ksur tal-kunfidenzjalità, l-integrità u d-disponibbiltà tal-assi ta' informazzjoni. Il-proċessi ta' monitoraġġ u identifikazzjoni kontinwi għandhom ikopru:

    a) fatturi interni u esterni rilevanti, inklużi funzjonijiet amministrattivi tan-negozju u tal-ICT;
    b) tranżazzjonijiet għad-detezzjoni tal-użu ħażin tal-aċċess minn partijiet terzi jew entitajiet oħra u użu ħażin intern ta' aċċess;
    c) theddid intern u estern potenzjali.

39. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu u jimplimentaw proċessi u strutturi organizzazzjonali sabiex jidentifikaw u jimmonitorjaw b'mod kostanti t-theddid għas-sigurtà li jista' jaffettwa fuq livell materjali l-abbiltajiet tagħhom li jipprovdu servizzi. L-istituzzjonijiet finanzjarji għandhom jimmonitorjaw l-iżviluppi teknoloġiċi b'mod attiv sabiex jiżguraw li huma konxji dwar ir-riskji ta' sigurtà. L-istituzzjonijiet finanzjarji għandhom jimplimentaw miżuri ta' identifikazzjoni, pereżempju sabiex jidentifikaw kxif possibbli ta' informazzjoni, kodifikazzjoni malizzjuża u theddid ieħor għas-sigurtà, u vulnerabbiltajiet magħrufa mill-pubbliku fis-softwer u l-ħardwer, u għandhom jiċċekkjaw għal aġġornamenti tas-sigurtà ġodda korrispondenti.

40. Il-proċess ta' monitoraġġ tas-sigurtà għandu jgħin ukoll lil istituzzjoni finanzjarja biex tifhem in-natura tal-inċidenti operazzjonali jew tas-sigurtà, tidentifika x-xejriet u tappoġġa l-investigazzjonijiet tal-organizzazzjoni.

1.4.6. Rieżamijiet, valutazzjoni u ttestjar tas-sigurtà tal-informazzjoni

41. L-istituzzjonijiet finanzjarji għandhom iwettqu varjetà ta' rieżamijiet, valutazzjonijiet u ttestjar tas-sigurtà tal-informazzjoni biex jiżguraw l-identifikazzjoni effettiva tal-vulnerabbiltajiet fis-sistemi tal-ICT u s-servizzi tal-ICT tagħhom. Pereżempju, l-istituzzjonijiet finanzjarji jistgħu jwettqu analiżi tan-nuqqasijiet meta mqabbla mal-istandards tas-sigurtà tal-informazzjoni, ir-rieżamijiet tal-konformità, il-verifiki interni u esterni tas-sistemi tal-informazzjoni, jew rieżamijiet fiżiċi tas-sigurtà. Barra minn hekk, l-istituzzjoni għandha tikkunsidra prattiki tajbin bħar-rieżamijiet tal-kodiċi tas-sors, il-valutazzjonijiet tal-vulnerabbiltà, it-testijiet ta' penetrazzjoni u l-eżerċizzji tat-tim l-aħmar.

42. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu u jimplimentaw qafas tal-ittestjar tas-sigurtà tal-informazzjoni li jivvalida r-robustezza u l-effettività tal-miżuri ta' sigurtà tal-informazzjoni tagħhom u jiżguraw li dan il-qafas jikkunsidra t-theddid u l-vulnerabbltajiet identifikati permezz tal-monitoraġġ tat-theddid u l-proċess tal-valutazzjoni tar-riskji tal-ICT u tas-sigurtà.

43. Il-qafas tal-ittestjar tas-sigurtà tal-informazzjoni għandu jiżgura li t-testijiet:

    a) jitwettqu minn eżaminaturi indipendenti b'għarfien, ħiliet u għarfien espert suffiċjenti fl-ittestjar tal-miżuri ta' sigurtà tal-informazzjoni u li mhumiex involuti fl-iżvilupp tal-miżuri ta' sigurtà tal-informazzjoni;
    b) jinkludu scans tal-vulnerabbiltà u testijiet tal-penetrazzjoni (inklużi fejn ikunu meħtieġa u xierqa testijiet tal-penetrazzjoni mmexxija mit-theddid) proporzjonati mal-livell ta' riskju identifikat mal-proċessi u s-sistemi tan-negozju.

44. L-istituzzjonijiet finanzjarji għandhom iwettqu testijiet kontinwi u ripetuti tal-miżuri ta' sigurtà. Għas-sistemi kritiċi kollha tal-ICT (il-paragrafu 17), dawn it-testijiet għandhom isiru tal-inqas fuq bażi annwali u, għall-PSPs, ikunu parti mill-valutazzjoni komprensiva tar-riskji tas-sigurtà relatati mas-servizzi ta' pagament li jipprovdu, skont l-Artikolu 95(2) tal-PSD2. Sistemi li mhumiex kritiċi għandhom jiġu ttestjati b'mod regolari bl-użu ta' approċċ ibbażat fuq ir-riskju, iżda tal-inqas kull 3 snin.

45. L-istituzzjonijiet finanzjarji għandhom jiżguraw li t-testijiet tal-miżuri ta' sigurtà jitwettqu f'każ ta' bidliet fl-infrastruttura, fil-proċessi jew fil-proċeduri u jekk isiru bidliet minħabba inċidenti operazzjonali kbar jew ta' sigurtà jew minħabba r-rilaxx ta' applikazzjonijiet ġodda jew mibdula b'mod sinifikanti li jiffaċċjaw l-internet.

46. L-istituzzjonijiet finanzjarji għandhom jimmonitorjaw u jevalwaw ir-riżultati tat-testijiet tas-sigurtà u jaġġornaw il-miżuri ta' sigurtà tagħhom kif xieraq mingħajr dewmien żejjed fil-każ ta' sistemi tal-ICT kritiċi.

47. Għall-PSPs, il-qafas tal-ittestjar għandu jinkorpora wkoll il-miżuri ta' sigurtà rilevanti għal (1) terminals u apparati ta' pagament użati għall-forniment tas-servizzi ta' pagament, (2) terminals u apparati ta' pagament użati għall-awtentikazzjoni tal-utenti tas-servizz tal-pagament (PSU) u (3) apparati u softwer ipprovduti mill-PSP lill-PSU għall-ġenerazzjoni/għar-riċezzjoni ta' kodiċi ta' awtentikazzjoni.

48. Abbażi tat-theddid għas-sigurtà osservat u l-bidliet li jsiru, għandu jitwettaq ittestjar sabiex jiġu inkorporati xenarji ta' attakki potenzjali magħrufa u rilevanti.

1.4.7. Taħriġ u sensibilizzazzjoni dwar is-sigurtà tal-informazzjoni

49. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu programm ta' taħriġ, inklużi programmi perjodiċi ta' sensibilizzazzjoni dwar is-sigurtà, għall-persunal u l-kuntratturi kollha sabiex jiżguraw li huma jkunu mħarrġa biex iwettqu d-dmirijiet u r-responsabbiltajiet tagħhom b'mod konsistenti mal-politiki u l-proċeduri ta' sigurtà rilevanti sabiex inaqqsu l-iżball uman, is-serq, il-frodi, l-użu ħażin jew it-telf u kif għandhom jindirizzaw riskji relatati mas-sigurtà tal-informazzjoni. L-istituzzjonijiet finanzjarji għandhom jiżguraw li l-programm ta' taħriġ jipprovdi taħriġ għall-membri kollha tal-persunal u l-kuntratturi tal-inqas kull sena.

1.5. Ġestjoni tal-operazzjonijiet tal-ICT

50. L-istituzzjonijiet finanzjarji għandhom jiġġestixxu l-operazzjonijiet tal-ICT tagħhom abbażi tal-proċessi u l-proċeduri dokumentati u implimentati (li, għall-PSPs, jinkludu d-dokument tal-politika tas-sigurtà skont l-Artikolu 5(1)(j) tal-PSD2) li huma approvati mill-korp ta' ġestjoni. Dan is-sett ta' dokumenti għandu jiddefinixxi kif l-istituzzjonijiet finanzjarji joperaw, jimmonitorjaw u jikkontrollaw is-sistemi u s-servizzi tal-ICT tagħhom, inkluża d-dokumentazzjoni ta' operazzjonijiet kritiċi tal-ICT, u għandhom jippermettu lill-istituzzjonijiet finanzjarji jżommu inventarju tal-assi tal-ICT aġġornat.

51. L-istituzzjonijiet finanzjarji għandhom jiżguraw li l-prestazzjoni tal-operazzjonijiet tal-ICT tagħhom tkun allinjata mar-rekwiżiti tan-negozju tagħhom. L-istituzzjonijiet finanzjarji għandhom iżommu u jtejbu, meta jkun possibbli, l-effiċjenza tal-operazzjonijiet tal-ICT tagħhom, inkluż iżda mhux limitat għall-ħtieġa li jiġi kkunsidrat kif jitnaqqsu kemm jista' jkun l-iżbalji potenzjali li jirriżultaw mit-twettiq ta' kompiti manwali.

52. L-istituzzjonijiet finanzjarji għandhom jimplimentaw proċeduri ta' reġistrazzjoni u monitoraġġ għal operazzjonijiet kritiċi tal-ICT biex ikunu jistgħu jiġu identifikati, analizzati u kkoreġuti l-iżbalji.

53. L-istituzzjonijiet finanzjarji għandhom iżommu inventarju aġġornat tal-assi tal-ICT tagħhom (inklużi sistemi tal-ICT, apparati tan-netwerk, bażijiet tad-*data*, eċċ.). L-inventarju tal-assi tal-ICT għandu jaħżen il-konfigurazzjoni tal-assi tal-ICT u l-konnessjonijiet u l-interdipendenzi bejn l-assi differenti tal-ICT, sabiex ikun jista' jsir proċess xieraq ta' konfigurazzjoni u ta' ġestjoni tat-tibdil.

54. L-inventarju tal-assi tal-ICT għandu jkun dettaljat biżżejjed biex jippermetti l-identifikazzjoni fil-pront ta' assi tal-ICT, is-sit tiegħu, il-klassifikazzjoni tas-sigurtà u s-sjieda. L-interdipendenzi bejn l-assi għandhom jiġu dokumentati biex jgħinu fir-rispons għal inċidenti ta' sigurtà u operazzjonali, inklużi l-attakki ċibernetiċi.

55. L-istituzzjonijiet finanzjarji għandhom jimmonitorjaw u jiġġestixxu ċ-ċikli tal-ħajja tal-assi tal-ICT, biex jiżguraw li jkomplu jissodisfaw u jappoġġaw ir-rekwiżiti tan-negozju u tal-ġestjoni tar-riskju. L-istituzzjonijiet finanzjarji għandhom jimmonitorjaw jekk l-assi tal-ICT tagħhom humiex appoġġati mill-bejjiegħa u mill-iżviluppaturi esterni jew interni tagħhom u jekk il-patches u l-aġġornamenti rilevanti kollha jiġux applikati abbażi ta' proċessi dokumentati. Ir-riskji li jirriżultaw minn assi tal-ICT skaduti jew mhux appoġġati għandhom jiġu vvalutati u mitigati.

56. L-istituzzjonijiet finanzjarji għandhom jimplimentaw proċessi ta' prestazzjoni u ta' ppjanar tal-kapaċità u ta' monitoraġġ biex jipprevjenu, jidentifikaw u jirrispondu għal problemi importanti ta' prestazzjoni tas-sistemi tal-ICT u ta' nuqqasijiet fil-kapaċità tal-ICT f'waqthom.

57. L-istituzzjonijiet finanzjarji għandhom jiddefinixxu u jimplimentaw *data* u proċeduri ta' backup u ta' rkupru tas-sistemi tal-ICT biex jiżguraw li dawn jistgħu jiġu rkuprati kif meħtieġ. Il-kamp ta' applikazzjoni u l-frekwenza ta' backup għandhom jiġu stabbiliti skont ir-rekwiżiti ta' rkupru tan-negozju u l-livell ta' kemm huma kritiċi d-*data* u s-sistemi tal-ICT u evalwati skont il-valutazzjoni tar-riskju mwettqa. L-ittestjar tal-proċeduri ta' backup u rkupru għandu jsir fuq bażi perjodika.

58. L-istituzzjonijiet finanzjarji għandhom jiżguraw li l-backups tad-*data* u tas-sistema tal-ICT jinħażnu b'mod sigur u jkunu remoti biżżejjed mis-sit primarju sabiex ma jkunux esposti għall-istess riskji.

3.5.1 Ġestjoni ta' inċidenti u problemi tal-ICT

59. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu u jimplimentaw proċess ta' ġestjoni ta' inċidenti u problemi biex jimmonitorjaw u jirreġistraw inċidenti operazzjonali u ta' sigurtà tal-ICT u biex jippermettu lill-istituzzjonijiet finanzjarji jkomplu jew jerġgħu jibdew, b'mod f'waqtu, funzjonijiet u proċessi tan-negozju kritiċi meta jkun hemm tfixkil. L-istituzzjonijiet finanzjarji għandhom jiddeterminaw il-kriterji u l-limiti xierqa għall-klassifikazzjoni ta' avvenimenti bħala inċidenti operazzjonali jew ta' sigurtà, kif stipulat fit-taqsima "Definizzjonijiet" ta' dawn il-linji gwida, kif ukoll indikaturi ta' twissija bikrija li jservu ta' allerti sabiex jippermettu l-identifikazzjoni bikrija ta' dawn l-inċidenti. Tali kriterji u livelli limitu, għall-PSPs, huma mingħajr preġudizzju għall-klassifikazzjoni ta' inċidenti kbar f'konformità mal-Artikolu 96 tal-PSD2 u l-Linji Gwida dwar ir-rapportar ta' inċidenti kbar taħt il-PSD2 (EBA/GL/2017/10).

60. Sabiex jiġi minimizzat l-impatt tal-avvenimenti avversi u jkun jista' jsir irkupru f'waqtu, l-istituzzjonijiet finanzjarji għandhom jistabbilixxu proċessi u strutturi organizzattivi xierqa biex jiżguraw monitoraġġ, indirizzar u segwitu konsistenti u integrati ta' inċidenti operazzjonali u ta' sigurtà u biex jiżguraw li l-kawżi ewlenin jiġu identifikati u eliminati biex tiġi evitata l-okkorrenza ta' inċidenti ripetuti. Il-proċess ta' ġestjoni ta' inċidenti u problemi għandu jistabbilixxi:

    a) il-proċeduri biex jiġu identifikati, intraċċati, reġistrati, kategorizzati u kklassifikati l-inċidenti skont il-livell ta' prijorità, abbażi ta' kemm huwa kritiku għan-negozju;
    b) ir-rwoli u r-responsabbiltajiet għal xenarji ta' inċidenti differenti (eż. żbalji, funzjonament ħażin, attakki ċibernetiċi);
    c) proċeduri ta' ġestjoni ta' problemi biex tiġi identifikata, analizzata u solvuta l-kawża ewlenija wara inċident wieħed jew aktar — istituzzjoni finanzjarja għandha tanalizza inċidenti operazzjonali jew ta' sigurtà li x'aktarx jaffettwaw lill-istituzzjoni finanzjarja li jkunu ġew identifikati jew li seħħew fi u/jew barra l-organizzazzjoni u għandha tqis it-tagħlimiet ewlenin minn dawn l-analiżijiet u taġġorna l-miżuri ta' sigurtà kif xieraq;
    d) pjanijiet ta' komunikazzjoni interna effettivi, inklużi notifiki ta' inċidenti u proċeduri ta' eskalazzjoni — li jkopru wkoll ilmenti ta' klijenti relatati mas-sigurtà — biex jiġi żgurat li:
        i) inċidenti b'impatt potenzjalment qawwi fuq sistemi kritiċi tal-ICT u servizzi tal-ICT jiġu rrapportati lill-maniġment superjuri rilevanti u lill-maniġment superjuri tal-ICT;
        ii) il-korp ta' ġestjoni jiġi infurmat fuq bażi ad hoc f'każ ta' inċidenti sinifikanti u, tal-inqas, infurmat dwar l-impatt, ir-rispons u l-kontrolli addizzjonali li għandhom jiġu definiti bħala riżultat tal-inċidenti.
    e) proċeduri ta' rispons għall-inċidenti biex jitnaqqsu l-impatti relatati mal-inċidenti u biex jiġi żgurat li s-servizz isir operattiv u sigur f'waqtu;
    f) pjanijiet ta' komunikazzjoni esterna speċifiċi għal funzjonijiet u proċessi tan-negozju kritiċi sabiex:

i) jikkollaboraw mal-partijiet ikkonċernati rilevanti biex jirrispondu b'mod effettiv għall-inċident u jirkupraw minnu;
ii) jipprovdu informazzjoni f'waqtha lil partijiet esterni (eż. klijenti, parteċipanti oħra fis-suq, l-awtorità superviżorja) kif xieraq u f'konformità ma' regolament applikabbli.

1.6. Ġestjoni tal-proġett tal-ICT u tat-tibdil

1.6.1. Ġestjoni tal-proġett tal-ICT

61. Istituzzjoni finanzjarja għandha timplimenta programm u/jew proċess ta' governanza ta' proġett li jiddefinixxi r-rwoli u r-responsabbiltajiet biex tiġi appoġġata b'mod effettiv l-implimentazzjoni tal-istrateġija tal-ICT.

62. Istituzzjoni finanzjarja għandha b'mod xieraq timmonitorja u timmitiga r-riskji li jirriżultaw mill-portafoll tagħhom ta' proġetti tal-ICT (ġestjoni tal-programm), filwaqt li tqis ukoll ir-riskji li jistgħu jirriżultaw minn interdipendenzi bejn proġetti differenti u minn dipendenzi ta' proġetti multipli fuq l-istess riżorsi u/jew għarfien espert.

63. Istituzzjoni finanzjarja għandha tistabbilixxi u timplimenta politika ta' ġestjoni ta' proġetti tal-ICT li tinkludi tal-inqas:

a) l-objettivi tal-proġett;
b) ir-rwoli u r-responsabbiltajiet;
c) valutazzjoni tar-riskju tal-proġett;
d) pjan, perjodu ta' żmien u passi ta' proġett;
e) stadji ewlenin;
f) rekwiżiti tal-ġestjoni tat-tibdil.

64. Il-politika tal-ġestjoni tal-proġetti tal-ICT għandha tiżgura li r-rekwiżiti tas-sigurtà tal-informazzjoni jiġu analizzati u approvati minn funzjoni li tkun indipendenti mill-funzjoni tal-iżvilupp.

65. Istituzzjoni finanzjarja għandha tiżgura li l-oqsma kollha milquta minn proġett tal-ICT ikunu rappreżentati fit-tim tal-proġett u li t-tim tal-proġett ikollu l-għarfien meħtieġ biex jiżgura implimentazzjoni tal-proġett sigura u ta' suċċess.

66. L-istabbiliment u l-progress ta' proġetti tal-ICT u r-riskji assoċjati magħhom għandhom jiġu rrapportati lill-korp ta' ġestjoni, b'mod individwali jew f'daqqa, skont l-importanza u d-daqs tal-proġetti tal-ICT, b'mod regolari u fuq bażi ad hoc kif xieraq. L-istituzzjonijiet finanzjarji għandhom jinkludu r-riskju tal-proġett fil-qafas tal-ġestjoni tar-riskji tagħhom.

1.6.2. Akkwist u żvilupp ta' sistemi tal-ICT

67. L-istituzzjonijiet finanzjarji għandhom jiżviluppaw u jimplimentaw proċess li jirregola l-akkwist, l-iżvilupp u l-manutenzjoni tas-sistemi tal-ICT. Dan il-proċess għandu jitfassal billi jintuża approċċ ibbażat fuq ir-riskju.

68. Istituzzjoni finanzjarja għandha tiżgura li, qabel ma jseħħ kwalunkwe akkwist jew żvilupp ta' sistemi tal-ICT, ir-rekwiżiti funzjonali u mhux funzjonali (inklużi r-rekwiżiti tas-sigurtà tal-informazzjoni) jiġu definiti b'mod ċar u approvati mill-maniġment tan-negozju rilevanti.

69. Istituzzjoni finanzjarja għandha tiżgura li jkunu fis-seħħ miżuri li jimmitigaw ir-riskju ta' alterazzjoni mhux intenzjonata jew manipulazzjoni intenzjonata tas-sistemi tal-ICT matul l-iżvilupp u l-implimentazzjoni fl-ambjent tal-produzzjoni.

70. L-istituzzjonijiet finanzjarji għandu jkollhom metodoloġija fis-seħħ għall-ittestjar u l-approvazzjoni tas-sistemi tal-ICT qabel ma jintużaw l-ewwel darba. Din il-metodoloġija għandha tikkunsidra kemm huma kritiċi l-proċessi u l-assi tan-negozju. L-ittestjar għandu jiżgura li sistemi ġodda tal-ICT jiffunzjonaw kif maħsub. Għandhom jużaw ukoll ambjenti ta' ttestjar li jirriflettu b'mod adegwat l-ambjent tal-produzzjoni.

71. L-istituzzjonijiet finanzjarji għandhom jittestjaw is-sistemi tal-ICT, is-servizzi tal-ICT u l-miżuri ta' sigurtà tal-informazzjoni biex jidentifikaw dgħufijiet fis-sigurtà, ksur u inċidenti relatati mas-sigurtà potenzjali.

72. Istituzzjoni finanzjarja għandha timplimenta ambjenti tal-ICT separati biex tiżgura segregazzjoni adegwata tad-dmirijiet u biex tnaqqas l-impatt ta' bidliet mhux verifikati għas-sistemi ta' produzzjoni. B'mod speċifiku, istituzzjoni finanzjarja għandha tiżgura s-segregazzjoni tal-ambjenti ta' produzzjoni minn ambjenti ta' żvilupp, ittestjar u li mhumiex ta' produzzjoni. Istituzzjoni finanzjarja għandha tiżgura l-integrità u l-kunfidenzjalità tad-*data* tal-produzzjoni f'ambjenti mhux tal-produzzjoni. L-aċċess għad-*data* tal-produzzjoni huwa ristrett għall-utenti awtorizzati.

73. L-istituzzjonijiet finanzjarji għandhom jimplimentaw miżuri biex jipproteġu l-integrità tal-kodiċijiet tas-sors tas-sistemi tal-ICT li huma żviluppati internament. Għandhom jiddokumentaw ukoll l-iżvilupp, l-implimentazzjoni, l-operat u/jew il-konfigurazzjoni tas-sistemi tal-ICT b'mod komprensiv biex titnaqqas kwalunkwe dipendenza mhux meħtieġa fuq l-esperti fis-suġġett. Id-dokumentazzjoni tas-sistema tal-ICT għandu jkun fiha, fejn applikabbli, tal-inqas id-dokumentazzjoni tal-utent, id-dokumentazzjoni tas-sistema teknika u l-proċeduri operattivi.

74. Il-proċessi ta' istituzzjoni finanzjarja għall-akkwist u l-iżvilupp ta' sistemi tal-ICT għandhom japplikaw ukoll għal sistemi tal-ICT żviluppati jew ġestiti minn utenti finali tal-funzjoni kummerċjali barra l-organizzazzjoni tal-ICT (eż. applikazzjonijiet tal-computing tal-utent finali) permezz ta' approċċ ibbażat fuq ir-riskju. L-istituzzjoni finanzjarja għandha żżomm reġistru ta' dawn l-applikazzjonijiet li jappoġġaw funzjonijiet jew proċessi tan-negozju kritiċi.

1.6.3. Ġestjoni tat-tibdil tal-ICT

75. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu u jimplimentaw proċess ta' ġestjoni tat-tibdil fl-ICT biex jiżguraw li l-bidliet kollha fis-sistemi tal-ICT jiġu rreġistrati, ittestjati, ivvalutati, approvati, implimentati u vverifikati b'mod ikkontrollat. L-istituzzjonijiet finanzjarji għandhom jittrattaw il-bidliet matul l-emerġenzi (jiġifieri bidliet li jridu jiġu introdotti malajr kemm jista' jkun) wara proċeduri li jipprovdu salvagwardji adegwati.

76. L-istituzzjonijiet finanzjarji għandhom jiddeterminaw jekk il-bidliet fl-ambjent operattiv eżistenti jinfluwenzawx il-miżuri ta' sigurtà eżistenti jew jirrikjedux l-adozzjoni ta' miżuri addizzjonali għall-mitigazzjoni tar-riskji involuti. Dawn il-bidliet għandhom ikunu skont il-proċess tal-ġestjoni tat-tibdil formali tal-istituzzjonijiet finanzjarji.

1.7. Ġestjoni tal-kontinwità tan-negozju

77. L-istituzzjonijiet finanzjarji għandhom jistabbilixxu proċess ta' ġestjoni tal-kontinwità tan-negozju (BCM) biex jimmassimizzaw il-kapaċitajiet tagħhom li jipprovdu servizzi fuq bażi kontinwa u jillimitaw it-telf fil-każ ta' tħarbit serju fl-attività f'konformità mal-Artikolu 85(2) tad-Direttiva 2013/36/UE u t-Titolu VI tal-Linji Gwida tal-EBA dwar il-governanza interna (EBA/GL/2017/11).

1.7.1. Analiżi tal-impatt tan-negozju

78. Bħala parti minn ġestjoni tal-kontinwità tan-negozju soda, l-istituzzjonijiet finanzjarji għandhom iwettqu analiżi tal-impatt tan-negozju (BIA) billi janalizzaw l-esponiment tagħhom għal tfixkil serju fl-attività u jivvalutaw l-impatti potenzjali tagħhom (inkluż dwar il-kunfidenzjalità, l-integrità u d-disponibbiltà), b'mod kwantitattiv u kwalitattiv, jużaw *data* interna u/jew esterna (eż. *data* ta' fornitur terz rilevanti għal proċess tan-negozju jew *data* disponibbli pubblikament li tista' tkun rilevanti għall-BIA) u analiżi tax-xenarji. Il-BIA għandha tikkunsidra wkoll kemm huma kritiċi l-funzjonijiet kummerċjali identifikati u kklassifikati, il-proċessi ta' appoġġ, il-partijiet terzi u l-assi ta' informazzjoni, u l-interdipendenzi tagħhom, skont it-Taqsima 1.3.3.

79. L-istituzzjonijiet finanzjarji għandhom jiżguraw li s-sistemi tal-ICT u s-servizzi tal-ICT tagħhom ikunu mfassla u allinjati mal-BIA tagħhom, pereżempju billi jitwarrbu ċerti komponenti kritiċi biex jiġi evitat it-tfixkil ikkawżat minn avvenimenti li jkollhom impatt fuq dawk il-komponenti.

1.7.2. Ippjanar għall-kontinwità tan-negozju

80. Abbażi tal-BIAs tagħhom, l-istituzzjonijiet finanzjarji għandhom jistabbilixxu pjanijiet biex jiżguraw il-kontinwità tan-negozju (pjanijiet ta' kontinwità tan-negozju, BCPs), li għandhom jiġu dokumentati u approvati mill-korpi ta' ġestjoni tagħhom. Il-pjanijiet għandhom jikkunsidraw b'mod speċifiku r-riskji li jista' jkollhom impatt negattiv fuq is-sistemi tal-ICT u s-servizzi tal-ICT. Il-pjanijiet għandhom jappoġġaw l-objettivi għall-protezzjoni, u jekk ikun meħtieġ, għall-istabbiliment mill-ġdid tal-kunfidenzjalità, l-integrità u d-disponibbiltà tal-funzjonijiet kummerċjali, il-proċessi ta' appoġġ u l-assi ta' informazzjoni tagħhom. L-istituzzjonijiet finanzjarji għandhom jikkoordinaw ma' partijiet ikkonċernati interni u esterni rilevanti, kif xieraq, matul l-istabbiliment ta' dawn il-pjanijiet.

81. L-istituzzjonijiet finanzjarji għandhom idaħħlu fis-seħħ BCPs biex jiżguraw li jkunu jistgħu jirreaġixxu b'mod xieraq għal xenarji potenzjali ta' falliment u li jkunu jistgħu jirkupraw l-operazzjonijiet tal-attivitajiet kummerċjali kritiċi tagħhom wara tfixkil fi ħdan objettiv tal-ħin ta' rkupru (RTO, iż-żmien massimu li fih sistema jew proċess bħal dan irid jiġi restawrat wara inċident) u objettiv ta' punt ta' rkupru (RPO, il-perjodu massimu ta' żmien li matulu jkun aċċettabbli li tintilef *data* f'każ ta' inċident). F'każijiet ta' tħarbit serju fl-attività li jiskatta

pjanijiet ta' kontinwità tan-negozju speċifiċi, l-istituzzjonijiet finanzjarji għandhom jagħtu prijorità lill-azzjonijiet ta' kontinwità tan-negozju li jużaw approċċ ibbażat fuq ir-riskju, li jista' jkun ibbażat fuq valutazzjonijiet tar-riskju mwettqa skont it-Taqsima 1.3.3. Għal PSPs dan jista' jinkludi, pereżempju, l-iffaċilitar tal-ipproċessar ulterjuri ta' tranżazzjonijiet kritiċi filwaqt li jkomplu l-isforzi ta' rimedju.

82. Istituzzjoni finanzjarja għandha tqis firxa ta' xenarji differenti fil-BCP tagħha, inklużi uħud estremi iżda plawżibbli li tista' tiġi esposta għalihom, inkluż xenarju ta' attakk ċibernetiku, u għandha tivvaluta l-impatt potenzjali li tali xenarji jista' jkollhom. Abbażi ta' dawn ix-xenarji, istituzzjoni finanzjarja għandha tiddeskrivi kif jiġu żgurati l-kontinwità tas-sistemi u s-servizzi tal-ICT, kif ukoll is-sigurtà tal-informazzjoni tal-istituzzjoni finanzjarja.

1.7.3. Pjanijiet ta' rispons u ta' rkupru

83. Abbażi tal-BIAs (paragrafu 78) u xenarji plawżibbli (paragrafu 82), l-istituzzjonijiet finanzjarji għandhom jiżviluppaw pjanijiet ta' rispons u ta' rkupru. Dawn il-pjanijiet għandhom jispeċifikaw liema kundizzjonijiet jistgħu jwasslu għall-attivazzjoni tal-pjanijiet u x'azzjonijiet għandhom jittieħdu biex jiżguraw id-disponibbiltà, il-kontinwità u l-irkupru ta', mill-inqas, is-sistemi tal-ICT u s-servizzi tal-ICT kritiċi tal-istituzzjonijiet finanzjarji. Il-pjanijiet ta' rispons u ta' rkupru għandu jkollhom l-għan li jilħqu l-objettivi ta' rkupru tal-operazzjonijiet tal-istituzzjonijiet finanzjarji.

84. Il-pjanijiet ta' rispons u ta' rkupru għandhom iqisu l-għażliet ta' rkupru kemm fuq terminu qasir kif ukoll fuq terminu twil. Il-pjanijiet għandhom:

    a) jiffukaw fuq l-irkupru tal-operazzjonijiet ta' funzjonijiet kummerċjali kritiċi, il-proċessi ta' appoġġ, l-assi ta' informazzjoni u l-interdipendenzi tagħhom biex jiġu evitati effetti negattivi fuq il-funzjonament tal-istituzzjonijiet finanzjarji u fuq is-sistema finanzjarja, inkluż fuq is-sistemi ta' pagament u fuq l-utenti ta' servizzi ta' pagament, u biex jiżguraw l-eżekuzzjoni tat-tranżazzjonijiet ta' pagament pendenti;

    b) jiġu dokumentati u jitqiegħdu għad-dispożizzjoni tan-negozji u l-unitajiet ta' appoġġ u jkunu aċċessibbli malajr f'każ ta' emerġenza;

    c) jiġu aġġornati f'konformità mat-tagħlimiet meħuda mill-inċidenti, it-testijiet, ir-riskji ġodda identifikati u t-theddid, u l-prijoritajiet u l-objettivi ta' rkupru mibdula.

85. Il-pjanijiet għandhom jikkunsidraw ukoll għażliet alternattivi fejn l-irkupru jista' ma jkunx prattiku fi żmien qasir minħabba l-ispejjeż, ir-riskji, il-loġistika jew ċirkostanzi mhux previsti.

86. Barra minn hekk, bħala parti mill-pjanijiet ta' rispons u ta' rkupru, istituzzjoni finanzjarja għandha tikkunsidra u timplimenta miżuri ta' kontinwità biex timmitiga n-nuqqasijiet ta' fornituri terzi, li huma ta' importanza ewlenija għall-kontinwità tas-servizz tal-ICT ta' istituzzjoni finanzjarja (f'konformità mad-dispożizzjonijiet tal-Linji Gwida tal-EBA dwar l-esternalizzazzjoni ta' arranġamenti (EBA/GL/2019/02) rigward il-pjanijiet ta' kontinwità tan-negozju).

1.7.4. Ittestjar tal-pjanijiet

87. Minn żmien għal żmien l-istituzzjonijiet finanzjarji għandhom jittestjaw il-BCPs tagħhom. B'mod partikolari, huma għandhom jiżguraw li l-BCPs tal-funzjonijiet kummerċjali kritiċi tagħhom, il-proċessi ta' appoġġ, l-assi ta' informazzjoni u l-interdipendenzi tagħhom (inklużi dawk ipprovduti minn partijiet terzi, fejn applikabbli) jiġu ttestjati mill-inqas kull sena, f'konformità mal-paragrafu 89.

88. Il-BCPs għandhom jiġu aġġornati mill-inqas kull sena, abbażi tar-riżultati tal-ittestjar, l-intelliġenza attwali dwar it-theddid u t-tagħlimiet li nstiltu mill-avvenimenti preċedenti. Kwalunkwe bidla fl-objettivi tal-irkupru (inklużi l-RTOs u l-RPOs) u/jew bidliet fil-funzjonijiet tan-negozju, proċessi ta' appoġġ u assi ta' informazzjoni, għandha tiġi kkunsidrata wkoll, fejn rilevanti, bħala bażi għall-aġġornament tal-BCPs.

89. L-ittestjar tal-BCPs tal-istituzzjonijiet finanzjarji għandu juri li dawn kapaċi jsostnu l-vijabbiltà tan-negozji tagħhom sakemm jiġu stabbiliti mill-ġdid l-operazzjonijiet kritiċi. B'mod partikolari, għandhom:

    a) jinkludu ttestjar ta' sett adegwat ta' xenarji serji iżda plawżibbli li jinkludu dawk meqjusa għall-iżvilupp tal-BCPs (kif ukoll l-ittestjar ta' servizzi fornuti minn partijiet terzi, fejn applikabbli); dan għandu jinkludi l-qlib tal-funzjonijiet kummerċjali kritiċi, proċessi ta' appoġġ u assi ta' informazzjoni għall-ambjent ta' rkupru minn diżastru u għandu juri li jistgħu jitħaddmu b'dan il-mod għal perjodu ta' żmien rappreżentattiv biżżejjed u li l-funzjonament normali jkun jista' jiġi rkuprat wara;
    b) jitfasslu biex jisfidaw il-preżunzjonijiet li jistrieħu fuqhom il-BCPs inklużi l-arranġamenti ta' governanza u l-pjanijiet ta' komunikazzjoni ta' kriżi; u
    c) jinkludu proċeduri li jivverifikaw l-abbiltà tal-persunal u l-kuntratturi tagħhom, is-sistemi tal-ICT u s-servizzi tal-ICT biex jirrispondu b'mod adegwat għax-xenarji definiti fil-paragrafu 89(a).

90. Ir-riżultati tat-test għandhom jiġu dokumentati u kwalunkwe nuqqas identifikat li jirriżulta mit-testijiet għandu jiġi analizzat, indirizzat u rrappurtat lill-korp ta' ġestjoni.

1.7.5. Komunikazzjonijiet f'sitwazzjoni ta' kriżi

91. F'każ ta' tħarbit jew emerġenza, u matul l-implimentazzjoni tal-BCPs, l-istituzzjonijiet finanzjarji għandhom jiżguraw li għandhom fis-seħħ miżuri ta' komunikazzjoni effettivi għal sitwazzjoni ta' kriżi sabiex il-partijiet ikkonċernati interni u esterni rilevanti kollha, inklużi l-awtoritajiet kompetenti meta meħtieġa minn regolamenti nazzjonali, u anki l-forniturі rilevanti (forniturі tal-esternalizzazzjoni, entitajiet fi grupp, jew forniturі terzi), jiġu infurmati fil-ħin u b'mod xieraq.

1.8. Ġestjoni tar-relazzjoni tal-utent ta’ servizzi ta’ pagament

92. Il-PSPs għandhom jistabbilixxu u jimplimentaw proċessi biex isaħħu l-għarfien tal-PSUs dwar ir-riskji tas-sigurtà marbuta mas-servizzi ta’ pagament billi jipprovdu assistenza u gwida lill-PSUs.

93. L-assistenza u l-gwida offruti lill-PSUs għandhom jiġu aġġornati fid-dawl ta’ theddid u vulnerabbiltajiet ġodda, u l-bidliet għandhom jiġu kkomunikati lill-PSU.

94. Meta l-funzjonalità tal-prodotti tkun tippermetti dan, il-PSPs għandhom jippermettu lill-PSUs biex jinvalidaw funzjonijiet ta’ pagament speċifiċi relatati mas-servizzi ta’ pagament offruti mill-PSP lill-PSU.

95. Meta, f’konformità mal-Artikolu 68(1) tad-Direttiva (UE) 2015/2366, PSP jaqbel mal-limiti tal-infiq tal-pagatur għat-tranżazzjonijiet ta’ pagament eżegwiti permezz ta’ strumenti ta’ pagament speċifiċi, il-PSP għandu jipprovdi lill-pagatur bl-għażla li jaġġusta dawn il-limiti sal-limitu massimu maqbul.

96. Il-PSPs għandhom jipprovdu lill-PSUs l-għażla li jirċievu allerti dwar tentattivi mibdija u/jew falluti sabiex jibdew it-tranżazzjonijiet ta’ pagament, li jippermettulhom jidentifikaw użu frodulenti jew malizzjuż tal-kontijiet tagħhom.

97. Il-PSPs għandhom iżommu lill-PSUs infurmati dwar l-aġġornamenti fil-proċeduri ta’ sigurtà li jaffettwaw lill-PSUs fir-rigward tal-forniment tas-servizzi ta’ pagament.

98. Il-PSPs għandhom jipprovdu lill-PSUs b'assistenza għall-mistoqsijiet, it-talbiet għall-appoġġ u n-notifiki ta’ anomaliji jew għall-kwistjonijiet fir-rigward ta’ affarijiet ta’ sigurtà relatati ma’ servizzi ta’ pagament kollha. Il-PSUs għandhom jiġu infurmati bix-xieraq dwar kif tista’ tinkiseb tali assistenza.