EBA/GL/2017/17

12/01/2018

Linji Gwida

dwar il-miżuri ta' sigurtà għar-riskji operazzjonali u ta' sigurtà tas-servizzi ta' pagament taħt id-Direttiva (UE) 2015/2366 (PSD2)

1. 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] . Skont l-Artikolu 16(3) tar-Regolament (UE) Nru 1093/2010, l-awtoritajiet kompetenti u l-istituzzjonijiet finanzjarji għandhom jagħmlu kull sforz possibbli biex jikkonformaw mal-linji gwida.

2. Il-linji gwida jipprovdu l-fehma tal-EBA dwar prattiki superviżorji xierqa fis-Sistema Ewropea ta' Superviżjoni Finanzjarja jew dwar kif il-liġi tal-Unjoni għandha tiġi applikata f'qasam partikolari. L-awtoritajiet kompetenti kif iddefiniti fl-Artikolu 4(2) tar-Regolament (UE) Nru 1093/2010 li għalihom japplikaw il-linji gwida għandhom jikkonformaw billi jinkorporawhom fil-prattiki superviżorji 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. B'konformità mal-Artikolu 16(3) tar-Regolament (UE) Nru 1093/2010, l-awtoritajiet kompetenti jridu jinnotifikaw lill-EBA dwar jekk jikkonformawx jew jekk hux beħsiebhom jikkonformaw ma' dawn il-linji gwida, jew inkella bir-raġunijiet għan-nuqqas ta' konformità, sa 12.03.2018 Fin-nuqqas ta' kwalunkwe notifika sa din l-iskadenza, l-awtoritajiet kompetenti jitqiesu mill-EBA li mhumiex konformi. In-notifiki għandhom jintbagħtu billi tiġi sottomessa l-formola disponibbli fuq is-sit web tal-ABE lil compliance@eba.europa.eubir-referenza 'EBA/GL/2017/17'. In-notifiki għandhom jiġu sottomessi minn persuni b'awtorità xierqa li jirrapportaw f'isem l-awtoritajiet kompetenti tagħhom. Kwalunkwe bidla fl-istat ta' konformità għandha tiġi rrapportata wkoll lill-EBA.

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

[1] Ir-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).

2. Suġġett, kamp ta' applikazzjoni u definizzjonijiet

Suġġett u kamp ta' applikazzjoni

5. Dawn il-linji gwida jissodisfaw il-mandat mogħti lill-EBA fl-Artikolu 95(3) tad-Direttiva (UE) 2015/2366[2] (PSD2).

6. Dawn il-Linji gwida jispeċifikaw ir-rekwiżiti għall-istabbiliment, l-implimentazzjoni u l-monitoraġġ tal-miżura ta' sigurtà li l-PSPs iridu jieħdu, f'konformità mal-Artikolu 95(1) tad-Direttiva (UE) 2015/2366, biex jimmaniġġjaw ir-riskji operazzjonali u ta' sigurtà fir-rigward tas-servizzi ta' pagament li jipprovdu.

Destinatarji

7. Dawn il-Linji gwida huma indirizzati lill-PSPs kif definit fl-Artikolu 4(11) tad-Direttiva (UE) 2015/2366 u kif imsemmi fid-definizzjoni ta' "istituzzjonijiet finanzjarji" fl-Artikolu 4(1) tar-Regolament (UE) 1093/2010 u lis-CAs kif definit fil-punt (i) tal-Artikolu 4(2) ta' dak ir-Regolament b'referenza għad-Direttiva 2007/64/KE[3] imħassra (bħalissa d-Direttiva (UE) 2015/2366[4]).

Definizzjonijiet

8. Sakemm ma jkunx speċifikat mod ieħor, it-termini użati u definiti fid-Direttiva (UE) 2015/2366 għandhom l-istess tifsira f'dawn il-Linji Gwida. Barra minn hekk, għall-finijiet ta' dawn il-Linji Gwida, għandhom japplikaw id-definizzjonijiet li ġejjin:

[2] Id-Direttiva (UE) 2015/2366 tal-Parlament Ewropew u tal-Kunsill tal-25 ta' Novembru 2015 dwar is-servizzi ta' pagament fis-suq intern, li temenda d-Direttivi 2002/65/KE, 2009/110/KE u 2013/36/UE u r-Regolament (UE) Nru 1093/2010, u li tħassar id-Direttiva 2007/64/KE (ĠU L 337, 23.12.2015, p. 35).

[3] Id-Direttiva 2007/64/KE tal-Parlament Ewropew u tal-Kunsill tat-13 ta' Novembru 2007 dwar is-servizzi ta' ħlas fis-suq intern li temenda d-Direttivi 97/7/KE, 2002/65/KE, 2005/60/KE u 2006/48/KE u li tħassar id-Direttiva 97/5/KE (ĠU L 319, 5.12.2007, p. 1).

[4] F'konformità mat-tieni subparagrafu tal-Artikolu 114 tad-Direttiva (UE) 2015/2366, kwalunkwe referenza għad-Direttiva 2007/64/KE imħassra għandha tiġi interpretata bħala referenza għad-Direttiva (UE) 2015/2366 u għandha tiġi interpretata f'konformità mat-tabella ta' korrelazzjoni fl-Anness II tad-Direttiva (UE) 2015/2366.

Korp maniġerjali	– Għall-PSPs li huma istituzzjonijiet tal-kreditu, dan it-terminu għandu l-istess tifsira tad-definizzjoni fil-punt (7) tal-Artikolu 3(1) tad-Direttiva 2013/36/UE[5]; – Għall-PSPs li huma istituzzjonijiet ta' pagament jew istituzzjonijiet ta' flus elettroniċi, dan it-terminu jfisser diretturi jew persuni responsabbli għall-immaniġġjar tal-PSP, u fejn rilevanti, persuni responsabbli għall-immaniġġjar tal-attivitajiet tas-servizzi ta' pagament tal-PSP; – 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 ta' sigurtà	Avveniment wieħed jew serje ta' avvenimenti marbutin mhux ippjanati mill-PSP li għandhom jew li probabbilment se jkollhom impatt negattiv fuq l-integrità, id-disponibbiltà, il-kunfidenzjalità, l-awtentiċità u/jew il-kontinwità tas-servizzi relatati mal-pagament.
Maniġment superjuri	(a) Għall-PSPs li huma istituzzjonijiet tal-kreditu, dan it-terminu għandu l-istess tifsira tad-definizzjoni fil-punt (9) tal-Artikolu 3(1) tad-Direttiva 2013/36/UE; (b) Għall-PSPs li huma istituzzjonijiet ta' pagament jew istituzzjonijiet ta' flus elettroniċi, dan it-terminu jfisser persuni fiżiċi li jeżerċitaw funzjonijiet eżekuttivi fi ħdan istituzzjoni u li jkunu responsabbli għall-immaniġġjar ta' kuljum tal-PSP, u marbuta li jagħtu rendikont ta' dan lill-korp maniġerjali; (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.
Riskju ta' sigurtà	Ir-riskju li jirriżulta minn proċessi interni inadegwati jew li ma rnexxewx jew avvenimenti esterni li għandhom jew li jista' jkollhom impatt negattiv fuq id-disponibbiltà, l-integrità, il-kunfidenzjalità ta' sistemi tat-teknoloġiji tal-informazzjoni u tal-komunikazzjoni (ICT) u/jew informazzjoni użati għall-forniment tas-servizzi ta' pagament. Dan jinkludi riskju minn attakki ċibernetiċi jew sigurtà fiżika inadegwata.
Predispożizzjoni għar-riskju	Il-livell aggregat u t-tipi ta' riskju li istituzzjoni hija lesta tassumi fil-kapaċità ta' riskju tagħha, f'konformità mal-mudell kummerċjali tagħha, biex tilħaq l-objettivi strateġiċi tagħha.

[5] Id-Direttiva 2013/36/UE tal-Parlament Ewropew u tal-Kunsill dwar l-aċċess għall-attività tal-istituzzjonijiet ta' kreditu u s-superviżjoni prudenzjali tal-istituzzjonijiet ta' kreditu u tad-ditti tal-investiment, li temenda d-Direttiva 2002/87/KE u li tħassar id-Direttivi 2006/48/KE u 2006/49/KE (ĠU L 176, 27.6.2013, p. 338).

3. Implimentazzjoni

Data tal-applikazzjoni

9. Dawn il-Linji Gwida jibdew japplikaw mit-13 ta' Jannar 2018.

4. Linji Gwida

Linja Gwida 1: Prinċipju ġenerali

1.1 Il-PSPs kollha għandhom jikkonformaw mad-dispożizzjonijiet kollha stipulati f'dawn il-Linji gwida. Il-livell ta' dettall għandu jkun proporzjonali għad-daqs tal-PSP u għan-natura, il-kamp ta' applikazzjoni, il-kumplessità u r-riskju tas-servizzi partikolari li l-PSP jipprovdi jew li beħsiebu jipprovdi.

Linja Gwida 2: Governanza

Qafas tal-immaniġġjar tar-riskju operazzjonali u ta' sigurtà

2.1 Il-PSPs għandhom jistabbilixxu qafas tal-immaniġġjar tar-riskju operazzjonali u ta' sigurtà (minn issa 'l quddiem "qafas tal-immaniġġjar tar-riskju"), li għandu jiġi approvat u eżaminat, mill-anqas darba f'sena, mill-korp maniġerjali, u meta rilevanti, mill-maniġment superjuri. Dan il-qafas għandu jiffoka fuq il-miżuri ta' sigurtà sabiex itaffi r-riskji operazzjonali u ta' sigurtà u għandu jiġi integrat bis-sħiħ fil-proċessi tal-immaniġġjar tar-riskju globali tal-PSP.

2.2 Il-qafas tal-immaniġġjar tar-riskju għandu:

a) jinkludi dokument ta' politika ta' sigurtà komprensiv kif imsemmi fl-Artikolu 5(1)(j) tad-Direttiva (UE) 2015/2366;

b) ikun konsistenti mal-predispożizzjoni għar-riskju tal-PSP;

c) jiddefinixxi u jassenja rwoli u responsabbiltajiet ewlenin kif ukoll il-linji ta' rapportar rilevanti meħtieġa għall-infurzar tal-miżuri ta' sigurtà u għall-immaniġġjar tar-riskji operazzjonali u ta' sigurtà;

d) jistabbilixxi l-proċeduri u s-sistemi meħtieġa għall-identifikazzjoni, il-kejl, il-monitoraġġ u l-immaniġġjar tal-firxa ta' riskji li jirriżultaw mill-attivitajiet relatati mal-pagament tal-PSP u li għalihom huwa espost il-PSP, inklużi arranġamenti dwar il-kontinwità tan-negozju.

2.3 Il-PSPs għandhom jiżguraw li l-qafas tal-immaniġġjar tar-riskju jiġi ddokumentat kif xieraq, u aġġornat b'"tagħlimiet mitgħallma" ddokumentati matul l-implimentazzjoni u l-monitoraġġ tiegħu.

2.4 Il-PSPs għandhom jiżguraw li qabel issir bidla radikali fl-infrastruttura, fil-proċessi jew fil-proċeduri u wara kull inċident operazzjonali jew ta' sigurtà li jaffettwa s-sigurtà tas-servizzi ta' pagament li jipprovdu, huma jeżaminaw jekk il-bidliet jew it-titjib fil-qafas tal-immaniġġjar tar-riskju humiex meħtieġa mingħajr dewmien żejjed jew le.

Mudelli tal-immaniġġjar tar-riskju u ta' kontroll

2.5 Il-PSPs għandhom jistabbilixu linji ta' difiża effettivi, jew mudell tal-immaniġġjar tar-riskju u l-kontroll intern ekwivalenti, sabiex jidentifikaw u jimmaniġġjaw riskji operazzjonali u ta' sigurtà. Il-PSPs għandhom jiżguraw li l-mudell ta' kontroll intern li ssemma' qabel ikollu biżżejjed awtorità, indipendenza, riżorsi u linji ta' rappurtar dirett għall-korp maniġerjali, u meta rilevanti, għall-maniġment superjuri.

2.6 Il-miżuri ta' sigurtà stipulati f'dawn il-Linji gwida għandhom jiġu awditjati minn awdituri b'għarfien espert fis-sigurtà tal-IT u l-pagamenti u li joperaw b'mod indipendenti fi ħdan il-PSP jew minnu. Il-frekwenza u l-enfasi ta' tali awditi għandha tqis ir-riskji ta' sigurtà korrispondenti.

Esternalizzazzjoni

2.7 Il-PSPs għandhom jiżguraw l-effettività tal-miżuri ta' sigurtà stipulati f'dawn il-Linji gwida meta l-funzjonijiet operazzjonali tas-servizzi ta' pagament, inkluż is-sistemi tal-IT, jiġu esternalizzati.

2.8 Il-PSPs għandhom jiżguraw li fil-kuntratti u l-ftehimiet dwar il-livell ta' servizz mal-forniturі li lilhom ikunu esternalizzaw tali funzjonijiet jiġu inklużi l-objettivi, il-miżuri u l-miri ta' prestazzjoni ta' sigurtà xierqa u proporzjonati. Il-PSPs 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.

Linja Gwida 3: Valutazzjoni tar-riskju

Identifikazzjoni ta' funzjonijiet, proċessi u assi

3.1 Il-PSPs għandhom jidentifikaw, jistabbilixxu u jaġġornaw b'mod regolari inventarju tal-funzjonijiet tan-negozju, ir-rwoli ewlenin u l-proċessi ta' appoġġ tagħhom sabiex jimmappjaw l-importanza ta' kull funzjoni, rwol u proċess ta' appoġġ, u l-interdipendenzi tagħhom relatati mar-riskji operazzjonali u ta' sigurtà.

3.2 Il-PSPs għandhom jidentifikaw, jistabbilixxu u jaġġornaw b'mod regolari inventarju ta' assi ta' informazzjoni, bħal sistemi tal-ICT, il-konfigurazzjonijiet tagħhom, infrastrutturi oħrajn kif ukoll l-interkonnessjonijiet ma' sistemi interni u esterni oħra sabiex ikunu kapaċi jimmaniġġjaw l-assi li jappoġġaw il-funzjonijiet u l-proċessi ta' negozju kritiċi tagħhom.

Klassifikazzjoni ta' funzjonijiet, proċessi u assi

3.3 Il-PSPs għandhom jikklassifikaw il-funzjonijiet ta' negozju, il-proċessi ta' appoġġ u l-assi ta' informazzjoni identifikati f'termini ta' kritikalità.

Valutazzjonijiet tar-riskju ta' funzjonijiet, proċessi u assi

3.4 Il-PSPs għandhom jiżguraw li huma jkomplu jimmonitorjaw it-theddid u l-vulnerabbiltajiet u jeżaminaw b'mod regolari x-xenarji ta' riskju li jolqtu l-funzjonijiet ta' negozju, il-proċessi kritiċi u l-assi ta' informazzjoni tagħhom. Bħala parti mill-obbligu li jikkontrollaw u jipprovdu CAs

b'valutazzjoni tar-riskju aġġornata u komprensiva tar-riskji operazzjonali u ta' sigurtà fir-rigward tas-servizzi ta' pagament li jipprovdu u dwar l-adegwatezza tal-miżuri ta' mitigazzjoni u l-mekkaniżmi ta' kontroll implimentati bħala reazzjoni għal dawn ir-riskji, kif stipulat fl-Artikolu 95(2) tad-Direttiva 2015/2366, il-PSPs għandhom iwettqu u jiddokumentaw valutazzjonijiet tar-riskju, mill-anqas darba fis-sena jew f'intervalli iqsar kif iddeterminat mis-CA, tal-funzjonijiet, il-proċessi u l-assi ta' informazzjoni li jkunu identifikaw u kklassifikaw sabiex jidentifikaw u jivvalutaw ir-riskji operazzjonali u ta' sigurtà ewlenin. Tali valutazzjonijiet tar-riskju għandhom isiru qabel isseħħ xi bidla radikali fl-infrastruttura, fil-proċessi jew fil-proċeduri li taffettwa s-sigurtà tas-servizzi ta' pagament.

3.5 Abbażi tal-valutazzjonijiet tar-riskju, il-PSPs għandhom jiddeterminaw jekk il-bidliet humiex meħtieġa u sa fejn, għall-miżuri ta' sigurtà eżistenti, it-teknoloġiji użati u l-proċeduri jew is-servizzi ta' pagament offruti. Il-PSPs għandhom iqisu ż-żmien meħtieġ għall-implimentazzjoni tal-bidliet u ż-żmien għat-teħid ta' miżuri ta' sigurtà *interim* sabiex jiġu minimizzati l-inċidenti operazzjonali u ta' sigurtà, il-frodi u l-effetti problematiċi potenzjali fil-forniment tas-servizzi ta' pagament.

Linja Gwida 4: Protezzjoni

4.1 Il-PSPs għandhom jistabbilixxu u jimplimentaw miżuri ta' sigurtà preventivi kontra r-riskji operazzjonali u ta' sigurtà identifikati. Dawn il-miżuri għandhom jiżguraw livell ta' sigurtà adegwat f'konformità mar-riskji identifikati.

4.2 Il-PSPs għandhom jistabbilixxu u jimplimentaw approċċ ta "difiża profonda" billi jistabbilixxu kontrolli ta' saffi multipli li jkopru lin-nies, lill-proċessi u lit-teknoloġija, b'kull saff iservi ta' xibka ta' sikurezza għal saffi preċedenti. Id-difiża profonda għandha tinftiehem bħala difiża li ddefinixxiet aktar minn kontroll wieħed li jkopri l-istess riskju, bħall-prinċipju ta' erba' għajnejn aħjar minn tnejn, l-awtentikazzjoni ta' żewġ fatturi, is-segmentazzjoni tan-netwerk u firewalls multipli.

4.3 Il-PSPs għandhom jiżguraw il-kunfidenzjalità, l-integrità u d-disponibbiltà tal-assi fiżiċi u loġiċi kritiċi tagħhom, ir-riżorsi u d-data sensittiva dwar pagamenti tal-PSUs tagħhom kemm jekk dawn mhux qed jintużaw, jekk qegħdin fi tranżitu jew qed jintużaw. Jekk id-data tkun tinkludi data personali, tali miżuri għandhom jiġu implimentati f'konformità mar-Regolament (UE) 2016/679[6] jew, jekk applikabbli, ir-Regolament (KE) 45/2001.[7]

4.4 Il-PSPs, fuq bażi kontinwa, għandhom jiddeterminaw jekk il-bidliet fl-ambjent operattiv eżistenti jinfluwenzawx il-miżuri ta' sigurtà eżistenti jew jeħtiġux l-adozzjoni ta' miżuri ulterjuri għall-mitigazzjoni tar-riskju involut. Dawn il-bidliet għandhom ikunu parti mill-proċess ta' mmaniġġjar ta' bidla formali tal-PSP, li għandu jiżgura li l-bidliet jiġu ppjanati, ittestjati, iddokumentati u

[6] Ir-Regolament (UE) tal-Parlament Ewropew u tal-Kunsill tas-27 ta' April 2016 dwar il-protezzjoni tal-persuni fiżiċi fir-rigward tal-ipproċessar ta' data personali u dwar il-moviment liberu ta' tali data, u li jħassar id-Direttiva 95/46/KE (Regolament Ġenerali dwar il-Protezzjoni tad-Data) (ĠU L 119, 4.5.2016, p. 1).

[7] Ir-Regolament (KE) Nru 45/2001 tal-Parlament Ewropew u tal-Kunsill tat-18 ta' Diċembru 2000 dwar il-protezzjoni ta' individwu fir-rigward tal-ipproċessar ta' data personali mill-istituzzjonijiet u l-korpi tal-Komunità u dwar il-movement liberu ta' dik id-data (ĠU L 8, 12.1.2001, p. 1).

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

4.5 Fl-iddisinjar, l-iżvilupp u l-forniment tas-servizzi ta' pagament, il-PSPs għandhom jiżguraw li jiġu applikati l-prinċipji tas-segregazzjoni tad-dmirijiet u tal-"anqas privileġġ". Il-PSPs għandhom jagħtu attenzjoni speċjali lis-segregazzjoni tal-ambjenti tal-IT, b'mod partikolari l-ambjenti tal-iżvilupp, tal-ittestjar u tal-produzzjoni.

Integrità u kunfidenzjalità tad-data u s-sistemi

4.6 Fl-iddisinjar, l-iżvilupp u l-forniment tas-servizzi ta' pagament, il-PSPs għandhom jiżguraw li l-ġbir, ir-rotot, l-ipproċessar, il-ħżin u/jew l-arkivjar u l-viżwalizzazzjoni ta' data sensittiva dwar pagamenti tal-PSU jkunu adegwati, rilevanti u limitati għal dak li hu meħtieġ għall-forniment tas-servizzi ta' pagament tiegħu.

4.7 Il-PSPs għandhom jivverifikaw b'mod regolari jekk is-softwer użat għall-forniment tas-servizzi ta' pagament, inkluż is-softwer relatat mal-pagament tal-utenti, ikunx aġġornat u li jintużaw il-patches ta' sigurtà kritiċi. Il-PSPs għandhom jiżguraw li l-mekkaniżmi ta' verifika tal-integrità jkunu qed joperaw sabiex jivverifikaw l-integrità tas-softwer, il-firmware u l-informazzjoni dwar is-servizzi ta' pagament tagħhom.

Sigurtà fiżika

4.8 Il-PSPs għandu jkollhom implimentati miżuri ta' sigurtà fiżika xierqa, b'mod partikolari sabiex jipproteġu d-data sensittiva dwar pagamenti tal-PSUs kif ukoll is-sistemi tal-ICT użati biex jipprovdu servizzi ta' pagament.

Kontroll tal-aċċess

4.9 L-aċċess fiżiku u loġiku għas-sistemi tal-ICT għandu jkun permess biss għal individwi awtorizzati. L-awtorizzazzjoni għandha tkun assenjata f'konformità mal-kompiti u r-responsabbiltajiet tal-persunal, u tkun limitata għal individwi li jiġu mħarrġa u mmonitorjati kif xieraq. Il-PSPs għandhom jistabbilixxu kontrolli li jillimitaw b'mod affidabbli tali aċċess għal sistemi tal-ICT għal dawk b'rekwiżit ta' negozju leġittimu. L-aċċess elettroniku permezz ta' applikazzjonijiet għad-data u s-sistemi għandu jkun limitat għall-miminu meħtieġ għall-forniment tas-servizz rilevanti.

4.10 Il-PSPs għandhom jistabbilixxu kontrolli b'saħħithom fuq l-aċċess privileġġat għas-sistema billi jillimitaw b'mod strett u jimmonitorjaw mill-qrib il-persunal b'intitolamenti ta' aċċess tas-sistema għoljin. Għandhom jiġu implimentati kontrolli bħal aċċess ibbażat fuq ir-rwoli, l-illoggjar u l-eżami tal-attivitajiet ta' sistemi ta' utenti privileġġati, l-awtentikazzjoni b'saħħitha u l-monitoraġġ għal anomaliji. Il-PSPs għandhom jikkontrollaw id-drittijiet ta' aċċess għall-assi ta' informazzjoni u s-sistemi ta' appoġġ tagħhom abbażi tal-ħtieġa ta' tagħrif.Id-drittijiet għall-aċċess għandhom jiġu eżaminati fuq livell perjodiku.

4.11 Il-logs tal-aċċess għandhom jinżammu għal perjodu li jikkorrispondi mal-kritikalità tal-funzjonijiet ta' negozju, il-proċessi ta' appoġġ u l-assi ta' informazzjoni identifikati, f'konformità ma' GL 3.1 u GL 3.2, mingħajr ħsara għar-rekwiżiti ta' ritenzjoni stipulati fil-liġi nazzjonali u tal-UE.Il-PSPs għandhom jużaw din l-informazzjoni biex jiffaċilitaw l-identifikazzjoni u l-investigazzjoni ta' attivitajiet anomali li jkunu ġew identifikati fil-forniment tas-servizzi ta' pagament.

4.12 Sabiex tiġi żgurata komunikazzjoni sigura u jitnaqqas ir-riskju, l-aċċess amministrattiv mill-bogħod għal komponenti tal-ICT kritiċi għandu jingħata biss abbażi ta' ħtieġa ta' tagħrif u meta jintużaw soluzzjonijiet ta' awtentikazzjoni b'saħħithom.

4.13 L-operazzjoni ta' prodotti, għodod u proċeduri relatati mal-proċessi tal-kontroll tal-aċċess għandha tipproteġi l-proċessi tal-kontroll tal-aċċess milli dawn jiġu mdgħajfa jew megħluba. Din tinkludi r-reġistrazzjoni, il-kunsinna, ir-revoka u l-irtirar ta' prodotti, għodod u proċeduri korrispondenti.

Linja Gwida 5: Identifikazzjoni

Monitoraġġ u identifikazzjoni kontinwa

5.1 Il-PSPs għandhom jistabbilixxu u jimplimentaw proċessi u kapaċitajiet sabiex jimmonitorjaw il-funzjonijiet ta' negozju, il-proċessi ta' appoġġ u l-assi ta' informazzjoni b'mod kontinwu sabiex jidentifikaw attivitajiet anomali fil-provvista tas-servizzi ta' pagament. Bħala parti minn dan il-monitoraġġ kontinwu, il-PSPs għandu jkollhom implimentati kapaċitajiet xierqa u effettivi għall-identifikazzjoni ta' intrużjoni fiżika jew loġika kif ukoll ksur tal-kunfidenzjalità, l-integrità u d-disponibbiltà tal-assi ta' informazzjoni użati fil-forniment tas-servizzi ta' pagament.

5.2 Il-proċessi ta' monitoraġġ u identifikazzjoni kontinwi għandhom ikopru:

a) fatturi interni u esterni rilevanti, inkluż funzjonijiet amministrattivi tan-negozju u tal-ICT;

b) tranżazzjonijiet sabiex jiġi identifikat l-użu ħażin tal-aċċess mill-fornituri tas-servizzi jew entitajiet oħra; u

c) theddid intern u estern potenzjali.

5.3 Il-PSPs għandhom jimplimentaw miżuri ta' identifikazzjoni sabiex jidentifikaw kxif possibbli ta' informazzjoni, kodifikazzjoni malizzjuża u theddid għas-sigurtà ieħor, u vulnerabbiltajiet magħrufa mill-pubbliku għas-softwer u l-ħardwer, u għandhom jiċċekkjaw għal aġġornamenti tas-sigurtà ġodda korrispondenti.

Monitoraġġ u rappurtar ta' inċidenti operazzjonali jew ta' sigurtà

5.4 Il-PSPs għandhom jiddeterminaw il-kriterji u l-limiti xierqa għall-klassifikazzjoni ta' avveniment bħala inċident operazzjonali jew ta' sigurtà, kif stipulat fit-taqsima "Definizzjonijiet" ta' dawn il-Linji gwida, kif ukoll bħala indikaturi ta' twissija bikrija li jservu ta' allerta għall-PSP sabiex jippermettu l-identifikazzjoni bikrija ta' inċidenti operazzjonali jew ta' sigurtà.

5.5 Il-PSPs għandhom jistabbilixxu proċessi u strutturi organizzazzjonali xierqa sabiex jiżguraw il-monitoraġġ konsistenti u integrat, it-trattament u s-segwitu ta' inċidenti operazzjonali jew ta' sigurtà.

5.6 Il-PSPs għandhom jistabbilixxu proċedura għar-rapportar ta' tali inċidenti operazzjonali jew ta' sigurtà kif ukoll ta' lmenti tal-konsumaturi relatati mas-sigurtà lill-maniġment superjuri tagħhom.

Linja Gwida 6: Kontinwità tan-negozju

6.1 Il-PSPs għandhom jistabbilixxu mmaniġġjar tal-kontinwità tan-negozju b'saħħtu sabiex isaħħu kemm jista' jkun il-kapaċità tagħhom li jipprovdu servizzi ta' pagament fuq bażi kontinwa u li jillimitaw it-telf f'każ ta' tqallib tal-operat kbir.

6.2 Sabiex jistabbilixxu mmaniġġjar tal-kontinwità tan-negozju b'saħħtu, il-PSPs għandhom janalizzaw bir-reqqa l-esponiment tagħhom għal taqlib kbir fl-operat, u (b'mod kwantitattiv u kwalitattiv) jivvalutaw l-impatt potenzjali tiegħu, billi jagħmlu użu minn data interna u/jew esterna u analiżi tax-xenarji. Abbażi tal-funzjonijiet, is-sistemi, it-tranżazzjonijiet u l-interdipendenzi kritiċi identifikati u kklassifikati f'konformità ma' GL 3.1 u GL 3.3, il-PSPs għandhom jagħtu prijorità lill-azzjonijiet ta' kontinwità tan-negozji bl-użu ta' approċċ b'bażi ta' riskju, li jista' jkun ibbażat fuq il-valutazzjonijiet tar-riskju mwettqa taħt GL 3. Skont il-mudell tan-negozju tal-PSP, dan jista', pereżempju jiffaċilita l-ipproċessar ulterjuri ta' tranżazzjonijiet kritiċi waqt li l-isforzi ta' rimedju jkomplu.

6.3 Abbażi tal-analiżi mwettqa taħt GL 6.2, PSP għandu jimplimenta:

a) BCPs biex jiżgura li jista' jirreaġixxi kif xieraq għall-emerġenzi u jkun kapaċi jmantni l-attivitajiet ta' negozju kritiċi tiegħu; u

b) miżuri ta' mitigazzjoni li għandhom jiġu adottati fil-każ li s-servizzi ta' pagament u l-kuntratti eżistenti tiegħu jiġu tterminati, sabiex jevita effetti negattivi fuq is-sistemi ta' pagament u fuq il-PSUs u biex jiżgura l-eżekuzzjoni ta' tranżazzjonijiet ta' pagament pendenti.

Ippjanar ta' kontinwità tan-negozju bbażat fuq ix-xenarju

6.4 Il-PSP għandu jqis firxa ta' xenarji differenti, inklużi uħud estremi iżda plawsibbli, li fihom jista' jiġi espost, u jivvaluta l-impatt potenzjali li tali xenarji jista' jkollhom.

6.5 Abbażi tal-analiżi mwettqa taħt GL 6.2 u x-xenarji plawsibbli identifikati taħt GL 6.4, il-PSP għandu jiżviluppa pjanijiet ta' reazzjoni u ta' rkupru, li għandhom:

a) jiffukaw fuq l-impatt fuq l-operazzjoni tal-funzjonijiet, il-proċessi, is-sistemi, it-tranżazzjonijiet u l-interdipendenzi kritiċi;

b) jiġu ddokumentati u jkunu disponibbli għan-negozji u l-unitajiet ta' appoġġ u jkunu aċċessibbli malajr f'każ ta' emerġenza, u

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

Ittestjar tal-pjanijiet ta' kontinwità tan-negozju

6.6 Il-PSPs għandhom jittestaw il-BCPs tagħhom, u jiżguraw li l-operat tal-funzjonijiet, il-proċessi, is-sistemi u l-interdipendenzi kritiċi jiġi ttestjat mill-anqas fuq bażi annwali. Il-pjanijiet għandhom jappoġġaw l-objettivi għall-protezzjoni, u jekk ikun meħtieġ, għall-istabbiliment mill-ġdid tal-integrità u d-disponibbiltà tal-operazzjonijiet tagħhom, u l-kunfidenzjalità tal-assi ta' informazzjoni tagħhom.

6.7 Il-pjanijiet għandhom jiġu aġġornati mill-anqas fuq bażi annwali, abbażi tar-riżultati tal-ittestjar, l-intelliġenza tat-theddid attwali, il-kondiviżjoni tal-informazzjoni u t-tagħlimiet mitgħallma minn avvenimenti preċedenti, u l-objettivi ta' rkupru li qed jinbidlu, kif ukoll fuq l-analiżi ta' xenarji operazzjonalment u teknikament plawsibbli li għadhom ma seħħewx, u, jekk rilevanti, wara bidliet fis-sistemi u l-proċessi. Il-PSPs għandhom jikkonsultaw u jikkoordinaw mal-partijiet ikkonċernati interni u esterni rilevanti matul l-istabbiliment tal-BCPs tagħhom.

6.8 L-ittestjar tal-PSPs tal-BCPs tagħhom għandu:

a) jinkludi sett ta' xenarji adegwat, kif imsemmi f'GL 6.4;

b) jiġi ddisinjat biex jisfida l-preżunzjonijiet li jistrieħu fuqhom il-BCPs inklużi l-arranġamenti ta' governanza u l-pjanijiet ta' komunikazzjoni ta' kriżi; u

c) jinkludi proċeduri għall-verifika tal-abbiltà tal-persunal tagħhom u proċessi għal reazzjoni adegwata għax-xenarji ta' hawn fuq.

6.9 Il-PSPs għandhom jimmonitorjaw b'mod perjodiku l-effettività tal-BCPs tagħhom, u jiddokumentaw u janalizzaw kwalunkwe sfida jew falliment li jirriżulta mit-testijiet.

Komunikazzjoni ta' kriżi

6.10 F'każ ta' taqlib jew emerġenza, u matul l-implimentazzjoni tal-BCPs, il-PSPs għandhom jiżguraw li għandhom implimentati miżuri ta' komunikazzjoni tal-kriżi effettivi sabiex il-partijiet ikkonċernati interni u esterni rilevanti kollha, inkluż il-forniturі tas-servizzi esterni, jiġu infurmati fil-ħin u b'mod xieraq.

Linja Gwida 7: Ittestjar ta' miżuri ta' sigurtà

7.1 Il-PSPs għandhom jistabbilixxu u jimplimentaw qafas tal-ittestjar li jivvalida l-qawwa u l-effettività tal-miżuri ta' sigurtà u jiżguraw li l-qafas tal-ittestjar jiġi adattat sabiex jitqiesu theddid u vulnerabbiltajiet ġodda, li jiġu identifikati permezz tal-attivitajiet ta' monitoraġġ tar-riskju.

7.2 Il-PSPs għandhom jiżguraw li, f'każ ta' bidliet fl-infrastruttura, fil-proċessi jew fil-proċeduri u f'każ ta' bidliet bħala konsegwenza ta' inċidenti operazzjonali jew ta' sigurtà ewlenin, jitwettqu testijiet.

7.3 Il-qafas tal-ittestjar għandu jinkorpora wkoll il-miżuri ta' sigurtà rilevanti għal (i) terminals u apparati ta' pagament użati għall-forniment tas-servizzi ta' pagament, (ii) terminals u apparati ta' pagament użati għall-awtentikazzjoni tal-PSU u (iii) apparati u softwer ipprovduti mill-PSP lill-PSU għall-ġenerazzjoni/riċezzjoni ta' kodiċi ta' awtentikazzjoni.

7.4 Il-qafas tal-ittestjar għandu jiżgura li t-testijiet:

a) jitwettqu bħala parti mill-proċess ta' mmaniġġjar ta' bidla formali tal-PSP sabiex tiġi żgurata l-qawwa u l-effettività tagħhom;

b) jitwettqu minn testers indipendenti li għandhom għarfien, ħiliet u ħila esperta suffiċjenti fl-ittestjar tal-miżuri ta' sigurtà tas-servizzi ta' pagament u li ma jkunux involuti fl-iżvilupp tal-miżuri ta' sigurtà għas-servizzi jew għas-sistemi ta' pagament korrispondenti li għandhom jiġu ttestjati, għallinqas għat-testijiet finali qabel ma jiġu implimentati l-miżuri ta' sigurtà; u

c) jinkludu skens tal-vulnerabbilità u testijiet tal-penetrazzjoni adegwati għal-livell ta' riskju identifikat fi ħdan is-servizzi ta' pagament.

7.5 Il-PSPs għandhom iwettqu testijiet kontinwi u ripetuti tal-miżuri tas-sigurtà għas-servizzi ta' pagament tagħhom. Fil-każ ta' sistemi li huma kritiċi għall-forniment tas-servizzi ta' pagament tagħhom (kif deskritt f'GL 3.2), dawn it-testijiet għandhom jitwettqu mill-anqas fuq bażi annwali. Sistemi li mhumiex kritiċi għandhom jiġu ttestjati b'mod regolari bl-użu ta' approċċ ibbażat fuq ir-riskju, iżda mill-anqas kull tliet snin.

7.6 Il-PSPs għandhom jimmonitorjaw u jevalwaw ir-riżultati tat-testijiet imwettqa, u jaġġornaw il-miżuri ta' sigurtà tagħhom kif xieraq u mingħajr dewmien żejjed fil-każ ta' sistemi kritiċi.

Linja Gwida 8: Għarfien tas-sitwazzjoni u tagħlim kontinwu

Xenarju ta' theddid u għarfien tas-sitwazzjoni

8.1 Il-PSPs għandhom jistabbilixxu u jimplimentaw proċessi u strutturi organizzazzjonali sabiex jidentifikaw u jimmonitorjaw b'mod kostanti t-theddid operazzjonali u ta' sigurtà li jista' jaffettwa fuq livell materjali l-abbiltà tagħhom li jipprovdu servizzi ta' pagament.

8.2 Il-PSPs għandhom janalizzaw l-inċidenti operazzjonali jew ta' sigurtà li jkunu ġew identifikati jew li jkunu seħħew fl-organizzazzjoni jew lil hinn minnha. Il-PSPs għandhom iqisu t-tagħlimiet mitgħallma ewlenin minn dawn l-analiżi u jaġġornaw il-miżuri ta' sigurtà skont dan.

8.3 Il-PSPs għandhom jimmonitorjaw l-iżviluppi teknoloġiċi b'mod attiv sabiex jiżguraw li huma konxji tar-riskji ta' sigurtà.

Programmi ta' taħriġ u ta' għarfien tas-sigurtà

8.4 Il-PSPs għandhom jistabbilixxu programm ta' taħriġ għall-persunal kollu 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. Il-PSPs għandhom jiżguraw li l-programm ta' taħriġ jipprevedi t-taħriġ għall-membri tal-persunal mill-anqas fuq bażi annwali, u aktar frekwenti jekk ikun meħtieġ.

8.5 Il-PSPs għandhom jiżguraw li l-membri tal-persunal li jokkupaw rwoli ewlenin identifikati taħt GL 3.1 jirċievu taħriġ dwar is-sigurtà tal-informazzjoni speċifiku fuq bażi annwali, jew aktar frekwenti jekk ikun meħtieġ.

8.6 Il-PSPs għandhom jistabbilixxu u jimplimentaw programmi ta' għarfien tas-sigurtà perjodiċi sabiex jedukaw il-persunal u jindirizzaw riskji relatati mas-sigurtà. Dawn il-programmi għandhom ikunu jirrikjedu li l-persunal tal-PSP jirrapporta kwalunkwe inċident jew attività mhux tas-soltu.

Linja Gwida 9: Immaniġġjar tar-relazzjoni tal-utent ta' servizzi ta' pagament

Għarfien tal-utent ta' servizzi ta' pagament dwar ir-riskji ta' sigurtà u l-azzjonijiet ta' mitigazzjoni tar-riskju

9.1 Il-PSPs għandhom jistabbilixxu u jimplimentaw proċessi biex isaħħu l-għarfien tal-PSUs tar-riskji ta' sigurtà marbuta mas-servizzi ta' pagament billi jipprovdu assistenza u gwida lill-PSUs.

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

9.3 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.

9.4 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-alternattiva li jaġġusta dawn il-limiti sal-limitu massimu maqbul.

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

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

9.7 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.