EBA/GL/2017/05

11/09/2017

Linji Gwida

Linji Gwida dwar il-Valutazzjoni tar-Riskju tal-ICT taħt il-proċess ta' Reviżjoni u Evalwazzjoni Superviżorji (SREP)

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 13.11.2017. 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/2017/05’. 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. Is-suġġett, il-kamp ta' applikazzjoni u definizzjonijiet

Is-suġġett u l-kamp ta' applikazzjoni

5. Dawn il-Linji Gwida, imfassla skont l-Artikolu 107(3) tad-Direttiva 2013/36/UE[2] għandhom l-għand li jiżguraw il-konverġenza tal-prattiki superviżorji fil-valutazzjoni tar-riskju tat-teknoloġija tal-informazzjoni u l-komunikazzjoni (ICT) taħt il-proċess ta' reviżjoni u evalwazzjoni superviżorji (SREP) imsemmija fl-Artikolu 97 tad-Direttiva 2013/36/UE u speċifikati aktar fil-Linji Gwida tal-EBA dwar il-proċeduri u l-metodoloġiji komuni għall-proċess ta' reviżjoni u evalwazzjoni superviżorji (SREP)[3]. B'mod partikolari, dawn il-Linji Gwida jispeċifikaw il-kriterji ta' valutazzjoni li għandhom jiġu applikati mill-awtoritajiet kompetenti fil-valutazzjoni superviżorja tal-governanza tal-istituzzjonijiet u fl-istrateġija dwar l-ICT u l-valutazzjoni superviżorja tal-esponimenti u l-kontrolli tar-riskji tal-ICT tal-istituzzjonijiet. Dawn il-Linji Gwida jiffurmaw parti integrali tal-Linji Gwida tas-SREP tal-EBA.

6. L-awtoritajiet kompetenti għandhom japplikaw dawn il-Linji Gwida f'konformità mal-livell ta' applikazzjoni tas-SREP speċifikat fil-Linji Gwida tal-EBA SREP u skont il-mudell ta' impenn minimu u r-rekwiżiti ta' proporzjonalità stabbiliti fihom.

Destinatarji

7. Dawn il-Linji gwida huma indirizzati lill-awtoritajiet kompetenti kif definit fil-punt (i) tal-Artikolu 4(2) tar-Regolament (UE) Nru 1093/2010.

Definizzjonijiet

8. Sakemm ma jkunx speċifikat mod ieħor, it-termini użati u definiti fid-Direttiva 2013/36/UE, fir-Regolament (UE) Nru 575/2013 u d-definizzjonijiet mil-Linji Gwida SREP EBA 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 2013/36/UE tal-Parlament Ewropew u tal-Kunsill tas-26 ta' Ġunju 2013 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 (1) - ĠU L 176, 27.6.2013.

[3] EBA/GL/2014/13

Sistemi tal-ICT	L-istabbiliment tal-ICT bħala parti minn mekkaniżmu jew netwerk ta' interkonnessjoni li jappoġġja l-operazzjonijiet ta' istituzzjoni.
Servizzi tal-ICT	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' rappurtar tad-data, iżda anki s-servizzi ta' appoġġ għall-monitoraġġ, għan-negozju u għad-deċiżjonijiet.
Disponibbiltà u riskju ta' kontinwità tal-ICT	Ir-riskju li l-prestazzjoni u d-disponibbiltà tas-sistemi u d-data tal-ICT jintlaqtu b'mod ħażin, inkluż l-inabbiltà li s-servizzi tal-istituzzjoni jiġu rkuprati fil-ħin, minħabba nuqqas tal-komponenti tal-ħardwer jew tas-softwer tal-ICT; nuqqasijiet fil-ġestjoni tas-sistemi tal-ICT; jew kwalunkwe avveniment ieħor, kif elaborat aktar fl-Anness.
Riskju ta' sigurtà tal-ICT	Ir-riskju ta' aċċess mhux awtorizzat għas-sistemi u d-data tal-ICT minn ġewwa jew barra l-istituzzjoni (eż. ċiberattakki), kif elaborat aktar fl-Anness.
Riskju ta' bidla tal-ICT	Ir-riskju li jirriżulta mill-inabbiltà tal-istituzzjoni biex timmaniġġja bidliet fis-sistemi tal-ICT f'waqtu u b'mod ikkontrollat, b'mod partikolari għal programmi ta' bidla kbar u kumplessi, kif elaborat aktar fl-Anness.
Riskju ta' integrità tad-data tal-ICT	Ir-riskju li data maħżuna u pproċessata mis-sistemi tal-ICT tkun inkompleta, impreċiża jew inkonsistenti f'sistemi tal-ICT differenti, pereżempju bħala riżultat ta' kontrolli tal-ICT dgħajfa jew assenti matul il-fażijiet differenti taċ-ċiklu tal-ħajja tad-data tal-ICT (jiġifieri l-iddisinjar tal-arkitettura tad-data, il-bini tal-mudell tad-data u/jew id-dizzjunarji tad-data, il-verifika tal-inputs tad-data, il-kontroll tal-estrazzjonijiet, it-trasferimenti u l-ipproċessar tad-data, inkluż outputs tad-data mogħtija), li jxekklu l-abbiltà ta' istituzzjoni biex tipprovdi servizzi u tipproduċi informazzjoni dwar il-ġestjoni (tar-riskju) u finanzjarja b'mod korrett u f'waqtu, kif elaborat aktar fl-Anness.
Riskju ta' esternalizzazzjoni tal-ICT	Ir-riskju li l-involviment ta' parti terza, jew entità oħra ta' Grupp (esternalizzazzjoni intragrupp), biex jingħataw sistemi tal-ICT jew servizzi relatati oħra jolqot b'mod ħażin il-prestazzjoni u l-ġestjoni tar-riskju tal-istituzzjoni, kif elaborat aktar fl-Anness.

3. Implimentazzjoni

Data ta’applikazzjoni

9. Dawn il-Linji Gwida japplikaw mill-1 ta’ Jannar 2018.

4. Rekwiżiti għall-Valutazzjoni tar-Riskju tal-ICT

Titolu 1 – Dispożizzjonijiet ġenerali

10. L-awtoritajiet kompetenti għandhom iwettqu l-valutazzjoni tar-riskju tal-ICT u l-arranġament tal-governanza u tal-istrateġija tal-ICT bħala parti mill-proċess SREP wara l-mudell ta' impenn u l-kriterji ta' proporzjonalità minimi speċifikati fit-Titolu 2 tal-Linji Gwida tal-EBA SREP. B'mod partikolari, dan ifisser li:

    a. il-frekwenza tal-valutazzjoni tar-riskju tal-ICT tiddependi fuq il-mudell ta' impenn minimu xprunat mill-kategorija SREP li istituzzjoni tiġi assenjata fiha u l-programm ta' eżaminazzjoni superviżorja speċifiku tagħha; u

    b. il-profondità, id-dettall u l-intensità tal-valutazzjoni tal-ICT għandha tkun proporzjonali għad-daqs, l-istruttura u l-ambjent operazzjonali tal-istituzzjoni kif ukoll għan-natura, l-iskala u l-kumplessità tal-attivitajiet tagħha.

11. Il-prinċipju tal-proporzjonalità japplika matul dawn il-Linji Gwida għall-kamp ta' applikazzjoni, il-frekwenza u l-intensità tal-impenn u d-djalogu superviżorju ma' istituzzjoni u l-aspettattivi superviżorji tal-istandards li l-istituzzjoni għandha tissodisfa.

12. L-awtoritajiet kompetenti jistgħu jibbażaw fuq u jqisu xogħol li diġà sar mill-istituzzjoni jew mill-awtorità kompetenti fil-kuntest tal-valutazzjonijiet ta' riskji jew elementi SREP oħra sabiex ikollhom aġġornament tal-valutazzjoni. Speċifikament, fit-twettiq ta' dawn il-valutazzjonijiet speċifikati f'dawn il-Linji Gwida, l-awtoritajiet kompetenti għandhom jagħżlu l-aktar approċċ u metodoloġija ta' valutazzjoni superviżorja xierqa li huma l-aktar adattati u proporzjonali għall-istituzzjoni, u l-awtoritajiet għandhom jużaw dokumentazzjoni eżistenti u disponibbli (eż. rapporti rilevanti u dokumenti oħrajn, sejbiet ta' spezzjonijiet fuq il-post) biex jinfurmaw il-valutazzjoni tal-awtoritajiet kompetenti.

13. L-awtoritajiet kompetenti għandhom jagħtu fil-qosor is-sejbiet tal-valutazzjonijiet tagħhom tal-kriterji speċifikati f'dawn il-Linji Gwida u jużawhom għall-finijiet biex jintlaħqu konklużjonijiet dwar il-valutazzjoni tal-elementi SREP kif speċifikat fil-Linji Gwida tal-EBA SREP.

14. B'mod partikolari, il-valutazzjoni tal-istrateġija tal-governanza u tal-ICT imwettqa skont it-Titolu 2 ta' dawn il-Linji Gwida għandha tirriżulta f'sejbiet li jinfurmaw is-sommarju tas-sejbiet dwar il-valutazzjoni tal-element ta' kontrolli ta' SREP tal-governanza interna u tal-istituzzjoni kollha kif speċifikat fit-Titolu 5 tal-Linji Gwida tal-EBA SREP u għandu jkun rifless fl-għoti ta' punteġġ rispettiv ta' dak l-element SREP. Barra minn hekk, l-awtoritajiet kompetenti għandhom jikkunsidraw li kull impatt negattiv sinifikanti tal-valutazzjoni tal-istrateġija tal-ICT fuq l-istrateġija tan-negozju tal-istituzzjoni jew kwalunkwe tħassib li l-

istituzzjoni jista' ma jkollhiex biżżejjed riżorsi tal-ICT u kapaċitajiet tal-ICT biex twettaq u tappoġġja bidliet strateġiċi importanti ppjanati għandhom jinformaw lill-analiżi tal-mudell tan-negozju li saret skont it-Titolu 4 tal-Linji Gwida tal-EBA SREP.

15. Kif speċifikat fit-Titolu 3 ta' dawn il-Linji Gwida, ir-riżultat tal-valutazzjoni tar-riskju tal-ICT għandu jinforma s-sejbiet tal-valutazzjoni tar-riskju operazzjonali u għandu jiġi kkunsidrat bħala li jinforma l-punteġġ rilevanti, kif speċifikat fit-Titolu 6.4 tal-Linji Gwida tal-EBA SREP.

16. Huwa nnotat li filwaqt li b'mod ġenerali l-awtoritajiet kompetenti għandhom jivvalutaw subkategoriji tar-riskji bħala parti mill-kategoriji ewlenin (jiġifieri, ir-riskju tal-ICT ser jiġi vvalutat bħala parti mir-riskju operazzjonali), fejn l-awtoritajiet kompetenti jqisu xi subkategoriji bħala materjali, jistgħu jivvalutaw dawn is-subkategoriji fuq bażi individwali. Għal dan il-għan, jekk riskju tal-ICT jiġi identifikat bħala riskju materjali mill-awtorità kompetenti, dawn il-Linji Gwida jipprovdu wkoll tabella ta' punteġġ (Tabella 1) li għandha tintuża biex jingħata punteġġ individwali tas-subkategorija għar-riskju tal-ICT li jsegwi l-approċċ ġenerali għall-għoti ta' punteġġ tar-riskji mal-kapital fil-Linji Gwida tal-EBA SREP.

17. Sabiex tintlaħaq fehma dwar jekk ir-riskju tal-ICT għandux jiġi kkunsidrat bħala materjali u għalhekk il-possibbiltà li r-riskju tal-ICT jiġi vvalutat u jingħata punteġġ bħala subkategorija individwali tar-riskju operazzjonali, l-awtoritajiet kompetenti jistgħu jużaw il-kriterji speċifikati fit-Taqsima 6.1 tal-Linji Gwida tal-EBA SREP.

18. Meta japplikaw dawn il-Linji Gwida, fejn ikun rilevanti, l-awtoritajiet kompetenti għandhom jikkunsidraw il-lista mhux eżawrjenti tas-subkategoriji tar-riskju u x-xenarji tar-riskju tal-ICT kif stabbilit fl-Anness, filwaqt li jinnutaw li l-Anness jiffoka fuq ir-riskji tal-ICT li jistgħu jirriżultaw f'telf ta' severità għolja. L-awtoritajiet kompetenti jistgħu jeskludu wħud mir-riskji tal-ICT inklużi fit-tassonomija jekk ma jkunux pertinenti għall-valutazzjoni tagħhom. L-istituzzjonijiet huma mistennija li jżommu t-tassonomiji tar-riskji tagħhom stess minflok jużaw it-tassonomija tar-riskju tal-ICT stabbilita fl-Anness.

19. Fejn dawn il-Linji gwida jiġu applikati fir-rigward ta' gruppi bankarji transkonfinali u l-entitajiet tagħhom, u jkun ġie stabbilit kulleġġ tas-superviżuri, l-awtoritajiet kompetenti involuti, fil-kuntest tal-kooperazzjoni tagħhom għall-valutazzjoni tas-SREP, f'konformità mat-Taqsima 11.1 tal-Linji Gwida tal-EBA SREP, għandhom jikkoordinaw sal-limitu massimu possibbli l-kamp ta' applikazzjoni eżatt u ddettaljat ta' kull oġġett ta' informazzjoni b'mod konsistenti għall-entitajiet tal-gruppi kollha.

Titolu 2 - Valutazzjoni tal-istrateġija u l-governanza tal-istituzzjonijiet dwar l-ICT

2.1 Prinċipji ġenerali

20. L-awtoritajiet kompetenti għandhom jivvalutaw jekk il-governanza ġenerali tal-istituzzjoni u l-qafas ta' kontroll intern ikoprux kif suppost is-sistemi tal-ICT u r-riskji relatati u jekk il-korp maniġerjali jindirizzax u jimmaniġġjax dawn l-aspetti b'mod adegwat, għax l-ICT hu integrali għall-funzjonament tajjeb ta' istituzzjoni.

21. Fit-twettiq ta' din il-valutazzjoni, l-awtoritajiet kompetenti għandhom jirreferu għar-rekwiżiti u l-istandards ta' governanza interna u arranġamenti ta' kontroll tar-riskju tajbin kif speċifikat fil-Linji Gwidi tal-EBA dwar il-Governanza Interna (GL 44)[4] u l-gwida internazzjonali f'dan il-qasam sal-punt fejn dawn ikunu applikabbli meta titqies l-ispeċifiċità tas-sistemi u r-riskji tal-ICT.

22. Il-valutazzjoni f'dan it-Titolu ma tkoprix l-elementi speċifiċi tal-governanza tas-sistema, tal-ġestjoni tar-riskju u tal-kontrolli tal-ICT li huma ffukati fuq il-ġestjoni ta' riskji speċifiċi tal-ICT indirizzati taħt it-Titolu 3 ta' dawn il-Linji Gwida, iżda tiffoka fuq l-oqsma li ġejjin:

    a. Strateġija tal-ICT - jekk l-istituzzjoni għandhiex strateġija tal-ICT li hi regolata b'mod xieraq u konformi mal-istrateġija tan-negozju tal-istituzzjoni;

    b. governanza interna ġenerali - jekk l-arranġamenti tal-governanza interna ġenerali tal-istituzzjoni humiex adegwati fir-rigward tas-sistemi tal-ICT tal-istituzzjoni; u

    c. ir-riskju tal-ICT fil-qafas tal-ġestjoni tar-Riskju tal-istituzzjoni - jekk il-qafas tal-ġestjoni tar-riskju u tal-kontroll intern tal-istituzzjoni jissalvagwardjax b'mod xieraq is-sistemi tal-ICT tal-istituzzjoni.

23. Il-Punt a) imsemmi fil-paragrafu 22, filwaqt li jipprovdi informazzjoni dwar elementi tal-governanza tal-istituzzjoni, għandu primarjament jikkontribwixxi għall-valutazzjoni tal-mudell tan-negozju indirizzat taħt it-Titolu 4 tal-Linji Gwida tal-EBA SREP. Il-Punti b) u c) ikomplu jikkomplimentaw il-valutazzjonijiet tas-suġġetti koperti mit-Titolu 5 tal-Linji Gwida tal-EBA SREP u l-valutazzjoni deskritta f'dawn il-Linji Gwida għandha tikkontribwixxi għall-valutazzjoni rispettiva taħt it-Titolu 5 tal-Linji Gwida tal-EBA SREP.

24. Ir-riżultat ta' din il-valutazzjoni għandu jinforma, fejn rilevanti, il-valutazzjoni tal-ġestjoni u l-kontrolli tar-riskju fit-Titolu 3 ta' dawn il-Linji Gwida.

[4] Linji Gwida tal-EBA dwar il-Governanza Interna, GL 44, 27 ta' Settembru 2011.

2.2 Strateġija tal-ICT

25. Taħt din it-taqsima l-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex strateġija fis-seħħ: li hi soġġetta għal sorveljanza adegwata mill-korp maniġerjali tal-istituzzjoni; li hi konsistenti mal-istrateġija tan-negozju; b'mod partikolari biex iżżomm l-ICT tagħha aġġornat u tippjana jew timplimenta bidliet tal-ICT importanti u kumplessi; u li tappoġġja l-mudell tan-negozju tal-istituzzjoni.

2.2.1 Żvilupp u adegwatezza tal-istrateġija tal-ICT

26. L-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex qafas fis-seħħ, proporzjonali għan-natura, l-iskala u l-kumplessità tal-attivitajiet tal-ICT tagħha, għat-tħejjija u l-iżvilupp tal-istrateġija tal-ICT tal-istituzzjoni. Fit-twettiq ta' din il-valutazzjoni, l-awtoritajiet kompetenti għandhom jikkunsidraw jekk:

    a. il-maniġment superjuri[5] tal-linja(i) tan-negozju ikunx involut b'mod adegwat fid-definizzjoni tal-prijoritajiet strateġiċi tal-ICT tal-istituzzjoni u jekk, min-naħa l-oħra, il-maniġment superjuri tal-funzjoni tal-ICT huwiex konxju tal-iżvilupp, id-disinn u l-bidu ta' strateġiji u inizjattivi tal-kummerċ ewlenin biex jiġi żgurat l-allinjament kontinwu bejn is-sistemi tal-ICT, is-servizzi tal-ICT u l-funzjoni tal-ICT (jiġifieri dawk responsabbli għall-ġestjoni u l-istazzjonament ta' dawn is-sistemi u s-servizzi), u l-istrateġija tan-negozju tal-istituzzjoni, u li l-ICT ikunu aġġornati b'mod effettiv;

    b. l-istrateġija tal-ICT hix dokumentata u appoġġjata bi pjanijiet ta' implimentazzjoni konkreti, b'mod partikolari fir-rigward tal-istadji importanti u l-ippjanar tar-riżorsi (inklużi riżorsi finanjarji u umani) biex jiġi żgurat li jkunu realistiċi u jippermettu l-wasla tal-istrateġija tal-ICT;

    c. l-istituzzjoni taġġornax l-istrateġija tal-ICT tagħha perjodikament, b'mod partikolari fit-tibdil tal-istrateġija tan-negozju, biex jiġi żgurat l-allinjament kontinwu bejn l-għanijiet, il-pjanijiet u l-attivitajiet fuq żmien medju u fit-tul tal-ICT u tan-negozju; u

    d. il-korp maniġerjali tal-istituzzjoni japprovax l-istrateġija tal-ICT, il-pjanijiet ta' implimentazzjoni u jimmonitorjax l-implimentazzjoni tagħha.

2.2.2 Implimentazzjoni tal-istrateġija tal-ICT

27. Jekk l-istrateġija tal-ICT tal-istituzzjoni teħtieġ l-implimentazzjoni ta' bidliet tal-ICT importanti u kumplessi, jew bidliet b'implikazzjonijiet materjali għall-mudell tan-negozju tal-istituzzjoni, l-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex qafas ta' kontroll fis-seħħ, xieraq għad-daqs tagħha, l-attivitajiet tal-ICT tagħha kif ukoll il-livell tal-attivitajiet ta' bidla, biex tiġi appoġġjata l-implimentazzjoni effettiva tal-istrateġija tal-ICT tal-istituzzjoni. Fit-twettiq ta' din il-valutazzjoni, l-awtoritajiet kompetenti għandhom jikkunsidraw jekk il-qafas ta' kontroll:

[5] Il-maniġment superjuri u l-korp maniġerjali kif definiti fid-Direttiva 2013/36/UE tas-26 ta' Ġunju 2013 fl-Artikolu 3 (7) "korp maniġerjali", u l-Artikolu 3 (9) "maniġment superjuri".

a. jinkludix proċessi ta' governanza (eż. monitoraġġ u rappurtar tal-progress u tal-baġit) u korpi rilevanti (eż. uffiċċju tal-ġestjoni tal-proġetti (PMO), grupp ta' tmexxija tal-ICT jew ekwivalenti) biex l-implimentazzjoni tal-programmi strateġiċi tal-ICT tiġi appoġġjata b'mod effettiv;

b. ikunx iddefinixxa u alloka r-rwoli u r-responsabbiltajiet għall-implimentazzjoni ta' programmi strateġiċi tal-ICT, fejn tingħata attenzjoni partikolari għall-esperjenza ta' partijiet ikkonċernati ewlenin fl-organizzazzjoni, it-tmexxija u l-monitoraġġ ta' bidliet importanti u kumplessi tal-ICT u l-ġestjoni tal-impatti organizzattivi u tal-bnedmin usa' (eż. il-ġestjoni tar-reżistenza għall-bidla, it-taħriġ u l-komunikazzjoni).

c. jinvolvix il-kontroll indipendenti u uffiċċji tal-awditjar interni biex tingħata l-assigurazzjoni li r-riskji assoċjati mal-implimentazzjoni tal-istrateġija tal-ICT ġew identifikati, ivvalutati u mtaffija b'mod effettiv u li l-qafas ta' governanza fis-seħħ biex tiġi implimentata l-istrateġija tal-ICH jkun effettiv; u

d. jkunx fih ippjanar u proċess ta' reviżjoni ta' ppjanar li jagħti l-flessibbiltà li tingħata risposta għal kwistjonijiet importanti identifikati (eż. problemi jew dewmien fl-implimentazzjoni li nqalgħu) jew żviluppi esterni (eż. bidliet importanti fl-ambjent tan-negozju, fi kwistjonijiet teknoloġiċi jew f'innovazzjonijiet) biex jiġi żgurat adattament f'waqtu tal-pjan strateġiku ta' implimentazzjoni.

2.3 Governanza interna ġenerali

28. Skont it-Titolu 5 tal-Linji Gwida tal-EBA SREP, l-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex struttura korporattiva xierqa u trasparenti li hi "adatta għall-iskop", u jekk implementatx arranġamenti xierqa ta' governanza. B'mod partikolari fir-rigward ta' sistemi tal-ICT u f'konformità mal-Linji Gwida tal-EBA dwar il-governanza interna, din il-valutazzjoni għandha tinkludi valutazzjoni dwar jekk l-istituzzjoni turix:

a. struttura organizzativa robusta u trasparenti b'responsabbiltajiet ċari dwar l-ICT, inkluż il-korp maniġerjali u l-kumitati tiegħu u jekk il-persuni responsabbli ewlenin għall-ICT (eż. uffiċjal kap tal-informazzjoni "CIO", uffiċjal kap operattiv "COO" jew rwol ekwivalenti) ikollhomx aċċess indirett jew dirett adegwat għall-korp maniġerjali, biex jiġi żgurat li informazzjoni jew kwistjonijiet importanti relatati mal-ICT jiġu rrappurtati, diskussi u deċiżi b'mod xieraq fil-livell tal-korp maniġerjali; u

b. li l-korp maniġerjali jaf u jindirizza r-riskji assoċjati mal-ICT;

29. Flimkien mat-taqsima 5.2 tal-Linji Gwida tal-EBA SREP, l-awtoritajiet kompetenti għandhom jivvalutaw jekk il-politika u l-istrateġija ta' esternalizzazzjoni tal-ICT tal-istituzzjoni tikkunsidrax, fejn rilevanti, l-impatt tal-esternalizzazzjoni tal-ICT fuq il-mudell tan-negozju tal-istituzzjoni.

2.4 Riskju tal-ICT fil-qafas tal-ġestjoni tar-riskju tal-istituzzjoni

30. Fil-valutazzjoni tal-ġestjoni tar-riskju u tal-kontrolli interni fl-istituzzjoni kollha tal-istituzzjoni, kif provdut mit-Titolu 5 tal-Linji Gwida tal-EBA SREP, l-awtoritajiet kompetenti għandhom jikkunsidraw jekk il-qafas

tal-ġestjoni tar-riskju u tal-kontroll intern tal-istituzzjoni jissalvagwardjax b'mod xieraq is-sistemi tal-ICT tal-istituzzjoni b'mod proporzjonali għad-daqs u l-attivitajiet tal-istituzzjoni u l-profil tar-riskju tal-ICT tagħha kif definit fit-Titolu 3. B'mod partikolari, l-awtoritajiet kompetenti għandhom jiddeterminaw jekk:

a. l-aptit għar-riskju u l-ICAAP ikoprux ir-riskji tal-ICT, bħala parti mill-kategorija tar-riskju operazzjonali aktar wiesgħa, għad-definizzjoni tal-istrateġija tar-riskju ġenerali u d-determinazzjoni tal-kapital intern; u

b. ir-riskji tal-ICT jaqgħux fil-kamp ta' applikazzjoni tal-oqfsa tal-ġestjoni tar-riskju u tal-oqfsa ta' kontroll intern fl-istituzzjoni kollha.

31. L-awtoritajiet kompetenti għandhom iwettqu l-valutazzjoni taħt il-punt (a) ta' fuq kemm fid-dawl tax-xenarji mistennija kif ukoll fid-dawl ta' dawk negattivi, eż. xenarji inklużi fit-test tal-istress speċifiku għall-istituzzjoni jew superviżorju.

32. B'attenzjoni speċifika għal b), l-awtoritajiet kompetenti għandhom jivvalutaw jekk il-kontroll indipendenti jew l-uffiċċji tal-awditjar interni, kif dettaljat fil-paragrafi 104 (a), 104 (d), 105 (a) u 105 (c) tal-Linji Gwida tal-EBA SREP, humiex xierqa biex jiġi żgurat livell suffiċjenti ta' indipendenza bejn l-ICT u l-kontroll u l-uffiċċji tal-awditjar, meta jitqies id-daqs u l-profil tar-riskju tal-ICT tal-istituzzjoni.

2.5 Sommarju tas-sejbiet

33. Dawn ir-riżultati għandhom ikunu riflessi fis-sommarju tas-sejbiet taħt it-Titolu 5 tal-Linji Gwida tal-EBA SREP u għandhom jiffurmaw parti mill-punteġġ rispettiv f'konformità mal-kunsiderazzjonijiet fit-Tabella 3 tal-Linji Gwida tal-EBA SREP.

34. Għall-valutazzjoni tal-istrateġija tal-ICT, fil-konklużjoni tal-valutazzjoni ta' hawn fuq għandhom jiġu kkunsidrati l-punti li ġejjin:

a. jekk l-awtoritajiet kompetenti jaslu għall-konklużjoni li l-qafas ta' governanza tal-istituzzjoni jkun inadegwat biex jiżviluppa u jimplimenta l-istrateġija tal-ICT tal-istituzzjoni taħt 2.2 mela din għandha tinforma l-valutazzjoni tal-governanza interna tal-istituzzjoni fit-Titolu 5 tal-Linji Gwida tal-EBA SREP taħt il-punt 87 (a);

b. jekk mill-valutazzjonijiet ta' hawn fuq taħt 2.2 l-awtoritajiet kompetenti jaslu għall-konklużjoni li jkun hemm nuqqas ta' allinjament sinifikanti bejn l-istrateġija tal-ICT u l-istrateġija tan-negozju li jista' jkollu impatt ħażin fuq l-għanijiet tan-negozju u/jew finanjarji fuq żmien twil tal-istituzzjoni, is-sostenibbiltà u/jew il-mudell tan-negozju tal-istituzzjoni, jew l-oqsma/il-linji tan-negozju tal-istituzzjoni li ġew determinati bħala l-aktar materjali fil-paragrafu 62 (a) tal-Linji Gwida tal-EBA SREP, mela din għandha tinforma l-valutazzjoni tal-mudell tan-negozju tat-Titolu 4 tal-GL SREP taħt il-punti 70 (b) u 70 (c); u

c. jekk mill-valutazzjonijiet ta' hawn fuq taħt 2.2 l-awtoritajiet kompetenti jaslu għall-konklużjoni li l-istituzzjoni jista' ma jkollhiex biżżejjed riżorsi tal-ICT u kapaċitajiet ta' implimentazzjoni tal-ICT biex twettaq u tappoġġja bidliet strateġiċi importanti ppjanati, din għandha tinforma lill-valutazzjoni tal-mudell tan-negozju tat-Titolu 4 tal-Linji Gwida tal-EBA SREP taħt il-punt 70 (b).

Titolu 3 - Valutazzjoni tal-esponimenti u l-kontrolli tar-riskji tal-ICT tal-istituzzjonijiet

3.1 Kunsiderazzjonijiet ġenerali

35. L-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni idenfikatx, ivvalutatx u taffitx kif suppost ir-riskji tal-ICT tagħha. Dan il-proċess għandu jkun parti mill-qafas tal-ġestjoni tar-riskju operazzjonali u konformi mal-approċċ li japplika għar-riskju operazzjonali.

36. L-awtoritajiet kompetenti l-ewwel għandhom jidentifikaw ir-riskji materjali inerenti tal-ICT li għalihom hi esposta jew tista' tiġi esposta l-istituzzjoni, segwita minn valutazzjoni tal-effettività tal-qafas, il-proċeduri u l-kontrolli tal-ġestjoni tar-riskji tal-ICT tal-istituzzjoni biex jitnaqqsu dawn ir-riskji. Ir-riżultat tal-valutazzjoni għandu jkun rifless f'sommarju tas-sejbiet li jikkontribwixxi għall-punteġġ tar-riskju operazzjonali fil-Linji Gwida tas-SREP. Fejn ir-riskju tal-ICT jitqies li jkun materjali u fejn l-awtoritajiet kompetenti jixtiequ jassenjaw punteġġ individwali, għandha tintuża t-Tabella 1 biex jiġi assenjat punteġġ bħala subriskju tar-riskju operazzjonali.

37. Meta titwettaq valutazzjoni taħt dan it-Titolu, l-awtoritajiet kompetenti għandhom jużaw is-sorsi ta' informazzjoni disponibbli kollha kif stabbilit fil-paragrafu 127 tat-Titolu 6 tal-Linji Gwida tal-EBA SREP eż. l-attivitajiet, ir-rappurtar u r-riżultati ta' ġestjoni tar-riskju ta' istituzzjoni, bħala bażi għall-identifikazzjoni tal-prijoritajiet tal-valutazzjoni superviżorja tagħhom. L-awtoritajiet kompetenti għandhom ukoll jużaw sorsi ta' informazzjoni oħrajn biex iwettqu din il-valutazzjoni, inklużi dawn li ġejjin, fejn rilevanti:

    a. awtovalutazzjonijiet tar-riskju u tal-kontrolli tal-ICT (jekk jingħataw fl-informazzjoni tal-ICAAP);
    b. Informazzjoni ta' Ġestjoni (MI) relatata mar-riskju tal-ICT ippreżentata lill-korp maniġerjali tal-istituzzjoni, eż. rappurtar tar-riskju tal-ICT perjodiku u xprunat mill-inċidenti (inkluż fil-bażi ta' data tat-telf operattiv), data ta' esponiment għar-riskju tal-ICT mill-funzjoni tal-ġestjoni tar-riskju tal-istituzzjoni;
    c. sejbiet tal-awditjar interni u esterni relatati mal-ICT irrappurtati lill-kumitat tal-awditjar tal-istituzzjoni.

3.2 Identifikazzjoni ta' riskji materjali tal-ICT

38. L-awtoritajiet kompetenti għandhom jidentifikaw ir-riskji materjali tal-ICT li għalihom l-istituzzjoni hi jew tista' tiġi esposta billi jsegwu l-passi t'hawn taħt.

3.2.1 Reviżjoni tal-profil tar-riskju tal-ICT tal-istituzzjoni

39. Fir-reviżjoni tal-profil tar-riskju tal-ICT tal-istituzzjoni, l-awtoritajiet kompetenti għandhom jikkunsidraw l-informazzjoni rilevanti kollha dwar l-esponimenti għar-riskju tal-ICT tal-istituzzjoni, inkluż l-informazzjoni taħt il-paragrafu 37 u n-nuqqasijiet materjali identifikati fil-kontrolli fl-organizzazzjoni u l-istituzzjoni kollha tal-ICT taħt it-Titolu 2 ta' dawn il-Linji Gwida, u, fejn rilevanti, għandhom jirrevedu din

l-informazzjoni b'mod proporzjonat. Bħala parti minn din ir-reviżjoni, l-awtoritajiet kompetenti għandhom jikkunsidraw:

a. l-impatt potenzjali ta' tfixkil sinifikanti dwar is-sistemi tal-ICT tal-istituzzjoni dwar is-sistema finanzjarja jew fil-livell domestiku jew fil-livell internazzjonali;
b. jekk l-istituzzjoni tistax tkun soġġetta għal riskji ta' sigurtà tal-ICT jew għal riskji ta'disponibbiltà u kontinwità tal-ICT minħabba dipendenzi tal-internet, adozzjoni għolja ta' soluzzjonijiet innovattivi tal-ICT jew mezzi ta' distribuzzjoni tan-negozju oħrajn li jistgħu jagħmluha aktar soġġetta għal ċiberattakki;
c. jekk l-istituzzjoni tistax tkun aktar esposta għal riskji ta' sigurtà, riskji ta' disponibbiltà u kontinwità tal-ICT jew riskji ta' bidla tal-ICT minħabba l-kumplessità (eż. bħala riżultat ta' fużjonijiet jew akkwisti) jew in-natura skaduta tas-sistemi tal-ICT tagħha;
d. jekk l-istituzzjoni hijiex qiegħda timplimenta bidliet materjali fis-sistemi tal-ICT u/jew funzjoni tal-ICT tagħha (eż. bħala riżultat ta' fużjonijiet, akkwisti, ċessjonijiet jew is-sostituzzjoni tas-sistemi ewlenin tal-ICT tagħha), li jistgħu jolqtu b'mod ħażin l-istabbiltà jew il-funzjonament tajjeb tas-sistemi tal-ICT u jistgħu jirriżultaw f'disponibbiltà u riskji ta' kontinwità materjali tal-ICT, riskji ta' sigurtà tal-ICT, riskji ta' bidla tal-ICT jew riskji ta' integrità tad-data tal-ICT;
e. jekk l-istituzzjoni esternalizzatx is-servizzi tal-ICT jew is-sistemi tal-ICT fi ħdan jew 'il barra mill-grupp li jista' jesponiha għal riskji ta' esternalizzazzjoni materjali tal-ICT;
f. jekk l-istituzzjoni tkunx qed timplimenta miżuri aggressivi ta' tnaqqis tal-ispejjeż tal-ICT li jistgħu jirriżultaw fit-tnaqqis ta' investimenti u riżorsi tal-ICT u għarfien espert tal-IT meħtieġa u li jistgħu jżidu l-esponiment għal kull tip ta' riskju tal-ICT fit-tassonomija;
g. jekk il-post tal-operazzjonijiet/ċentri tad-data importanti tal-ICT (eż. reġjuni, pajjiżi) jistax jesponi lill-istituzzjoni għal diżastri naturali (eż. għargħar, terremoti), instabbiltà politika jew kunflitti tax-xogħol u disturbi ċivili li jistgħu jirriżultaw f'żieda materjali tar- riskji ta' disponibbiltà u kontinwità tal-ICT u riskji ta' sigurtà tal-ICT.

3.2.2 Reviżjoni tas-sistemi u s-servizzi kritiċi tal-ICT

40. Bħala parti mill-proċess ta' identifikazzjoni tar-riskji tal-ICT b'impatt prudenzjali sinifikanti potenzjali fuq l-istituzzjoni, l-awtoritajiet kompetenti għandhom jirrevedu d-dokumentazzjoni mill-istituzzjoni u jiffurmaw opinjoni dwar liem sistemi u servizzi tal-ICT huma kritiċi għall-funzjonament, id-disponibbiltà, il-kontinwità u s-sigurtà xierqa tal-attivitajiet essenzjali tal-istituzzjoni.

41. Għal dan il-għan, l-awtoritajiet kompetenti għandhom jirrevedu l-metodoloġija u l-proċessi applikati mill-istituzzjoni biex jiġu identifikati s-sistemi u s-servizzi tal-ICT li huma kritiċi, filwaqt li jitqies li ċerti sistemi u servizzi tal-ICT jistgħu jiġu kkunsidrati bħala kritiċi mill-istituzzjoni minn perspettiva ta' kontinwità u disponibbiltà tan-negozju, perspettiva ta' sigurtà (eż. prevenzjoni tal-frodi) u/jew perspettiva ta' kunfidenzjalità (eż. data kunfidenzjali). Meta jwettqu r-reviżjoni, l-awtoritajiet kompetenti għandhom iwettqu r-reviżjoni tagħhom filwaqt li jqisu li sistemi u servizzi kritiċi tal-ICT mill-inqas għandhom jissodisfaw waħda mill-kundizzjonijiet li ġejjin:

a. li jappoġġjaw l-operazzjonijiet tan-negozju u l-mezzi ta' distribuzzjoni ewlenin (eż. ATMs, ibbankjar bl-internet u bil-mowbajl) tal-istituzzjoni;

b. li jappoġġjaw proċessi ta' governanza u funzjonijiet korporattivi essenzjali, inkluż il-ġestjoni tar-riskju (eż. sistemi tal-ġestjoni tar-riskju u l-immaniġġjar tal-flus);

c. li jaqgħu taħt rekwiżiti legali jew regolatorji speċjali (jekk hemm) li jimponu rekwiżiti ta' disponibbiltà, reżiljenza, kunfidenzjalità jew sigurtà miżjuda (eż. leġiżlazzjoni dwar il-protezzjoni tad-data jew il-possibbiltà ta' "Għanijiet tal-Ħin ta' Rkupru" (RTO, iż-żmien massimu li fih għandhom jiġu restawrati sistema jew proċess wara inċident) u "Għan tal-Punt ta' Rkupru" (RPO, il-perjodu massimu ta' żmien li matulu tista' tintilef data f'każ ta' inċident)) għal ċerti servizzi sistematikament importanti (jekk u fejn applikabbli));

d. li jipproċessaw jew jaħżnu data kunfidenzjali jew sensittiva li aċċess mhux awtorizzat għaliha jista' jkollu impatt sinifikanti fuq ir-reputazzjoni u r-riżultati finanzjarji tal-istituzzjoni jew is-soliditá u l-kontinwità tan-negozju tagħha (eż. bażijiet ta' data b'data sensittiva dwar il-klijenti); u/jew

e. li jipprovdu l-funzjonalitajiet bażiċi li huma vitali għall-funzjonament xieraq tal-istituzzjoni (eż. servizzi ta' telekomunikazzjoni u konnettività, servizzi tal-ICT u taċ-ċibersigurtà).

3.2.3 Identifikazzjoni ta' riskji materjali tal-ICT għal Sistemi u Servizzi kritiċi tal-ICT

42. Filwaqt li jqisu r-reviżjonijiet imwettqa tal-profil tar-riskju u s-sistemi u s-servizzi kritiċi tal-ICT tal-istituzzjoni ta' hawn fuq, l-awtoritajiet kompetenti għandhom jiffurmaw opinjoni dwar ir-riskji materjali tal-ICT li, fil-ġudizzju superviżorju tagħhom, jistgħu jkollhom impatt prudenzjali sinifikanti fuq is-sistemi u s-servizzi kritiċi tal-ICT tal-istituzzjoni.

43. Meta jivvalutaw l-impatt potenzjali tar-riskji tal-ICT fuq is-sistemi u s-servizzi kritiċi tal-ICT ta' istituzzjoni, l-awtoritajiet kompetenti għandhom jikkunsidraw:

a. L-impatt finanzjarju, inkluż (iżda mhux limitat għal) telf ta' fondi jew assi, kumpens potenzjali għall-klijenti, spejjeż legali u ta' rimedju, danni kuntrattwali, dħul mitluf;

b. Il-potenzjal għal tqallib tal-operat, filwaqt li jqisu (iżda ma jkunux limitata għal) il-kritikalità tas-servizzi finanzjarji affettwati; in-numru ta' klijenti u/jew fergħat u impjegati li potenzjalment ġew affettwati;

c. L-impatt reputazzjonali potenzjali fuq l-istituzzjoni bbażat fuq il-kritikalità tas-servizz jew l-attività operazzjonali bankarja affettwata (eż. serq ta' data dwar il-klijenti); il-profil/viżibbiltà esterna tas-sistemi u s-servizzi tal-ICT affettwati (eż. sistemi bankarji fuq il-mowbajl jew online, punt tal-bejgħ, ATMs jew sistemi ta' pagament);

d. L-impatt regolatorju, inkluż il-potenzjal għal ċensura pubblika mir-regolatur, multi jew anki varjazzjoni tal-permessi.

e. L-impatt strateġiku fuq l-istituzzjoni, pereżempju jekk il-prodott strateġiku jew il-pjanijiet tan-negozju jiġu kompromessi jew jinsterqu.

44. L-awtoritajiet kompetenti mbagħad għandhom jirrappreżentaw ir-riskji tal-ICT identifikati li huma kkunsidrati materjali fil-kategoriji tar-riskji tal-ICT li ġejjin li għalihom jingħataw deskrizzjonijiet u eżempji

ta' riskji ulterjuri fl-Anness. L-awtoritajiet kompetenti għandhom jirriflettu fuq ir-riskji tal-ICT fl-Anness bħala parti mill-valutazzjoni taħt it-Titolu 3:

a. Disponibbiltà u riskju ta' kontinwità tal-ICT
b. Riskju ta' sigurtà tal-ICT
c. Riskju ta' bidla tal-ICT
d. Riskju ta' integrità tad-data tal-ICT
e. Riskju ta' esternalizzazzjoni tal-ICT

Ir-rappreżentazzjoni qiegħda biex tgħin lill-awtoritajiet kompetenti jiddeterminaw liema riskji huma materjali (jekk hemm) u għalhekk għandhom ikunu soġġetti għal reviżjoni aktar mill-viċin u/jew aktar fil-fond fil-passi ta valutazzjoni li ġejjin.

3.3 Valutazzjoni tal-kontrolli biex jitnaqqsu riskji materjali tal-ICT

45. Biex jiġi vvalutat l-esponiment għar-riskju residwu tal-ICT tal-istituzzjoni, l-awtoritajiet kompetenti għandhom jirrevedu kif l-istituzzjoni tidentifika, timmonitorja, tivvaluta u tnaqqas ir-riskji materjali identifikati mill-awtoritajiet kompetenti fil-valutazzjoni ta' hawn fuq.

46. Għal dan l-iskop, għar-riskji materjali tal-ICT identifikati, l-awtoritajiet kompetenti għandhom jirrevedu l-applikabbli:

    a. Politika, proċessi tal-ġestjoni tar-riskju u limiti ta' tolleranza tar-riskju tal-ICT;

    b. Ġestjoni organizzazzjonali u qafas ta' sorveljanza;

    c. Kopertura u sejbiet tal-awditjar intern; u

    d. Kontrolli tar-riskju tal-ICT li huma speċifiċi għar-riskju materjali tal-ICT identifikat.

47. Il-valutazzjoni għandha tqis ir-riżultat tal-analiżi tal-ġestjoni tar-riskju u l-qafas ta' kontroll intern ġenerali kif imsemmi fit-Titolu 5 tal-Linji Gwida tal-EBA SREP, kif ukoll tal-governanza u l-istrateġija tal-istituzzjoni indirizzati fit-Titolu 2 ta' dawn il-Linji Gwida, peress li nuqqasijiet sinifikanti identifikati f'dawn l-oqsma jistgħu jinfluwenzaw l-abbiltà tal-istituzzjoni biex timmaniġġja u tnaqqas l-esponimenti għar-riskju tal-ICT tagħha. Fejn rilevanti, l-awtoritajiet kompetenti għandhom ukoll jużaw sorsi ta' informazzjoni fil-paragrafu 37 ta' dawn il-Linji Gwida.

48. L-awtoritajiet kompetenti għandhom iwettqu l-passi ta' valutazzjoni li ġejjin b'mod li jkun proporzjonali għan-natura, l-iskala u l-kumplessità tal-attivitajiet tal-isituzzjoni u billi japplikaw reviżjoni superviżorja li hi xierqa għall-profil tar-riskju tal-ICT tal-istituzzjoni.

3.3.1 Politika, proċessi u limiti ta' tolleranza tal-ġestjoni tar-riskju tal-ICT

49. L-awtoritajiet kompetenti għandhom jirrevedu jekk l-istituzzjoni għandhiex politiki, proċessi u limiti ta' tolleranza tal-ġestjoni tar-riskju xierqa fis-seħħ għar-riskji materjali tal-ICT identifikati. Dawn jistgħu jkunu parti mill-qafas tal-ġestjoni tar-riskju operazzjonali jew minn dokument separat. Għal din il-valutazzjoni, l-awtoritajiet kompetenti għandhom iqisu jekk:

    a. il-politika tal-ġestjoni tar-riskju tkunx formalizzata u approvata mill-korp maniġerjali u jkunx fiha gwida suffiċjenti dwar l-aptit għar-riskju tal-ICT tal-istitituzzjoni, u dwar l-għanijiet tal-ġestjoni tar-riskju ewlenin tal-ICT segwiti u/jew il-limiti ta' tolleranza tar-riskju tal-ICT applikati. Il-politika tal-ġestjoni tar-riskju tal-ICT rilevanti għandhiex ukoll tiġi kkomunikata lill-partijiet ikkonċernati rilevanti kollha;

    b. il-politika applikabbli tkoprix l-elementi sinifikanti kollha għall-ġestjoni tar-riskju tar-riskji materjali tal-ICT identifikati;

    c. l-istituzzjoni tkunx implimentat proċess u proċeduri sottostanti għall-identifikazzjoni (eż. "awtovalutazzjonijiet tal-kontroll tar-riskju" (RCSA), analiżi tax-xenarju tar-riskju) u l-monitoraġġ tar-riskji materjali tal-ICT involuti; u

    d. l-istituzzjoni jkollhiex rappurtar tal-ġestjoni tar-riskju tal-ICT fis-seħħ li jipprovdi informazzjoni f'waqtha lill-maniġment superjuri u lill-korp maniġerjali, li jippermetti lill-maniġment superjuri u/jew lill-korp maniġerjali jivvalutaw u jimmonitorjaw jekk il-pjanijiet u l-miżuri ta' mitigazzjoni tar-riskju tal-ICT tal-istituzzjoni jkunux konsistenti mal-aptit tar-riskju u/jew il-limiti ta' tolleranza approvati (fejn rilevanti) u jimmonitorjaw bidliet ta' riskji materjali tal-ICT.

3.3.2 Ġestjoni organizzazzjonali u qafas ta' sorveljanza

50. L-awtoritajiet kompetenti għandhom jivvalutaw kif ir-rwoli u l-responsabbiltajiet tal-ġestjoni tar-riskju applikabbli jiġu inkorporati u integrati fl-organizzazzjoni interna biex jiġu mmaniġġjati u sorveljati r-riskji materjali tal-ICT identifikati. F'dan ir-rigward, l-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni turix:

    a. rwoli u responsabbiltajiet ċari għall-identifikazzjoni, il-valutazzjoni, il-monitoraġġ, il-mitigazzjoni, ir-rappurtar u s-sorveljanza tar-riskju materjali tal-ICT involut;

    b. li r-responsabbiltajiet u r-rwoli tar-riskju jiġu kkomunikati, allokati u inkorporati b'mod ċar fil-partijiet (eż. linji tan-negozju, IT) u l-proċessi rilevanti kollha tal-organizzazzjoni, inkluż ir-rwoli u r-responsabbiltajiet għall-ġbir u l-aggregazzjoni tal-informazzjoni tar-riskju u r-rappurtar tagħha lill-maniġment superjuri u/jew lill-korp maniġerjali;

    c. li l-attivitajiet tal-ġestjoni tar-riskju tal-ICT jitwettqu b'riżorsi umani u tekniċi xierqa b'mod kwalitattiv u suffiċjenti. Biex tiġi vvalutata l-kredibbiltà tal-pjanijiet ta' mitigazzjoni tar-riskju applikabbli, l-awtoritajiet kompetenti għandhom ukoll jivvalutaw jekk l-istituzzjoni tkunx allokat biżżejjed baġits finanzjarji u/jew riżorsi meħtieġa oħrajn għall-implimentazzjoni tagħhom;

    d. segwitu u rispons xieraq tal-korp maniġerjali rigward sejbiet importanti mill-funzjonijiet ta' kontroll indipendenti rigward ir-riskju(i) tal-ICT, li jqisu d-delegazzjoni possibbli ta' ċerti aspetti għal kumitat, fejn dan jeżisti; u

e. li eċċezzjonijiet minn regolamenti u politiki tal-ICT applikabbli jiġu rreġistrati u soġġetti għal reviżjoni u rappurtar dokumentati mill-funzjoni ta' kontroll indipendenti b'attenzjoni fuq ir-riskji relatati.

3.3.3 Kopertura u sejbiet tal-awditjar intern

51. L-awtoritajiet kompetenti għandhom jikkunsidraw jekk l-Uffiċċju tal-Awditjar Intern ikunx effettiv fir-rigward tal-awditjar tal-qafas tal-ġestjoni tar-riskju tal-ICT applikabbli, billi jirrevedu jekk:

a. il-qafas tal-kontroll tar-riskju tal-ICT ikunx awditjat bil-kwalità, dettall u frekwenza meħtieġa u proporzjonali mad-daqs, mal-attivitajiet u mal-profil tar-riskju tal-ICT tal-istituzzjoni;

b. il-pjan tal-awditu jinkludix verifiki dwar ir-riskji kritiċi tal-ICT identifikati mill-istituzzjoni;

c. is-sejbiet tal-awditjar tal-ICT importanti, inkluż l-azzjonijiet miftiehma, jiġux irrappurtati lill-korp maniġerjali; u

d. is-sejbiet tal-awditjar tal-ICT, inkluż l-azzjonijiet miftiehma, jiġux segwiti u r-rapporti ta' progress jiġux perjodikament riveduti mill-maniġment superjuri u/jew mill-kumitat tal-awditjar.

3.3.4 Kontrolli tar-riskju tal-ICT li huma speċifiċi għar-riskji materjali tal-ICT identifikati

52. Għar-riskji materjali tal-ICT identifikati, l-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex kontrolli speċifiċi fis-seħħ biex dawn ir-riskji jiġu indirizzati. It-taqsimiet li ġejjin jipprovdu lista mhux eżawrjenti tal-kontrolli speċifiċi li għandhom jiġu kkunsidrati fil-valutazzjoni tar-riskji materjali identifikati taħt il-punt 3.2.3 li ġew irrappreżentati fil-kategoriji tar-riskju tal-ICT li ġejjin:

a. Riskji ta' disponibbiltà u kontinwità tal-ICT;
b. Riskji ta' sigurtà tal-ICT;
c. Riskji ta' bidla tal-ICT;
d. Riskji ta' integrità tad-data tal-ICT;
e. Riskji ta' esternalizzazzjoni tal-ICT.

(a) Kontrolli għall-ġestjoni ta' riskji ta' disponibbiltà u kontinwità materjali tal-ICT

53. Minbarra r-rekwiżiti fil-Linji Gwida tal-EBA SREP (para 279 - 281), l-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex qafas xieraq fis-seħħ għall-identifikazzjoni, il-fehim, il-kejl u l-mitigazzjoni ta' riskji ta' disponibbiltà u kontinwità tal-ICT.

54. Għal din il-valutazzjoni, l-awtoritajiet kompetenti, b'mod partikolari, għandhom iqisu jekk il-qafas:

a. jidentifikax il-proċessi kritiċi tal-ICT u s-sistemi ta' appoġġ tal-ICT rilevanti li għandhom ikunu parti mill-pjanijiet ta' kontinwità u reżiljenza tan-negozju b':

i. analiżi komprensiva tad-dipendenzi bejn il-proċessi kritiċi tan-negozju u s-sistemi ta' appoġġ;

ii. determinazzjoni ta' għanijiet ta' rkupru għas-sistemi ta' appoġġ tal-ICT (eż. tipikament determinati min-negozju u/jew mir-regolamenti f'termini ta' RTO u RPO);

iii. ippjanar ta' kontinġenza xieraq biex id-disponibbiltà, il-kontinwità u l-irkupru ta' sistemi u servizzi kritiċi tal-ICT ikunu jistgħu jimminimizzaw it-tfixkil tal-operazzjonijiet ta' istituzzjoni fi ħdan limiti aċċettabbli.

b. ikollux reżiljenza tan-negozju, politiki u standards ambjentali dwar il-kontroll tal-kontinwità u kontrolli operazzjonali li jinkludu:

i. Miżuri biex jiġi evitat li xenarju, inċident jew diżastru wieħed ikun jista' jħalli impatt kemm fuq is-sistemi ta' produzzjoni kif ukoll fuq dawk ta' rkupru tal-ICT;

ii. proċeduri ta' backup u ta' rkupru tas-sistema tal-ICT għal softwer u data kritiċi, li jiżguraw li dawn il-backups jinħażnu f'post sigur u biżżejjed remot, sabiex inċident jew diżastru ma jkunx jista' jeqred jew jikkorrompi din id-data kritika;

iii. sistemi ta' monitoraġġ għad-detezzjoni f'waqtha ta' inċidenti ta' disponibbiltà u kontinwità tal-ICT;

iv. proċess dokumentat ta' ġestjoni u eskalazzjoni dwar l-inċidenti, li jipprovdi wkoll gwida dwar ir-rwoli u r-responsabbiltajiet differenti tal-ġestjoni u l-eskalazzjoni dwar l-inċidenti, il-membri tal-kumitat(i) tal-kriżi u l-linja ta' kmand f'każ ta' emerġenza;

v. miżuri fiżiċi li kemm jipproteġu l-infrastruttura kritika tal-ICT tal-istituzzjoni (eż. ċentri tad-data) minn riskji ambjentali (eż. għargħar u diżastri naturali oħrajn) kif ukoll li jiżguraw ambjent operattiv xieraq għal sistemi tal-ICT (eż. arja kundizzjonata);

vi. proċessi, rwoli u responsabbiltajiet biex jiġi żgurat ukoll li sistemi u servizzi esternalizzati tal-ICT ikunu koperti wkoll minn soluzzjonijiet u pjanijiet ta' reżiljenza u kontinwità xierqa tan-negozju;

vii. ippjanar tal-prestazzjoni u l-kapaċità tal-ICT u soluzzjonijiet ta' monitoraġġ tal-ICT għal sistemi u servizzi kritiċi tal-ICT b'rekwiżiti definiti ta' disponibbiltà, għad-detezzjoni f'waqtha ta' limitazzjonijiet importanti fuq il-prestazzjoni u l-kapaċità;

viii. soluzzjonijiet biex jiġu protetti attivitajiet jew servizzi kritiċi tal-internet (eż. servizzi tal-e-banking), fejn meħtieġ u xieraq, kontra ċ-ċaħda mis-servizz u ċiberattakki oħrajn mill-internet, bl-għan li jipprevjenu jew ixekklu l-aċċess għal dawn l-attivitajiet u s-servizzi.

c. jittestjax soluzzjonijiet ta' disponibbiltà u kontinwità tal-ICT, kontra firxa ta' xenarji realistiċi fosthom ċiberattakki, testijiet ta' fail-over u testijiet ta' back-ups għal softwer u data kritiċi li:

i. huma ppjanati, formalizzati u dokumentati, u r-riżultati tat-testijiet jintużaw biex tissaħħaħ l-effettività tas-soluzzjonijiet ta' disponibbiltà u kontinwità tal-ICT;

ii. jinkludu partijiet ikkonċernati u funzjonijiet fi ħdan l-organizzazzjoni, bħall-ġestjoni tal-linja operatorja, inkluż il-kontinwità tan-negozju, timijiet ta' rispons f'każ ta' inċident jew kriżi, kif ukoll partijiet ikkonċernati esterni rilevanti fl-ekosistema;

iii. il-korp maniġerjali u l-maniġment superjuri huma involuti fihom b'mod xieraq (eż. bħala parti mit-timijiet tal-ġestjoni tal-kriżijiet) u jiġu informati dwar ir-riżultati tat-testijiet.

(b) Kontrolli għall-ġestjoni ta' riskji ta' sigurtà materjali tal-ICT

55. L-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex qafas effettiv fis-seħħ għall-identifikazzjoni, il-ftehim, il-kejl u l-mitigazzjoni tar-riskju ta' sigurtà tal-ICT. Għal din il-valutazzjoni, l-awtoritajiet kompetenti, b'mod partikolari, għandhom iqisu jekk il-qafas jikkunsidrax:

a. rwoli u responsabbiltajiet iddefiniti b'mod ċar li jirrigwardaw:
   i. il-persuna(i) u/jew il-kumitati li huma responsabbli għall-ġestjoni ta' kuljum tas-sigurtà tal-ICT u għall-elaborazzjoni tal-politiki ġenerali tas-sigurtà tal-ICT, b'attenzjoni għall-indipendenza meħtieġa tagħhom;
   ii. it-tfassil, l-implimentazzjoni, il-ġestjoni u l-monitoraġġ tal-kontrolli tas-sigurtà tal-ICT;
   iii. il-protezzjoni ta' sistemi u servizzi kritiċi tal-ICT, pereżempju bl-adozzjoni ta' proċess tal-valutazzjoni tal-vulnerabbiltà, ġestjoni ta' softwer korrettiv, protezzjoni tal-punt tat-tmiem (eż. virus tal-malwer), għodod ta' detenzjoni u prevenzjoni ta' intrużjoni;
   iv. il-monitoraġġ, il-klassifikazzjoni u t-trattament ta' inċidenti ta' sigurtà esterni jew interni tal-ICT; inkluż ir-rispons għall-inċidenti u t-tkomplija u l-irkupru tas-sistemi u s-servizzi tal-ICT;
   v. valutazzjonijiet tat-theddid regolari u proattiv biex jinżammu kontrolli ta' sigurtà xierqa.

b. politika ta' sigurtà tal-ICT li tqis u, fejn xieraq, taderixxi għal standards ta' sigurtà u prinċipji ta' sigurtà tal-ICT li huma rikonoxxuti fuq livell internazzjonali (eż. il-"prinċipju tal-inqas privileġġ" jiġifieri l-limitazzjoni tal-aċċess għal-livell minimu li ser jippermetti l-funzjonament normali għall-ġestjoni tad-dritt ta' aċċess u l-prinċipju ta' "difiża profonda" jiġifieri mekkaniżmi ta' sigurtà fuq livelli differenti li jżidu s-sigurtà tas-sistema kollha kemm hi għat-tfassil ta' arkitettura ta' sigurtà);

c. proċess biex jiġu identifikati sistemi, servizzi u rekwiżiti ta' sigurtà proporzjonali tal-ICT li jirriflettu riskju ta' frodi potenzjali u/jew użu ħażin possibbli u/jew abbużi ta' data kunfidenzjali flimkien ma' aspettattivi ta' sigurtà dokumentati li dawn is-sistemi, is-servizzi u d-data identifikati tal-ICT għandhom jaderixxu għalihom, li għandhom ikunu allinjati mat-tolleranza tar-riskju tal-istituzzjoni u li għandhom ikunu mmonitorjati għall-implimentazzjoni korretta tagħhom;

d. proċess dokumentat ta' sigurtà ta' ġestjoni u eskalazzjoni dwar l-inċidenti, li jipprovdi gwida dwar ir-rwoli u r-responsabbiltajiet differenti tal-ġestjoni u tal-eskalazzjoni dwar l-inċidenti, il-membri tal-kumitat(i) tal-kriżi u l-linja ta' kmand f'każ ta' emerġenzi ta' sigurtà;

e. illoggjar tal-attivitajiet tal-utent u amministrattiv li jippermetti l-monitoraġġ effettiv u d-detezzjoni u r-rispons f'waqthom għal attività mhux awtorizzata; li jgħin fi jew iwettaq investigazzjonijiet tal-forensika ta' inċidenti ta' sigurtà. L-istituzzjoni għandu jkollha politiki ta' lloggjar fis-seħħ li jiddefinixxu tipi ta' reġistri xierqa li għandhom jinżammu u l-perjodu ta' żamma tagħhom;

f. kampanji jew inizjattivi ta' sensibilizzazzjoni u informazzjoni biex il-livelli kollha fl-istituzzjoni jiġu infurmati dwar l-użu sigur u l-protezzjoni tas-sistemi tal-ICT tal-istituzzjoni u r-riskji ewlenin ta' sigurtà tal-ICT (u oħrajn) li għandhom ikunu konxji tagħhom, b'mod partikolari li jirrigwardaw it-theddidiet ċibernetiċi eżistenti u li qed jevolvu (eż. virusijiet tal-kompjuter, abbużi jew attakki interni jew esterni possibbli, ċiberattakki) u r-rwol tagħhom fil-mitigazzjoni ta' ksur tas-sigurtà;

g. miżuri xierqa ta' sigurtà fis-seħħ (eż. CCTV, allarm kontra s-serq, bibien ta' sigurtà) biex jipprevjenu l-aċċess fiżiku mhux awtorizzat għal sistemi kritiċi u sensittivi tal-ICT (eż. ċentri tad-data);

h. miżuri biex is-sistemi tal-ICT jiġu protetti minn attakki mill-Internet (jiġifieri ċiberattakki) jew minn netwerks esterni oħrajn (eż. konnessjonijiet ta' telekomunikazzjoni tradizzjonali jew konnessjonijiet ma' sħab affidabbli). L-awtoritajiet kompetenti għandhom jirrevedu jekk il-qafas tal-istituzzjoni jikkunsidrax:

   i. proċess u soluzzjonijiet biex iżomm inventarju sħiħ u aġġornat u ħarsa ġenerali tal-punti ta' konnessjoni kollha tan-netwerk li jħarsu 'l barra (eż. siti web, applikazzjonijiet tal-internet, WIFI, aċċess remot) li permezz tagħhom il-partijiet terzi jkunu jistgħu jidħlu fis-sistemi interni tal-ICT.

   ii. miżuri ta' sigurtà mmaniġġjati u mmonitorjati mill-viċin (eż. firewalls, proxy servers, mail relays, antivirus u skanners tal-kontenut) biex jiġi żgurat traffiku tan-netwerk dieħel u ħiereġ (eż. posta elettronika) u l-konnessjonijiet tan-netwerk li jħarsu 'l barra li permezz tagħhom il-partijiet terzi jkunu jistgħu jidħlu fis-sistemi interni tal-ICT;

   iii. proċessi u soluzzjonijiet biex jiġu żgurati siti web u applikazzjonijiet li jistgħu jiġu attakkati direttament mill-internet u/jew minn barra, li jistgħu jservu bħala punt ta' dħul fis-sistemi interni tal-ICT. B'mod ġenerali dawn jinkludu taħlita ta' prattiki ta' żvilupp sigur rikonoxxuti, prattiki ta' twebbis u skennjar tal-vulnerabbiltà tas-sistema tal-ICT, u/jew l-implimentazzjoni ta' soluzzjonijiet ta' sigurtà addizzjonali, bħal pereżempju firewalls tal-applikazzjonijiet u/jew sistemi ta' detezzjoni ta' intrużjoni (IDS) u/jew sistemi ta' prevenzjoni ta' intrużjoni (IPS);

   iv. ittestjar tal-penetrazzjoni tas-sigurtà perjodiku biex tiġi vvalutata l-effettività tal-miżuri u l-proċessi ta' sigurtà interna u ċibernetika tal-ICT implimentati. Dawn it-testijiet għandhom isiru mill-persunal u/jew minn esperti esterni bl-għarfien espert meħtieġ, fejn ir-riżultati u l-konklużjonijiet tat-testijiet dokumentati jiġu rrappurtati lill-maniġment superjuri u/jew lill-korp maniġerjali. Fejn meħtieġ u applikabbli, l-istituzzjoni minn dawn it-testijiet għandha titgħallem fejn tkompli ttejjeb il-kontrolli u l-proċessi tas-sigurtà u/jew tikseb assigurazzjoni aħjar dwar l-effettività tagħhom.

(c) Kontrolli għall-ġestjoni ta' riskji ta' bidla materjali fl-ICT

56. L-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex qafas effettiv fis-seħħ għall-identifikazzjoni, il-ftehim, il-kejl u l-mitigazzjoni tar-riskju ta' bidla tal-ICT proporzjonali man-natura, l-iskala u l-kumplessità tal-attivitajiet tal-istituzzjoni u tal-profil tar-riskju tal-ICT tal-istituzzjoni. Il-qafas tal-istituzzjoni għandu jkopri r-riskji assoċjati mal-iżvilupp, l-ittestjar u l-approvazzjoni ta' bidliet fis-sistemi tal-ICT, inkluż l-iżvilupp jew bidliet fis-softwer, qabel ma jittieħdu għall-ambjent tal-produzzjoni u jiżguraw ġestjoni adegwata taċ-ċiklu tal-ħajja tal-ICT. Għal din il-valutazzjoni, l-awtoritajiet kompetenti, b'mod partikolari, għandhom iqisu jekk il-qafas jikkunsidrax:

   a. proċessi dokumentati għall-ġestjoni u l-kontroll ta' bidliet fis-sistemi (eż. konfigurazzjoni u ġestjoni ta' softwer korrettiv) u data (eż. korrezzjonijiet ta' bugs jew korrezzjonijiet ta' data) tal-ICT, li jiżguraw l-involviment xieraq tal-ġestjoni tar-riskju tal-ICT għal bidliet importanti tal-ICT li jistgħu jħallu impatt sinifikanti fuq il-profil tar-riskju jew l-esponiment tal-istituzzjoni;

   b. speċifikazzjonijiet li jirrigwardaw is-segregazzjoni tad-doveri meħtieġa matul il-fażijiet differenti tal-proċessi ta' bidla tal-ICT implimentati (eż. tfassil tas-soluzzjoni u żvilupp, ittestjar u approvazzjoni ta'

softwer ġdid u/jew bidliet, migrazzjoni u implimentazzjoni fl-ambjent ta' produzzjoni, u korrezzjoni ta' bugs), b'attenzjoni fuq is-soluzzjonijiet implimentati u s-segregazzjoni tad-doveri biex jiġu mmaniġġjati u kkontrollati bidliet għas-sistemi u d-data ta' produzzjoni tal-ICT mill-persunal tal-ICT (eż. żviluppaturi, amministraturi tas-sistema tal-ICT, amministraturi tal-bażi tad-data) jew kwalunkwe parti oħra (eż. utenti ta' negozju, fornituri ta' servizz);

c. ambjenti tal-ittestjar li jirriflettu b'mod xieraq ambjenti ta' produzzjoni;

d. inventarju tal-assi tal-applikazzjonijiet u s-sistemi tal-ICT eżistenti fl-ambjent tal-produzzjoni, kif ukoll fl-ambjent tal-ittestjar u tal-iżvilupp, sabiex il-bidliet meħtieġa (eż. aġġornamenti jew titjib tal-verżjoni, patching tas-sistemi, bidliet fil-konfigurazzjoni) ikunu jistgħu jiġu mmaniġġjati, implimentati u mmonitorjati kif suppost għas-sistemi tal-ICT involuti.

e. proċess li jimmonitorja u jimmaniġġja ċ-ċiklu tal-ħajja tas-sistemi tal-ICT użati, biex jiġi żgurat li jkomplu jissodisfaw u jappoġġjaw ir-rekwiżiti tan-negozju u tal-ġestjoni tar-riskju attwali u li jiżgura li s-soluzzjonijiet u s-sistemi tal-ICT użati għadhom appoġġjati mill-bejjiegħa tagħhom; u li dan ikun akkompanjat bi proċeduri adegwati taċ-ċiklu tal-ħajja tal-iżvilupp tas-softwer (SDLC).

f. sistema ta' kontroll tal-kodiċi tas-sors bħala softwer u proċeduri xierqa biex jiġu evitati bidliet mhux awtorizzati fil-kodiċi tas-sors ta' softwer li jiġi żviluppat internament;

g. proċess li jwettaq skrinjar tas-sigurtà u tal-vulnerabbiltà ta' sistemi u softwer tal-ICT ġodda jew immodifikati materjalment, qabel ma jinħarġu għall-produzzjoni u jiġu esposti għal ċiberattakki possibbli;

h. proċess u soluzzjonijiet biex jiġi evitat l-iżvelar mhux awtorizzat jew mhux intenzjonat ta' data kunfidenzjali, meta jiġu sostitwiti, arkivjati, mormija jew meqruda sistemi tal-ICT;

i. reviżjoni indipendenti u proċessi ta' validazzjoni biex jitnaqqsu r-riskji għall-iżbalji tal-bnedmin meta jsiru bidliet għas-sistemi tal-ICT li jista' jkollhom effett negattiv importanti fuq id-disponibbiltà, il-kontinwità jew is-sigurtà tal-istituzzjoni (eż. bidliet importanti għall-konfigurazzjoni tal-firewall), jew is-sigurtà tal-istituzzjoni (eż. bidliet lill-firewalls).

(d) Kontrolli għall-ġestjoni ta' riskji ta' integrità ta' data materjali tal-ICT;

57. L-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex qafas effettiv fis-seħħ għall-identifikazzjoni, il-ftehim, il-kejl u l-mitigazzjoni tar-riskju tal-integrità tad-data tal-ICT proporzjonali man-natura, l-iskala u l-kumplessità tal-attivitajiet tal-istituzzjoni u tal-profil tar-riskju tal-ICT tal-istituzzjoni. Il-qafas tal-istituzzjoni għandu jikkunsidra r-riskji assoċjati mal-preservazzjoni tal-integrità tad-data maħżuna u pproċessata mis-sistemi tal-ICT. Għal din il-valutazzjoni, l-awtoritajiet kompetenti, b'mod partikolari, għandhom iqisu jekk il-qafas jikkunsidrax:

a. politika li tiddefinixxi r-rwoli u r-responsabbiltajiet għall-ġestjoni tal-integrità tad-data fis-sistemi tal-ICT (eż. perit tad-data, uffiċjali tad-data[6], kustodji tad-data[7], sidien/amministraturi (stewards)

[6] Uffiċjal tad-data hu responsabbli għall-ipproċessar u l-użu tad-data.

[7] Kustodju tad-data hu responsabbli għall-kustodja, it-trasport u l-ħżin sigur tad-data.

tad-data[8]) u li tipprovdi gwida dwar liema data hi kritika minn perspettiva ta' integrità tad-data u liem għandha tkun soġġetta għal kontrolli (eż. kontrolli tal-validazzjoni tal-input awtomatizzati, kontrolli tat-trasferiment tad-data, rekonċiljazzjonijiet, eċċ.) jew reviżjonijiet (eż. verifika tal-kompatibbiltà mal-arkitettura tad-data) speċifiċi tal-ICT fil-fażijiet differenti taċ-ċiklu tal-ħajja tad-data tal-ICT;

b. arkitettura tad-data, mudell u/jew dizzjunarju tad-data dokumentat, li jkun validat ma' partijiet ikkonċernati rilevanti tan-negozju u tal-IT biex tiġi żgurata l-konsistenza tad-data meħtieġa madwar is-sistemi tal-ICT u biex jiġi żgurat li l-arkitettura tad-data, il-mudell u/jew id-dizzjunarju tad-data jibqgħu allinjati mal-ħtiġijiet tal-ġestjoni tan-negozju u tar-riskju;

c. politika li tirrigwarda l-użu permess ta' u d-dipendenza fuq l-Informatika tal-Utent Finali, b'mod partikolari li tirrigwarda l-identifikazzjoni, ir-reġistrazzjoni u d-dokumentazzjoni ta' soluzzjonijiet importanti tal-informatika tal-utent finali (eż. meta tiġi pproċessata data importanti) u l-livelli ta' sigurtà mistennija biex jiġu evitati modifiki mhux awtorizzati, kemm fl-għodda nnifisha, kif ukoll fid-data maħżuna fiha;

d. proċessi dokumentati tat-trattament tal-eċċezzjonijiet biex jiġu solvuti kwistjonijiet ta' integrità tad-data tal-ICT identifikati f'konformità mal-kritikalità u s-sensittività tagħhom.

58. Għal istituzzjonijiet sorveljati li jaqgħu taħt il-kamp ta' applikazzjoni tal-prinċipji tal-BCBS 239 għall-aggregazzjoni tad-data ta' riskju u r-rappurtar tar-riskji effettivi (principles for effective risk data aggregation and risk reporting)[9], l-awtoritajiet kompetenti għandhom jirrevedu l-analiżi tar-riskju tal-istituzzjoni tal-kapaċitajiet tar-rappurtar tar-riskji u tal-aggregazzjoni tad-data tagħha mqabbla mal-prinċipji u d-dokumentazzjoni ppreparata fuqhom, filwaqt li jqisu l-iskeda taż-żmien tal-implimentazzjoni u l-ftehimiet tranżizzjonali f'dawn il-prinċipji.

(e) Kontrolli għall-ġestjoni ta' riskji ta' esternalizzazzjoni materjali tal-ICT

59. L-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istrateġija tal-esternalizzazzjoni tal-istituzzjoni, f'konformità mar-rekwiżiti tal-Linji Gwida tas-CEBS dwar l-esternalizzazzjoni (2006) u b'żieda mar-rekwiżit fil-paragrafu 85 (d) tal-Linji Gwida tal-EBA SREP, tapplikax b'mod adegwat għall-esternalizzazzjoni tal-ICT, inkluż esternalizzazzjoni intragrupp li tipprovdi servizzi tal-ICT fi ħdan il-grupp. Meta jkunu qed jivvalutaw ir-riskji ta' esternalizzazzjoni tal-ICT, l-awtoritajiet kompetenti għandhom iqisu li r-riskji ta' esternalizzazzjoni tal-ICT jistgħu jiġu koperti wkoll bħala parti mill-valutazzjoni ta' riskji operazzjonali inerenti taħt il-paragrafu 240 (j) tal-Linji Gwida tal-EBA SREP, biex jiġi evitat xogħol doppju jew għadd doppju.

60. B'mod partikolari, l-awtoritajiet kompetenti għandhom jivvalutaw jekk l-istituzzjoni għandhiex qafas effettiv fis-seħħ għall-identifikazzjoni, il-fehim u l-kejl tar-riskju ta' esternalizzazzjoni tal-ICT, u b'mod partikolari, kontrolli u ambjent ta' kontroll fis-seħħ għall-mitigazzjoni tar-riskji relatati ma' servizzi

[8] Amministratur tad-data hu responsabbli għall-ġestjoni u l-idoneità tal-elementi tad-data – kemm il-kontenut kif ukoll il-metadata.

[9] Kumitat ta' Basel dwar is-Superviżjoni Bankarja, Prinċipji għall-aggregazzjoni tad-data ta' riskju u r-rappurtar tar-riskji effettivi, Jannar 2013, disponibbli online: http://www.bis.org/publ/bcbs239.pdf.

esternalizzati materjali tal-ICT li huma proporzjonali għad-daqs, mal-attivitajiet u mal-profil tar-riskju tal-ICT tal-istituzzjoni u jinkludu:

a. valutazzjoni tal-impatt tal-esternalizzazzjoni tal-ICT fuq il-ġestjoni tar-riskju tal-istituzzjoni relatata mal-użu ta' forniturі ta' servizz (eż. forniturі ta' servizz ta' cloud) u s-servizzi tagħhom matul il-proċess ta' akkwist li hu dokumentat u li jitqies mill-maniġment superjuri jew mill-korp maniġerjali għad-deċiżjoni dwar jekk is-servizzi jiġux esternalizzati jew le. L-istituzzjoni għandha tirrevedi l-politiki tal-ġestjoni tar-riskju tal-ICT u l-kontrolli tal-ICT u l-ambjent ta' kontroll tal-fornitur tas-servizz biex jiġi żgurat li jissodisfaw l-għanijiet tal-ġestjoni tar-riskju u l-aptit għar-riskju interni tal-istituzzjoni. Din ir-reviżjoni għandha tiġi aġġornata perjodikament matul il-perjodu tal-esternalizzazzjoni kuntrattwali, filwaqt li jitqiesu l-karatteristiċi tas-servizzi esternalizzati;

b. monitoraġġ tar-riskji tal-ICT tas-servizzi esternalizzati matul il-perjodu tal-esternalizzazzjoni kuntrattwali bħala parti mill-ġestjoni tar-riskju tal-istituzzjoni, li jikkontribwixxi għar-rappurtar tal-ġestjoni tar-riskju tal-ICT tal-istituzzjoni (eż. rappurtar dwar il-kontinwità tan-negozju, rappurtar dwar is-sigurtà);

c. monitoraġġ u paragun tal-livelli ta' servizz riċevuti mal-livelli ta' servizz miftiehma kuntrattwalment li għandhom jiffurmaw parti mill-kuntratt tal-esternalizzazzjoni jew mill-ftehim dwar il-livell ta' servizz (FLS); u

d. persunal, riżorsi u kompetenzi adegwati biex jiġu mmonitorjati u amministrati r-riskji tal-ICT mis-servizzi esternalizzati.

3.4 Sommarju tas-sejbiet u għoti ta' punteġġ

61. Wara l-valutazzjoni ta' hawn fuq, l-awtoritajiet kompetenti għandhom jiffurmaw opinjoni dwar ir-riskju tal-ICT tal-istituzzjoni. Din l-opinjoni għandha tkun riflessa f'sommarju tas-sejbiet li l-awtoritajiet kompetenti għandhom jikkunsidraw meta jassenjaw il-punteġġ tar-riskju operazzjonali fit-Tabella 6 tal-Linji Gwida tal-EBA SREP. L-awtoritajiet kompetenti għandhom jibbażaw il-perspettiva tagħhom fuq ir-riskji materjali tal-ICT filwaqt li jqisu l-kunsiderazzjonijiet li ġejjin biex jikkontribwixxu għall-valutazzjoni tar-riskji operazzjonali:

a. Kunsiderazzjonijiet tar-Riskju

   i. Il-profil tar-riskju tal-ICT u l-esponimenti tal-istituzzjoni;
   ii. Is-sistemi u s-servizzi kritiċi tal-ICT identifikati; u
   iii. Il-materjalità tar-riskju tal-ICT li jirrigwarda sistemi kritiċi tal-ICT.

b. Kunsiderazzjonijiet tal-Ġestjoni u tal-Kontrolli

   i. Jekk hemmx konsistenza bejn il-politika u l-istrateġija tal-ġestjoni tar-riskju tal-ICT tal-istituzzjoni u l-istrateġija ġenerali u l-aptit għar-riskju tagħha.
   ii. Jekk il-qafas organizzazzjonali għall-ġestjoni tar-riskju tal-ICT ikunx robust b'responsabbiltajiet ċari u b'separazzjoni ċara tal-kompiti bejn is-siedien tar-riskju u l-funzjonijiet tal-ġestjoni u tal-kontroll;
   iii. Jekk is-sistemi tal-kejl, tal-monitoraġġ u tar-rappurtar tar-riskju tal-ICT ikunux xierqa; u
   iv. Jekk l-oqfsa tal-kontroll għar-riskji materjali tal-ICT humiex b'saħħithom.

62. Jekk l-awtoritajiet kompetenti jqisu r-riskju tal-ICT bħala materjali u l-awtorità kompetenti tiddeċiedi li tivvaluta u tagħti punteġġ lil dan ir-riskju bħala subkategorija ta' riskju operazzjonali, it-tabella ta' hawn taħt (Tabella 1) tagħti l-kunsiderazzjonijiet tal-punteġġ tar-riskju tal-ICT.

Tabella 1: Kunsiderazzjonijiet superviżorji għall-assenjament ta' punteġġ tar-riskju tal-ICT

Punteġġ tar-Riskju	Perspettiva superviżorja	Kunsiderazzjonijiet għal riskju inerenti	Kunsiderazzjonijiet għal ġestjoni u kontrolli adegwati
1	Ma jidher li hemm l-ebda riskju ta' impatt prudenzjali sinifikanti fuq l-istituzzjoni meta jitqies il-livell tar-riskju inerenti u l-ġestjoni u l-kontrolli.	• Is-sorsi tal-informazzjoni li għandhom jiġu kkunsidrati taħt il-paragrafu 37 ma żvelaw l-ebda esponimenti sinifikanti għar-riskju tal-ICT. • In-natura tal-profil tar-riskju tal-ICT tal-istituzzjoni, flimkien mar-reviżjoni tas-sistemi kritiċi tal-ICT u r-riskji materjali tal-ICT għas-Sistemi u s-Servizzi tal-ICT ma żvelaw l-ebda riskji materjali tal-ICT.	• Il-politika u l-istrateġija tar-riskju tal-ICT tal-istituzzjoni huma proporzjonali mal-istrateġija ġenerali u l-aptit għar-riskju tagħha. • Il-qafas organizzazzjonali għar-riskju tal-ICT hu robust b'responsabbiltajiet ċari u b'separazzjoni ċara tal-kompiti bejn is-sidien tar-riskju u l-funzjonijiet tal-ġestjoni u tal-kontroll. • Is-sistemi tal-kejl, tal-monitoraġġ u tar-rappurtar tar-riskju tal-ICT huma xierqa. • Il-qafas tal-kontroll għar-riskju tal-ICT hu b'saħħtu.
2	Hemm riskju baxx ta' impatt prudenzjali sinifikanti fuq l-istituzzjoni meta jitqies il-livell tar-riskju inerenti u l-ġestjoni u l-kontrolli.	• Is-sorsi tal-informazzjoni li għandhom jiġu kkunsidrati taħt il-paragrafu 37 ma żvelaw l-ebda esponimenti sinifikanti għar-riskju tal-ICT. • In-natura tal-profil tar-riskju tal-ICT tal-istituzzjoni, flimkien mar-reviżjoni tas-sistemi kritiċi tal-ICT u r-riskji materjali tal-ICT għas-Sistemi u s-Servizzi tal-ICT żvelaw esponiment limitat għar-riskju tal-ICT (eż. mhux aktar minn 2 minn 5 tal-kategoriji tar-riskji tal-ICT iddefiniti minn qabel).	
3	Hemm riskju medju ta' impatt prudenzjali sinifikanti fuq l-istituzzjoni meta jitqies il-livell tar-riskju inerenti u tal-ġestjoni u tal-kontrolli.	• Is-sorsi tal-informazzjoni li għandhom jiġu kkunsidrati taħt il-paragrafu 37 żvelaw indikazzjonijiet ta' esponimenti sinifikanti potenzjali għar-riskju tal-ICT. • In-natura tal-profil tar-riskju tal-ICT tal-istituzzjoni, flimkien mar-reviżjoni tas-sistemi kritiċi tal-ICT u	

		r-riskji materjali tal-ICT għas-Sistemi u s-Servizzi tal-ICT żvelaw esponiment miżjud għar-riskju tal-ICT (eż. 3 jew aktar minn 5 tal-kategoriji tar-riskji tal-ICT iddefiniti minn qabel).	
4	Hemm riskju għoli ta' impatt prudenzjali sinifikanti fuq l-istituzzjoni meta jitqies il-livell tar-riskju inerenti u l-ġestjoni u l-kontrolli.	• Is-sorsi tal-informazzjoni li għandhom jiġu kkunsidrati taħt il-paragrafu 37 ipprovdew diversi indikazzjonijiet ta' esponimenti sinifikanti għar-riskju tal-ICT. • In-natura tal-profil tar-riskju tal-ICT tal-istituzzjoni, flimkien mar-reviżjoni tas-sistemi kritiċi tal-ICT u r-riskji materjali tal-ICT għas-Sistemi u s-Servizzi tal-ICT żvelaw esponiment għoli għar-riskju tal-ICT (eż. 4 jew 5 minn 5 tal-kategoriji tar-riskji tal-ICT iddefiniti minn qabel).	

Anness – Tassonomija tar-Riskju tal-ICT

5 kategoriji tar-riskju tal-ICT b'lista mhux eżawrjenti tar-riskji tal-ICT b'severità għolja u/jew b'impatt operazzjonali, reputazzjonali jew finanzjarju potenzjali

Kategoriji tar-riskju tal-ICT	Riskji tal-ICT (mhux eżawrjenti[10])	Deskrizzjoni tar-riskju	Eżempji
Riskji ta' disponibbiltà u kontinwità tal-ICT	Ġestjoni inadegwata tal-kapaċità	Nuqqas ta' riżorsi (eż. ħardwer, sosftwer, persunal, fornituri ta' servizz) jista' jirriżulta f'inabbiltà li s-servizz jiżdied biex jissodisfa l-ħtiġijiet tan-negozju, f'interruzzjonijiet tas-sistema, f'degradazzjoni tas-servizz u/jew fi żbalji operazzjonali.	• Nuqqas fil-kapaċità jista' jaffettwa r-rati tat-trażmissjoni u d-disponibbiltà tan-netwerk (internet) għal servizzi bħall-internet banking (ibbankjar bl-internet). • Nuqqas ta' persunal (intern jew ta' parti terza) jista' jirriżulta f'interruzzjonijiet tas-sistema u/jew fi żbalji operazzjonali.
	Nuqqasijiet tas-sistema tal-ICT	Telf ta' disponibbiltà minħabba problemi fil-ħardwer.	• Nuqqas/funzjonament ħażin tal-ħżin (diski riġidi), tas-server jew ta' tagħmir ieħor tal-ICT ikkawżat minn, pereżempju, nuqqas ta' manutenzjoni.
		Telf ta' disponibbiltà minħabba nuqqasijiet fis-softwer u bugs.	• Ċirkwit infinit fis-softwer tal-applikazzjoni jipprevjeni l-eżekuzzjoni tat-tranżazzjoni. • Interruzzjonijiet minħabba l-użu kontinwu ta' sistemi u soluzzjonijiet antikwati li m'għadhomx jissodisfaw ir-rekwiżiti preżenti tad-disponibbiltà u tar-reżiljenza u/jew li m'għadhomx aktar appoġġjati mill-bejjiegħa tagħhom.
	Ippjanar inadegwat ta' kontinwità u rkupru minn diżastri tal-ICT	Nuqqas ta' soluzzjonijiet ta' disponibbiltá u/jew ta' kontinwitá u/jew ta' rkupru minn diżastri tal-ICT ippjanati (eż. ċentru tad-data ta' rkupru ta' riżerva) meta jiġu attivati b'risposta għal aċċident.	• Differenzi fil-konfigurazzjoni bejn iċ-ċentru tad-data primarju u dak sekondarju jistgħu jirriżultaw fl-inkapaċità li ċ-ċentru tad-data ta' riżerva jipprovdi l-kontinwità ppjanata tas-servizz.

[10] Ir-riskji tal-ICT jitniżżlu taħt il-kategorija tar-riskju li l-aktar ikollhom impatt fuqha iżda jista' jkollhom impatt fuq kategoriji tar-riskju oħrajn

Kategoriji tar-riskju tal-ICT	Riskji tal-ICT (mhux eżawrjenti[10])	Deskrizzjoni tar-riskju	Eżempji
	Ċiberattakki ta' tfixkil u distruttivi	Attakki għal finijiet differenti (eż. attiviżmu, rikattar), li jirriżultaw f'tagħbija eċċessiva tas-sistemi u n-netwerk, li jipprevjenu l-aċċess għas-servizzi online tal-kompjuter mill-utenti leġittimi tagħhom.	• Attakki ta' Ċaħda mis-Servizz Distribwiti jitwettqu permezz ta' numru kbir ta' sistemi tal-kompjuter fuq l-internet ikkontrollati minn hacker, li jibagħtu numru kbir ta' talbiet għas-servizzi li jidhru leġittimi lis-servizzi tal-internet (eż. e-banking).
Riskji ta' sigurtà tal-ICT	Ċiberattakki u attakki oħrajn esterni bbażati fuq l-ICT	Attakki li jitwettqu mill-internet jew minn netwerks ta' barra għal finijiet differenti (eż. frodi, spjunaġġ, attiviżmu / sabotaġġ, terroriżmu ċibernetiku) bl-użu ta' varjetà ta' tekniki (eż. social engineering, attentati ta' intrużjoni permezz tal-isfruttament tal-vulnerabbiltajiet, skjerament ta' softwer malizzjuż) jirriżultaw fit-teħid tal-kontroll tas-sistemi interni tal-ICT.	Tipi differenti ta' attakki: • APT (Theddida Persistenti Avvanzata) biex jittieħed il-kontroll ta' sistemi interni jew biex tinsteraq informazzjoni (eż. informazzjoni relatata mas-serq ta' identità, informazzjoni tal-karta tal-kreditu). • Softwer malizzjuż (eż. programm ta' riskatt) li jikkodifika d-data bl-għan ta' rikattar. • Infezzjoni ta' sistemi interni tal-ICT b'Trojan horses biex jitwettqu azzjonijiet ta' ħsara fis-sistemi bil-moħbi. • Sfruttament tas-sistema tal-ICT u/jew vulnerabbiltajiet tal-applikazzjoni (tal-web) (eż. injezzjoni SQL ...) biex jinkiseb l-aċċess għas-sistema interna tal-ICT.
		Eżekuzzjoni ta' tranżazzjonijiet ta' pagament frodulenti minn hackers permezz tal-ksur jew taċ-ċirkomvenzjoni tas-sigurtà tal-e-banking u tas-servizzi ta' pagament u/jew bl-attakk u l-isfruttament tal-vulnerabbiltajiet tas-sigurtà fis-sistemi interni ta' pagament tal-istituzzjoni.	• Attakki kontra servizzi tal-e-banking jew ta' pagament bl-għan li jsiru tranżazzjonijiet mhux awtorizzati. • Il-ħolqien u l-ibgħit ta' tranżazzjonijiet ta' pagament frawdolenti minn ġewwa s-sistemi interni ta' pagament tal-istituzzjoni (eż. messaġġi frawdolenti SWIFT).
		Eżekuzzjoni ta' tranżazzjonijiet ta' titoli frawdolenti minn hackers permezz tal-ksur jew taċ-ċirkomvenzjoni tas-sigurtà tas-servizzi tal-e-banking li wkoll jipprovdu aċċess għall-kontijiet tat-titoli tal-klijent.	• Attakki "pump and dump" fejn l-aggressuri jiksbu l-aċċess għall-kontijiet tat-titoli tal-e-banking tal-klijenti u jagħmlu ordnijiet ta' xiri jew bejgħ frodulenti biex jinfluwenzaw il-prezz tas-suq u/jew jagħmlu qligħ fuq bażi ta' pożizzjonijiet ta' titoli

Kategoriji tar-riskju tal-ICT	Riskji tal-ICT (mhux eżawrjenti[10])	Deskrizzjoni tar-riskju	Eżempji
			stabbiliti qabel.
		Attakki fuq konnessjonijiet ta' komunikazzjoni u konverżazzjonijiet tat-tipi kollha ta' sistemi tal-ICT bl-għan li tinġabar informazzjoni u/jew jitwettaq frodi.	• Smigħ sigriet/interċettazzjoni ta' trażmissjoni mhux protetta ta' data ta' awtentifikazzjoni bħala test sempliċi.
	Sigurtà interna inadegwata tal-ICT	Kisba ta' aċċess mhux awtorizzat għal sistemi kritiċi tal-ICT minn ġewwa l-istituzzjoni għal finijiet differenti (eż. frodi, it-twettiq u l-ħabi ta' attivitajiet ta' negozju illegali, serq ta' data, attiviżmu / sabotaġġ) permezz ta' varjetà ta' tekniki (eż. abbuż u/jew eskalazzjoni tal-privileġġi, serq ta' identità, social engineering, sfruttament ta' vulnerabbiltajiet fis-sistemi tal-ICT, skjerament ta' softwer malizzjuż).	• Installazzjoni ta' loggers tal-ittastjar (key loggers) biex jinsterqu IDs u passwords tal-utenti biex jinkiseb l-aċċess mhux awtorizzat għal data kunfidenzjali u/jew titwettaq frodi. • Cracking/Tbassir ta' passwords mhux b'saħħithom biex jinkisbu drittijiet ta' aċċess illeġittimi jew elevati. • Amministratur tas-sistema juża sistemi operattivi jew utilitajiet tal-bażi tad-data (għal modifiki diretti għall-bażi tad-data) biex iwettaq frodi.
		Manipulazzjonijiet tal-ICT mhux awtorizzati minħabba proċeduri u prattiki inadegwati tal-ġestjoni tal-aċċess tal-ICT.	• Nuqqas ta' diżattivazzjoni jew tħassir ta' kontijiet li mhumiex meħtieġa bħal dawk ta' persunal li bidel il-funzjonijiet u/jew telaq mill-istituzzjoni, inkluż mistiedna jew fornituri li m'għadx għandhom bżonn l-aċċess, li jipprovdi aċċess mhux awtorizzat lis-sistemi tal-ICT. • Għoti ta' drittijiet u privileġġi eċċessivi ta' aċċess u/jew isir possibbli li attivitajiet illegali jinħbew.
		Theddidiet għas-sigurtà minħabba nuqqas ta' sensibilizzazzjoni tas-sigurtà li minħabba fiha l-impjegati ma jifhmux, jittraskuraw jew jonqsu milli jaderixxu mal-politiki u l-proċeduri ta' sigurtà tal-ICT.	• Impjegati li jitqarrqu biex jipprovdu għajnuna għal attakk (jiġifieri social engineering). • Prattiċi ħżiena fir-rigward tal-kredenzjali: qsim ta' passwords, użu ta' passwords li "faċilment" jitbassru, użu tal-istess password għal ħafna finijiet differenti, eċċ. • Ħżin ta' data kunfidenzjali mhux ikkodifikata fuq laptops u soluzzjonijiet ta' ħżin ta' data portabbli (eż. stikek tal-USB) li jistgħu jintilfu jew jinsterqu.

Kategoriji tar-riskju tal-ICT	Riskji tal-ICT (mhux eżawrjenti[10])	Deskrizzjoni tar-riskju	Eżempji
		Il-ħżin jew it-trasferiment mhux awtorizzat ta' informazzjoni kunfidenzjali barra mill-istituzzjoni.	• Persuni li jisirqu jew li intenzjonalment jiżvelaw jew joħorġu bil-moħbi informazzjoni kunfidenzjali lil persuni mhux awtorizzati jew lill-pubbliku.
	Sigurtà fiżika inadegwata tal-ICT	Użu ħażin jew serq ta' assi tal-ICT permezz ta' aċċess fiżiku li jikkawża ħsara, telfien ta' assi jew data jew biex theddidiet oħra jsiru possibbli.	• Dħul fiżiku fil-bini għall-uffiċċji u/jew ċentri tad-data biex jinsteraq tagħmir tal-ICT (eż. kompjuters, laptops, soluzzjonijiet ta' ħżin) u/jew biex tiġi kkupjata data bl-aċċess fiżiku tas-sistemi tal-ICT.
		Ħsara intenzjonata jew aċċidentali lil assi fiżiċi tal-ICT kkawżati minn terroriżmu, aċċidenti jew manipulazzjonijiet sfortunati/żbaljati mill-persunal tal-istituzzjoni u/jew ta' partijiet terzi (fornituri, persuna li tagħmel tiswijiet).	• Terroriżmu fiżiku (jiġifieri bombi terroristiċi) jew sabotaġġ tal-assi tal-ICT. • Qerda ta' ċentru tad-data kkawżata minn nar, tnixxija tal-ilma jew fatturi oħrajn.
		Protezzjoni fiżika insuffiċjenti kontra diżastri naturali li tirriżulta f'qerda parzjali jew sħiħa ta' sistemi/ċentri tad-data tal-ICT minn diżastri naturali.	• Terremoti, sħana estrema, maltempati tar-riħ, maltempati tas-silġ qawwijin, għargħar, nar, sajjetti.
Riskji ta' bidla tal-ICT	Kontrolli inadegwati fuq bidliet fis-sistema tal-ICT u fuq l-iżvilupp tal-ICT	Inċidenti kkawżati minn żbalji jew vulnerabbiltajiet mhux skoperti bħala riżultat ta' bidla (eż. effetti mhux previsti ta' bidla jew bidla ġestita ħażin minħabba nuqqas ta' ttestjar jew prattiċi ta' ġestjoni ta' bidla mhux xierqa) lil eż. softwer, sistemi u data tal-ICT.	• Ħruġ għall-produzzjoni ta' softwer jew bidliet fil-konfigurazzjoni li ma ġewx ittestjati biżżejjed b'effetti negattivi mhux mistennija fuq data (eż. korruzzjoni, tħassir) u/jew fuq il-prestazzjoni tas-sistema tal-ICT (eż. waqfien, degradazzjoni fil-prestazzjoni). • Bidliet mhux ikkontrollati għal sistemi jew data tal-ICT fl-ambjent tal-produzzjoni. • Ħruġ għall-produzzjoni ta' sistemi tal-ICT u applikazzjonijiet tal-internet b'sigurtà baxxa, li joħloq opportunitajiet għal hackers biex jattakkaw is-servizzi tal-internet mogħtija u/jew jkissru s-sistemi interni tal-ICT. • Bidliet mhux ikkontrollati fil-kodiċi tas-sors ta' softwer żviluppat internament. • Ittestjar insuffiċjenti minħabba n-nuqqas ta'

Kategoriji tar-riskju tal-ICT	Riskji tal-ICT (mhux eżawrjenti[10])	Deskrizzjoni tar-riskju	Eżempji
			ambjenti tal-ittestjar adegwati.
	Arkitettura inadegwata tal-ICT	Ġestjoni tal-akritettura tal-ICT dgħajfa fit-tfassil, fil-bini u fil-manteniment ta' sistemi tal-ICT (eż. softwer, ħardwer, data) maż-żmien tista' twassal għal sistemi tal-ICT kumplessi, diffiċli, għaljin biex jiġu immaniġġjati u riġidi, li m'għadhomx biżżejjed allinjati mal-ħtiġijiet tan-negozju u, meta mqabbla mar-rekwiżiti tal-ġestjoni tar-riskju attwali, mhux qed ilaħħqu.	• Bidliet immaniġġjati ħażin lis-sistemi, softwer u/jew data tal-ICT fuq perjodu twil ta' żmien, li jwassal għal sistemi u arkitetturi tal-ICT kumplessi, eteroġeni u diffiċli biex jiġu mmaniġġjati, li jirriżultaw f'ħafna impatti negattivi fuq in-negozji u fuq il-ġestjoni tar-riskju (eż. nuqqas ta' flessibbiltà u aġilità, inċidenti u nuqqasijiet tal-ICT, kost operazzjonali għoli, sigurtà u reżiljenza mdgħajfa tal-ICT, tnaqqis fil-kwalità dat-data u fil-kapaċitajiet ta' rappurtar.) • Il-personalizzazzjoni u l-estensjoni estensiva ta' pakketti ta' softwer kummerċjali b'softwer żviluppat internament, li jwassal għall-inkapaċità li jiġu implimentati verżjonijiet u aġġornamenti futuri tas-softwer kummerċjali u għar-riskju li ma jibqax aktar appoġġjat mill-bejjiegħ.
	Ċiklu tal-ħajja u ġestjoni ta' softwer korrettiv inadegwati	In-nuqqas li jinżamm inventarju adegwat tal-assi kollha tal-ICT f'appoġġ, u flimkien ma', prattiċi taċ-ċiklu tal-ħajja u tal-ġestjoni ta' softwer korrettiv tajbin. Dan iwassal għal sistemi tal-ICT mhux patched biżżejjed (u għalhekk aktar vulnerabbli) u antikwati li ma jappoġġjawx il-ħtiġijiet tan-negozju u tal-ġestjoni tar-riskju.	• Sistemi tal-ICT mhux patched u antikwati li jistgħu joħolqu impatti negattivi fuq in-negozju u l-ġestjoni tar-riskju (eż. nuqqas ta' flessibbiltà u aġilità, interruzzjonijiet tal-ICT, sigurtà u reżiljenza mdgħajfa tal-ICT).
Riskji ta' integrità tad-data tal-ICT	Ipproċessar u mmaniġġjar tad-data tal-ICT li ma jaħdmux sew	Minħabba żbalji jew nuqqasijiet fis-sistema, fil-komunikazzjoni u/jew fl-applikazzjoni, jew minħabba l-proċess ta' estrazzjoni, trasferiment u llowdjar (ETL) tad-data li twettaq b'mod żbaljat, id-data tista' tiġi mħassra jew tintilef.	• Żball fis-sistema tal-IT fl-ipproċessar tal-lott, li joħloq bilanċi żbaljati fil-kontijiet tal-bank tal-klijent. • Domandi eżegwiti ħażin. • Telfien ta' data minħabba żball fir-replikazzjoni (backup) tad-data.
	Kontrolli ta' validazzjoni tad-	Żbalji relatati ma' input tad-data u kontrolli ta' approvazzjoni (eż. għal data użata ta' parti terza),	• Ifformattjar/validazzjoni insuffiċjenti jew invalidi ta' inputs tad-data f'applikazzjonijiet u/jew f'interfaċċi

Kategoriji tar-riskju tal-ICT	Riskji tal-ICT (mhux eżawrjenti[10])	Deskrizzjoni tar-riskju	Eżempji
	data mfassla ħażin f'sistemi tal-ICT	trasferiment, ipproċessar u kontrolli tal-output tad-data neqsin jew mhux effettivi fis-sistemi tal-ICT (eż. kontrolli ta' validità tal-input, rekonċiljazzjonijiet tad-data).	tal-utent. • Nuqqas ta' kontrolli ta' rikonċiljazzjoni tad-data fuq outputs prodotti • Nuqqas ta' kontrolli fuq il-proċessi tal-estrazzjoni tad-data eżegwiti (eż. domandi fuq il-bażi tad-data) li jwasslu għal data żbaljata. • Użu ta' data esterna difettuża.
	Bidliet fid-data kkontrollati ħażin fis-sistemi tal-produzzjoni tal-ICT.	Żbalji fid-data introdotti minħabba nuqqas ta' kontrolli fuq il-korrettezza u n-natura ġġustifikata tal-manipulazzjonijiet tad-data mwettqa fil-produzzjoni ta' sistemi tal-ICT	• Żviluppaturi jew amministraturi tal-bażi tad-data li jaċċessaw jew ibiddlu direttament id-data fis-sistemi tal-produzzjoni tal-ICT b'mod mhux kontrollat eż. fil-każ ta' inċident tal-ICT.
	Arkitettura tad-data, flussi tad-data, mudelli tad-data jew dizzjunarji tad-data mfassla u/jew immaniġġjati ħażin	Arkitettura tad-data, flussi tad-data, mudelli tad-data jew dizzjunarji tad-data mmaniġġjati ħażin jistgħu jirriżultaw f'diversi verżjonijiet tal-istess data matul is-sistemi tal-ICT, li m'għadhomx konsistenti minħabba mudelli tad-data jew definizzjonijiet tad-data applikati b'mod differenti u/jew differenzi fil-proċess sottostanti tal-ġenerazzjoni u tat-tibdil fid-data.	• L-eżistenza ta' bażijiet ta' data tal-klijenti differenti għal kull prodott jew unità tan-negozju b'definizzjonijiet u oqsma tad-data differenti, li tirriżulta f'data integrata dwar il-klijent mhux rikonċiljata u diffiċli li titqabbel fil-livell tal-istituzzjoni jew tal-grupp sħiħ.
Riskji ta' esternalizzazzjoni tal-ICT	Reżiljenza inadegwata ta' servizzi ta' parti terza jew ta' entità oħra tal-Grupp	In-nuqqas ta' disponibbiltà ta' servizzi tal-ICT, servizzi u utilitajiet tat-telekomunikazzjoni kritiċi esternalizzati. Telfien jew korruzzjoni ta' data kritika/sensittiva fdata lill-fornitur tas-servizz	• Indisponibbiltà ta' servizzi ewlenin bħala riżultat ta' nuqqasijiet fis-sistemi jew fl-applikazzjonijiet (esternalizzati) tal-ICT tal-forniturі. • Tfixkil fil-konnessjonijiet tat-telekomunikazzjoni. • Nuqqas fil-provvista tal-enerġija.
	Governanza ta' esternalizzazzjoni inadegwata	Degradazzjoni jew nuqqasijiet kbar fis-servizz minħabba tħejjija jew proċessi ta' kontroll ineffiċjenti tal-fornitur tas-servizz esternalizzat. Governanza ta' esternalizzazzjoni ineffettiva tista'	• Proċeduri ta' ġestjoni tal-inċidenti ħżiena, mekkaniżmi u garanziji ta' kontroll kuntrattwali mfassla fil-ftehim tal-fornitur tas-servizz li jżidu d-dipendenza fuq l-impjegat ewlieni fuq il-partijiet

Kategoriji tar-riskju tal-ICT	Riskji tal-ICT (mhux eżawrjenti[10])	Deskrizzjoni tar-riskju	Eżempji
		tirriżulta f'nuqqas ta' ħiliet u kapaċitajiet adegwati biex jiġu identifikati, ivvalutati, mitigati u mmonitorjati r-riskji tal-ICT u tista' tillimita l-kapaċitajiet operazzjonali tal-istituzzjonijiet.	terzi u l-bejjiegħa. • Kontrolli tal-ġestjoni tat-tibdil mhux xierqa li jikkonċernaw l-ambjent tal-ICT tal-fornitur tas-servizz jistgħu joħolqu degradazzjoni jew nuqqas kbir fis-servizz.
	Sigurtà inadegwata ta' parti terza jew ta' entità oħra tal-Grupp	Hacking tas-sistemi tal-ICT tal-partijiet terzi li jfornu s-servizz, b'impatt dirett fuq is-servizzi esternalizzati jew id-data kritika/kunfidenzjali maħżuna għand il-fornitur tas-servizz. Persunal tal-fornitur tas-servizz li jikseb aċċess mhux awtorizzat għal data kritika/sensittiva maħżuna għand il-fornitur tas-servizz	• Hacking ta' fornituri tas-servizz minn kriminali jew terroristi, bħala punt ta' dħul fis-sistemi tal-ICT tal-istituzzjonijiet jew biex jaċċessaw/jeqirdu data kritika jew sensittiva maħżuna għand il-fornitur tas-servizz. • Informazzjoni privileġġata malizzjuża min-naħa tal-fornitur tas-servizz li jipprova jisraq u jbigħ data sensittiva.