2024/1774

25.6.2024

REGOLAMENT DELEGAT TAL-KUMMISSJONI (UE) 2024/1774

tat-13 ta' Marzu 2024

li jissupplimenta r-Regolament (UE) 2022/2554 tal-Parlament Ewropew u tal-Kunsill fir-rigward ta' standards tekniċi regolatorji li jispeċifikaw l-għodod, il-metodi, il-proċessi u l-politiki tal-ġestjoni tar-riskju tal-ICT u l-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT

(Test b'rilevanza għaż-ŻEE)

IL-KUMMISSJONI EWROPEA,

Wara li kkunsidrat it-Trattat dwar il-Funzjonament tal-Unjoni Ewropea,

Wara li kkunsidrat ir-Regolament (UE) 2022/2554 tal-Parlament Ewropew u tal-Kunsill tal-14 ta' Diċembru 2022 dwar ir-reżiljenza operazzjonali diġitali għas-settur finanzjarju u li jemenda r-Regolamenti (KE) Nru 1060/2009, (UE) Nru 648/2012, (UE) Nru 600/2014, (UE) Nru 909/2014 u (UE) 2016/1011 ([1]), u b'mod partikolari l-Artikolu 15, ir-raba' subparagrafu, u l-Artikolu 16(3), ir-raba' subparagrafu tiegħu,

Billi:

(1) Ir-Regolament (UE) 2022/2554 ikopri varjetà wiesgħa ta' entitajiet finanzjarji li jvarjaw fid-daqs, fl-istruttura, fl-organizzazzjoni interna, u fin-natura u fil-kumplessità tal-attivitajiet tagħhom, u b'hekk żiedu jew naqqsu l-elementi ta' kumplessità jew riskji. Biex jiġi żgurat li dik il-varjetà titqies kif xieraq, kwalunkwe rekwiżit fir-rigward tal-politiki, tal-proċeduri, tal-protokolli u tal-għodod tas-sigurtà tal-ICT, u fir-rigward ta' qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT, jenħtieġ li jkun proporzjonat għal dak id-daqs, l-istruttura, l-organizzazzjoni interna, in-natura u l-kumplessità ta' dawk l-entitajiet finanzjarji u għar-riskji korrispondenti.

(2) Minħabba l-istess raġuni, l-entitajiet finanzjarji soġġetti għar-Regolament (UE) 2022/2554 jenħtieġ li jkollhom ċerta flessibbiltà fil-mod kif jikkonformaw ma' kwalunkwe rekwiżit fir-rigward tal-politiki, tal-proċeduri, tal-protokolli u tal-għodod tas-sigurtà tal-ICT, u fir-rigward ta' kwalunkwe qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT. Minħabba dik ir-raġuni, jenħtieġ li l-entitajiet finanzjarji jitħallew jużaw kwalunkwe dokumentazzjoni li diġà għandhom biex jikkonformaw ma' kwalunkwe rekwiżit ta' dokumentazzjoni li jirriżulta minn dawk ir-rekwiżiti. Minn dan jirriżulta li l-iżvilupp, id-dokumentazzjoni u l-implimentazzjoni ta' politiki speċifiċi tas-sigurtà tal-ICT jenħtieġ li jkunu meħtieġa biss għal ċerti elementi essenzjali, filwaqt li jitqiesu, fost l-oħrajn, il-prattiki u l-istandards ewlenin tal-industrija. Barra minn hekk, biex jiġu koperti aspetti speċifiċi ta' implimentazzjoni teknika, huwa meħtieġ li jiġu żviluppati, iddokumentati u implimentati proċeduri ta' sigurtà tal-ICT biex jiġu koperti aspetti speċifiċi ta' implimentazzjoni teknika, inklużi l-ġestjoni tal-kapaċità u tal-prestazzjoni, il-ġestjoni tal-vulnerabbiltà u tal-patches, is-sigurtà tad-*data* u tas-sistema, u r-reġistrazzjoni.

(3) Sabiex tiġi żgurata l-implimentazzjoni korretta maż-żmien tal-politiki, il-proċeduri, il-protokolli u l-għodod tas-sigurtà tal-ICT imsemmija fit-Titolu II, il-Kapitolu I ta' dan ir-Regolament, huwa importanti li l-entitajiet finanzjarji jassenjaw u jżommu b'mod korrett kwalunkwe rwol u responsabbiltà relatati mas-sigurtà tal-ICT, u li jistabbilixxu l-konsegwenzi tan-nuqqas ta' konformità mal-politiki jew mal-proċeduri tas-sigurtà tal-ICT.

(4) Sabiex jiġi limitat ir-riskju ta' kunflitti ta' interess, l-entitajiet finanzjarji jenħtieġ li jiżguraw is-segregazzjoni tad-dmirijiet meta jassenjaw ir-rwoli u r-responsabbiltajiet tal-ICT.

(5) Sabiex tiġi żgurata l-flessibbiltà u jiġi ssimplifikat il-qafas ta' kontroll tal-entitajiet finanzjarji, jenħtieġ li l-entitajiet finanzjarji ma jkunux mitluba jiżviluppaw dispożizzjonijiet speċifiċi dwar il-konsegwenzi tan-nuqqas ta' konformità mal-politiki, il-proċeduri u l-protokolli tas-sigurtà tal-ICT imsemmija fit-Titolu II, il-Kapitolu I ta' dan ir-Regolament meta tali dispożizzjonijiet ikunu diġà stabbiliti f'politika jew proċedura oħra.

([1]) ĠU L 333, 27.12.2022, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

(6) F'ambjent dinamiku fejn hemm ir-riskju li l-ICT tevolvi b'mod kostanti, huwa importanti li l-entitajiet finanzjarji jiżviluppaw is-sett tagħhom ta' politiki tas-sigurtà tal-ICT abbażi ta' prattiki ewlenin, u meta applikabbli, ta' standards kif iddefiniti fl-Artikolu 2, il-punt (1) tar-Regolament (UE) Nru 1025/2012 tal-Parlament Ewropew u tal-Kunsill ([2]). Dan jenħtieġ li jippermetti lill-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jibqgħu informati u mħejjija f'xenarju li qed jinbidel.

(7) Biex tiġi żgurata r-reżiljenza operazzjonali diġitali tagħhom, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li, bħala parti mill-politiki, mill-proċeduri, mill-protokolli u mill-għodod tas-sigurtà tal-ICT tagħhom, jiżviluppaw u jimplimentaw politika tal-ġestjoni tal-assi tal-ICT, proċeduri ta' ġestjoni tal-kapaċità u tal-prestazzjoni, u politiki u proċeduri għall-operazzjonijiet tal-ICT. Dawk il-politiki u l-proċeduri huma meħtieġa biex jiżguraw il-monitoraġġ tal-istatus tal-assi tal-ICT matul iċ-ċikli tal-ħajja tagħhom, sabiex dawk l-assi jintużaw u jinżammu b'mod effettiv (ġestjoni tal-assi tal-ICT). Dawk il-politiki u l-proċeduri jenħtieġ li jiżguraw ukoll l-ottimizzazzjoni tat-tħaddim tas-sistemi tal-ICT u li l-prestazzjoni tas-sistemi u tal-kapaċità tal-ICT tissodisfa l-objettivi stabbiliti tas-sigurtà tan-negozju u tal-informazzjoni (ġestjoni tal-kapaċità u tal-prestazzjoni). Fl-aħħar nett, dawk il-politiki u l-proċeduri jenħtieġ li jiżguraw il-ġestjoni u t-tħaddim effettivi u bla xkiel ta' kuljum tas-sistemi tal-ICT (operazzjonijiet tal-ICT), u b'hekk jimminimizzaw ir-riskju ta' telf ta' kunfidenzjalità, integrità u disponibbiltà tad-*data*. Għalhekk, dawk il-politiki u l-proċeduri huma meħtieġa biex tiġi żgurata s-sigurtà tan-networks, biex jiġu previsti salvagwardji adegwati kontra l-intrużjonijiet u l-użu ħażin tad-*data*, u biex jiġu ppreżervati d-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data*.

(8) Biex tiġi żgurata ġestjoni xierqa tar-riskju tas-sistemi tal-ICT miruta, jenħtieġ li l-entitajiet finanzjarji jirreġistraw u jimmonitorjaw id-dati finali tas-servizzi ta' appoġġ ta' partijiet terzi tal-ICT. Minħabba l-impatt potenzjali li jista' jkollu telf ta' kunfidenzjalità, integrità u disponibbiltà tad-*data*, l-entitajiet finanzjarji jenħtieġ li jiffokaw fuq dawk l-assi jew is-sistemi tal-ICT li huma kritiċi għall-operazzjoni tan-negozju meta jirreġistraw u jimmonitorjaw dawk id-dati finali.

(9) Il-kontrolli kriptografiċi jistgħu jiżguraw id-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data*. Għalhekk, jenħtieġ li l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jidentifikaw u jimplimentaw dawn il-kontrolli abbażi ta' approċċ ibbażat fuq ir-riskju. Għal dak il-għan, l-entitajiet finanzjarji jenħtieġ li jikkriptaw id-*data* kkonċernata waqt li tkun wieqfa, fi tranżitu jew, meta meħtieġ, waqt l-użu, abbażi tar-riżultati ta' proċess b'żewġ binarji, jiġifieri l-klassifikazzjoni tad-*data* u valutazzjoni komprensiva tar-riskju tal-ICT. Minħabba l-kumplessità tal-kriptaġġ tad-*data* waqt l-użu, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jikkriptaw id-*data* waqt l-użu biss meta dan ikun xieraq fid-dawl tar-riżultati tal-valutazzjoni tar-riskju tal-ICT. Madankollu, meta l-kriptaġġ tad-*data* waqt l-użu ma jkunx fattibbli jew ikun kumpless wisq, jenħtieġ li l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament ikunu jistgħu jipproteġu l-kunfidenzjalità, l-integrità u d-disponibbiltà tad-*data* kkonċernata permezz ta' miżuri oħrajn ta' sigurtà tal-ICT. Minħabba l-iżviluppi teknoloġiċi rapidi fil-qasam tat-tekniki kriptografiċi, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jibqgħu aġġornati dwar l-iżviluppi rilevanti fil-kriptanaliżi u jikkunsidraw prattiki u standards ewlenin. Għalhekk, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jsegwu approċċ flessibbli, ibbażat fuq il-mitigazzjoni u l-monitoraġġ tar-riskju, biex jittrattaw ix-xenarju dinamiku tat-theddid kriptografiku, inkluż it-theddid minn avvanzi kwantistiċi.

(10) Is-sigurtà tal-operazzjonijiet tal-ICT u l-politiki operazzjonali, il-proċeduri, il-protokolli u l-għodod huma essenzjali biex jiġu żgurati l-kunfidenzjalità, l-integrità, u d-disponibbiltà tad-*data*. Wieħed mill-aspetti ewlenin huwa s-separazzjoni stretta tal-ambjenti ta' produzzjoni tal-ICT mill-ambjenti fejn is-sistemi tal-ICT jiġu żviluppati u ttestjati jew minn ambjenti oħrajn mhux tal-produzzjoni. Din is-separazzjoni jenħtieġ li sservi bħala miżura importanti ta' sigurtà tal-ICT kontra aċċess mhux intenzjonat u mhux awtorizzat għal *data* fl-ambjent ta' produzzjoni, u l-modifiki u t-tħassir tagħha, li jistgħu jirriżultaw f'interruzzjonijiet kbar fl-operazzjonijiet kummerċjali tal-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament. Madankollu, meta jitqiesu l-prattiki kurrenti tal-iżvilupp tas-sistemi tal-ICT, f'ċirkostanzi eċċezzjonali, l-entitajiet finanzjarji jenħtieġ li jitħallew jittestjaw fl-ambjenti ta' produzzjoni, dment li jiġġustifikaw dan l-ittestjar u jiksbu l-approvazzjoni meħtieġa.

([2]) Ir-Regolament (UE) Nru 1025/2012 tal-Parlament Ewropew u tal-Kunsill tal-25 ta' Ottubru 2012 dwar l-Istandardizzazzjoni Ewropea, li jemenda d-Direttivi tal-Kunsill 89/686/KEE u 93/15/KEE u d-Direttivi 94/9/KE, 94/25/KE, 95/16/KE, 97/23/KE, 98/34/KE, 2004/22/KE, 2007/23/KE, 2009/23/KE u 2009/105/KE tal-Parlament Ewropew u tal-Kunsill u li jħassar id-Deċiżjoni tal-Kunsill 87/95/KEE u d-Deċiżjoni Nru 1673/2006/KE tal-Parlament Ewropew u tal-Kunsill (ĠU L 316, 14.11.2012, p. 12, ELI: https://eur-lex.europa.eu/eli/reg/2012/1025/oj).

(11) In-natura li qed tevolvi malajr tax-xenarji tal-ICT, tal-vulnerabbiltajiet tal-ICT u tat-theddid ċibernetiku teħtieġ approċċ proattiv u komprensiv għall-identifikazzjoni, għall-evalwazzjoni u għall-indirizzar tal-vulnerabbiltajiet tal-ICT. Minħajr approċċ bħal dan, l-entitajiet finanzjarji, il-klijenti, l-utenti jew il-kontropartijiet tagħhom jistgħu jkunu esposti b'mod sever għal riskji, li jpoġġu f'riskju r-reżiljenza operazzjonali diġitali tagħhom, is-sigurtà tan-networks tagħhom u d-disponibbiltà, l-awtenticità, l-integrità u l-kunfidenzjalità tad-*data* li l-politiki u l-proċeduri tas-sigurtà tal-ICT jenħtieġ li jipproteġu. Għalhekk, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jidentifikaw u jirrimedjaw il-vulnerabbiltajiet fl-ambjent tal-ICT tagħhom, u kemm l-entitajiet finanzjarji kif ukoll il-fornituri terzi ta' servizzi tal-ICT tagħhom jenħtieġ li jaderixxu ma' qafas tal-ġestjoni tal-vulnerabbiltà koerenti, trasparenti u responsabbli. Minħabba l-istess raġuni, l-entitajiet finanzjarji jenħtieġ li jimmonitorjaw il-vulnerabbiltajiet tal-ICT bl-użu ta' riżorsi affidabbli u għodod awtomatizzati, filwaqt li jivverifikaw li l-fornituri terzi ta' servizzi tal-ICT jiżguraw azzjoni immedjata dwar il-vulnerabbiltajiet fis-servizzi tal-ICT ipprovduti.

(12) Il-ġestjoni tal-patches jenħtieġ li tkun parti kruċjali minn dawk il-politiki u l-proċeduri tas-sigurtà tal-ICT li, permezz tal-ittestjar u l-varar f'ambjent ikkontrollat, għandha ssolvi l-vulnerabbiltajiet identifikati u tipprevjeni tfixkil mill-installazzjoni ta' patches.

(13) Biex tiġi żgurata komunikazzjoni f'waqtha u trasparenti ta' theddid potenzjali għas-sigurtà li jista' jkollu impatt fuq l-entità finanzjarja u l-partijiet ikkonċernati tagħha, jenħtieġ li l-entitajiet finanzjarji jistabbilixxu proċeduri għad-divulgazzjoni responsabbli tal-vulnerabbiltajiet tal-ICT lill-klijenti, lill-kontropartijiet u lill-pubbliku. Meta jistabbilixxu dawk il-proċeduri, l-entitajiet finanzjarji jenħtieġ li jqisu l-fatturi, inkluża s-severità tal-vulnerabbiltà, l-impatt potenzjali ta' din il-vulnerabbiltà fuq il-partijiet ikkonċernati u l-prontezza ta' tiswija jew ta' miżuri ta' mitigazzjoni.

(14) Biex jippermettu l-assenjazzjoni tad-drittijiet ta' aċċess għall-utenti, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jistabbilixxu miżuri b'saħħithom biex tiġi aċċertata l-identifikazzjoni unika ta' individwi u sistemi li se jaċċessaw l-informazzjoni tal-entità finanzjarja. In-nuqqas li jsir dan jesponi lill-entitajiet finanzjarji għal aċċess mhux awtorizzat potenzjali, ksur ta' *data* u attivitajiet frawdolenti, u b'hekk jiġu kompromessi l-kunfidenzjalità, l-integrità u d-disponibbiltà ta' *data* finanzjarja sensittiva. Filwaqt li l-użu ta' kontijiet ġeneriċi jew kondiviżi jenħtieġ li jkun permess b'mod eċċezzjonali f'ċirkostanzi speċifikati minn entitajiet finanzjarji, jenħtieġ li l-entitajiet finanzjarji jiżguraw li tinżamm l-akkontabilità għall-azzjonijiet meħuda permezz ta' dawk il-kontijiet. Minħajr dik is-salvagwardja, l-utenti potenzjali malizzjużi jkunu jistgħu jfixklu l-miżuri investigattivi u korrettivi, u jħallu lill-entitajiet finanzjarji vulnerabbli għal attivitajiet malizzjużi mhux individwati jew penali għal nuqqas ta' konformità.

(15) Biex jiġġestixxu l-avvanz rapidu fl-ambjenti tal-ICT, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jimplimentaw politiki u proċeduri robusti ta' ġestjoni tal-proġetti tal-ICT biex iżommu d-disponibbiltà, l-awtenticità, l-integrità u l-kunfidenzjalità tad-*data*. Dawk il-politiki u l-proċeduri tal-ġestjoni tal-proġetti tal-ICT jenħtieġ li jidentifikaw l-elementi li huma meħtieġa għall-ġestjoni b'suċċess tal-proġetti tal-ICT, inklużi t-tibdiliet fis-sistemi tal-ICT tal-entità finanzjarja, l-akkwiżizzjonijiet, iż-żamma u l-iżviluppi tagħhom, irrispettivament mill-metodoloġija tal-ġestjoni tal-proġetti tal-ICT magħżula mill-entità finanzjarja. Fil-kuntest ta' dawk il-politiki u l-proċeduri, l-entitajiet finanzjarji jenħtieġ li jadottaw prattiki u metodi ta' ttestjar li jissodisfaw il-ħtiġijiet tagħhom, filwaqt li jaderixxu ma' approċċ ibbażat fuq ir-riskju u jiżguraw li jinżamm ambjent tal-ICT sigur, affidabbli u reżiljenti. Biex tiġi ggarantita l-implimentazzjoni sigura ta' proġett tal-ICT, l-entitajiet finanzjarji jenħtieġ li jiżguraw li l-persunal minn setturi jew rwoli speċifiċi tan-negozju influwenzati jew affettwati minn dak il-proġett tal-ICT ikun jista' jipprovdi l-informazzjoni u l-għarfien espert meħtieġa. Biex tiġi żgurata sorveljanza effettiva, jenħtieġ li jiġu ppreżentati rapporti dwar il-proġetti tal-ICT, b'mod partikolari dwar proġetti li jaffettwaw funzjonijiet kritiċi jew importanti u dwar ir-riskji assoċjati tagħhom, lill-korp maniġerjali. L-entitajiet finanzjarji jenħtieġ li jfasslu l-frekwenza u d-dettalji tar-rieżamijiet u r-rapporti sistematiċi u kontinwi għall-importanza u d-daqs tal-proġetti tal-ICT ikkonċernati.

(16) Huwa meħtieġ li jiġi żgurat li l-pakketti ta' software li l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jiksbu u jiżviluppaw jiġu integrati b'mod effettiv u sigur fl-ambjent eżistenti tal-ICT, f'konformità mal-objettivi stabbiliti tas-sigurtà tan-negozju u tal-informazzjoni. Għalhekk, jenħtieġ li l-entitajiet finanzjarji jevalwaw bir-reqqa dawn il-pakketti ta' software. Għal dak il-għan, u biex jiġu identifikati l-vulnerabbiltajiet u d-diskrepanzi potenzjali fis-sigurtà kemm fil-pakketti tas-software kif ukoll fis-sistemi usa' tal-ICT, jenħtieġ li l-entitajiet finanzjarji jwettqu ttestjar tas-sigurtà tal-ICT. Biex tiġi vvalutata l-integrità tas-software u biex jiġi żgurat li l-użu ta' dak is-software ma joħloqx riskji għas-sigurtà tal-ICT, jenħtieġ li l-entitajiet finanzjarji jirrieżaminaw ukoll il-kodiċijiet tas-sors ta' software miksub, inkluż, meta fattibbli, ta' software proprjetarju pprovdut minn fornituri terzi ta' servizzi tal-ICT, bl-użu ta' metodi ta' ttestjar kemm statiċi kif ukoll dinamiċi.

(17) It-tibdiliet, irrispettivament mill-iskala tagħhom, iġibu magħhom riskji inerenti u jistgħu joħolqu riskji sinifikanti ta' telf ta' kunfidenzjalità, integrità u disponibbiltà tad-*data*, u għalhekk jistgħu jwasslu għal tfixkil serju fin-negozju. Biex l-entitajiet finanzjarji jiġu ssalvagwardjati minn vulnerabbiltajiet u dgħufijiet potenzjali tal-ICT li jistgħu jesponuhom għal riskji sinifikanti, huwa meħtieġ proċess ta' verifika rigoruż biex jiġi kkonfermat li t-tibdiliet kollha jissodisfaw ir-rekwiżiti meħtieġa tas-sigurtà tal-ICT. Għalhekk, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li, bħala element essenzjali tal-politiki u l-proċeduri tas-sigurtà tal-ICT tagħhom, ikollhom stabbiliti politiki u proċeduri sodi ta' ġestjoni tat-tibdil fl-ICT. Biex jiġu rrispettati l-oġġettività u l-effettività tal-proċess tal-ġestjoni tat-tibdil fl-ICT, biex jiġu pprevenuti l-kunflitti ta' interess u biex jiġi żgurat li t-tibdiliet fl-ICT jiġu evalwati b'mod oġġettiv, huwa meħtieġ li l-funzjonijiet responsabbli għall-approvazzjoni ta' dawk it-tibdiliet jiġu sseparati mill-funzjonijiet li jitolbu u jimplimentaw dawk it-tibdiliet. Biex jinkisbu tranżizzjonijiet effettivi, l-implimentazzjoni kkontrollata tat-tibdil fl-ICT u t-tfixkil minimu fit-tħaddim tas-sistemi tal-ICT, l-entitajiet finanzjarji jenħtieġ li jassenjaw rwoli u responsabbiltajiet ċari li jiżguraw li t-tibdiliet fl-ICT jiġu ppjanati, ittestjati b'mod adegwat u li tiġi żgurata l-kwalità. Biex jiġi żgurat li s-sistemi tal-ICT ikomplu jaħdmu b'mod effettiv, u biex jipprovdu xibka ta' sikurezza għall-entitajiet finanzjarji, jenħtieġ li l-entitajiet finanzjarji jiżviluppaw u jimplimentaw ukoll proċeduri ta' riżerva. L-entitajiet finanzjarji jenħtieġ li jidentifikaw b'mod ċar dawk il-proċeduri ta' riżerva u jassenjaw responsabbiltajiet biex jiżguraw rispons rapidu u effettiv fil-każ ta' tibdiliet fl-ICT li ma jirnexxux.

(18) Biex jindividwaw, jimmaniġġaw u jirrapportaw inċidenti relatati mal-ICT, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jistabbilixxu politika dwar inċidenti relatati mal-ICT li tinkludi l-komponenti ta' proċess ta' ġestjoni tal-inċidenti relatati mal-ICT. Għal dak il-għan, jenħtieġ li l-entitajiet finanzjarji jidentifikaw il-kuntatti rilevanti kollha ġewwa u barra l-organizzazzjoni li jistgħu jiffaċilitaw il-koordinazzjoni u l-implimentazzjoni korretti tal-fażijiet differenti f'dak il-proċess. Sabiex jiġu ottimizzati d-detezzjoni ta' inċidenti relatati mal-ICT u r-rispons għalihom, u biex jiġu identifikati x-xejriet fost dawk l-inċidenti, li huma sors siewi ta' informazzjoni li tippermetti lill-entitajiet finanzjarji jidentifikaw u jindirizzaw il-kawżi u l-problemi ewlenin b'mod effettiv, jenħtieġ li l-entitajiet finanzjarji janalizzaw b'mod partikolari fid-dettall l-inċidenti relatati mal-ICT li huma jqisu bħala l-aktar sinifikanti, fost l-oħrajn minħabba l-okkorrenza mill-ġdid regolari tagħhom.

(19) Sabiex tiġi ggarantita detezzjoni bikrija u effettiva ta' attivitajiet anomali, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jiġbru, jimmonitorjaw u janalizzaw is-sorsi differenti ta' informazzjoni u jenħtieġ li jallokaw rwoli u responsabbiltajiet relatati. Fir-rigward tas-sorsi interni ta' informazzjoni, ir-reġistri huma sors estremament rilevanti, iżda l-entitajiet finanzjarji jenħtieġ li ma jibbażawx biss fuq ir-reġistri. Minflok, jenħtieġ li l-entitajiet finanzjarji jqisu informazzjoni usa' biex jinkludu dak li jiġi rrapportat minn funzjonijiet interni oħrajn, peress li dawk il-funzjonijiet spiss ikunu sors siewi ta' informazzjoni rilevanti. Minħabba l-istess raġuni, l-entitajiet finanzjarji jenħtieġ li janalizzaw u jimmonitorjaw l-informazzjoni miġbura minn sorsi esterni, inkluża l-informazzjoni pprovduta mill-fornituri terzi tal-ICT dwar inċidenti li jaffettwaw is-sistemi u n-networks tagħhom, u sorsi oħrajn ta' informazzjoni li l-entitajiet finanzjarji jqisu rilevanti. Sa fejn din l-informazzjoni tikkostitwixxi *data* personali, tapplika l-liġi tal-Unjoni dwar il-protezzjoni tad-*data*. Id-*data* personali jenħtieġ li tkun limitata għal dak li huwa meħtieġ għall-individwazzjoni tal-inċident.

(20) Biex tiġi ffaċilitata l-individwazzjoni ta' inċidenti relatati mal-ICT, jenħtieġ li l-entitajiet finanzjarji jżommu evidenza ta' dawk l-inċidenti. Biex jiġi żgurat, minn naħa waħda, li din l-evidenza tinżamm għal biżżejjed żmien u biex jiġi evitat, min-naħa l-oħra, piż regolatorju eċċessiv, jenħtieġ li l-entitajiet finanzjarji jiddeterminaw il-perjodu ta' żamma filwaqt li jqisu, fost affarijiet oħrajn, il-kritikalità tar-rekwiżiti tad-*data* u taż-żamma li jirriżultaw mid-dritt tal-Unjoni.

(21) Biex jiġi żgurat li l-inċidenti relatati mal-ICT jiġu individwati fil-ħin, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jqisu l-kriterji identifikati għall-iskattar tal-individwazzjoni ta' inċidenti relatati mal-ICT u r-risponsi għalihom bħala mhux eżawrjenti. Barra minn hekk, filwaqt li l-entitajiet finanzjarji jenħtieġ li jqisu kull wieħed minn dawk il-kriterji, jenħtieġ li ċ-ċirkostanzi deskritti fil-kriterji ma jkollhomx għalfejn iseħħu simultanjament u jenħtieġ li l-importanza tas-servizzi tal-ICT affettwati titqies kif xieraq biex jiġu skattati l-proċessi ta' individwazzjoni u ta' rispons tal-inċidenti relatati mal-ICT.

(22) Meta jiżviluppaw politika ta' kontinwità tal-operat tal-ICT, l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jqisu l-komponenti essenzjali tal-ġestjoni tar-riskju tal-ICT, inklużi l-istrateġiji tal-ġestjoni tal-inċidenti u ta' komunikazzjoni relatati mal-ICT, il-proċess ta' ġestjoni tat-tibdil fl-ICT u r-riskji assoċjati ma' fornituri terzi ta' servizzi tal-ICT.

(23) Huwa meħtieġ li jiġi stabbilit is-sett ta' xenarji li l-entitajiet finanzjarji msemmija fit-Titolu II ta' dan ir-Regolament jenħtieġ li jqisu kemm għall-implimentazzjoni tal-pjanijiet ta' rispons u rkupru tal-ICT kif ukoll għall-ittestjar tal-pjanijiet ta' kontinwità tal-operat tal-ICT. Dawk ix-xenarji jenħtieġ li jservu bħala punt ta' tluq għall-entitajiet finanzjarji biex janalizzaw kemm ir-rilevanza kif ukoll il-plawżibbiltà ta' kull xenarju u l-ħtieġa li jiġu żviluppati xenarji alternattivi. L-entitajiet finanzjarji jenħtieġ li jiffokaw fuq dawk ix-xenarji li fihom l-investiment f'miżuri ta' reżiljenza jista' jkun aktar effiċjenti u effettiv. Bl-ittestjar ta' kommutazzjonijiet bejn l-infrastruttura primarja tal-ICT u kwalunkwe kapaċità żejda, backup u faċilità żejda, l-istituzzjonijiet finanzjarji jenħtieġ li jivvalutaw jekk dik il-kapaċità, backup u dawk il-faċilitajiet joperawx b'mod effettiv għal perjodu ta' żmien suffiċjenti u jiżguraw li l-funzjonament normali tal-infrastruttura primarja tal-ICT jiġi rrestawrat f'konformità mal-objettivi ta' rkupru.

(24) Huwa meħtieġ li jiġu stabbiliti rekwiżiti għar-riskju operazzjonali, u b'mod partikolari rekwiżiti għall-ġestjoni tal-proġetti tal-ICT u tat-tibdil u għall-ġestjoni tal-kontinwità tal-operat tal-ICT li jibnu fuq dawk li diġà japplikaw għal kontropartijiet ċentrali, depożitorji ċentrali tat-titoli u ċentri tan-negozjar skont, rispettivament, ir-Regolamenti (UE) Nru 648/2012 ([3]), (UE) Nru 600/2014 ([4]) u (UE) Nru 909/2014 ([5]) tal-Parlament Ewropew u tal-Kunsill.

(25) L-Artikolu 6(5) tar-Regolament (UE) 2022/2554 jirrikjedi li l-entitajiet finanzjarji jirrieżaminaw il-qafas tal-ġestjoni tar-riskju tal-ICT tagħhom u jipprovdu lill-awtorità kompetenti tagħhom b'rapport dwar dak ir-rieżami. Biex l-awtoritajiet kompetenti jkunu jistgħu jipproċessaw faċilment l-informazzjoni f'dawk ir-rapporti, u biex jiggarantixxu trażmissjoni adegwata ta' dik l-informazzjoni, jenħtieġ li l-entitajiet finanzjarji jippreżentaw dawk ir-rapporti f'format elettroniku li jippermetti t-tiftix.

(26) Ir-rekwiżiti għall-entitajiet finanzjarji li huma soġġetti għall-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT imsemmija fl-Artikolu 16 tar-Regolament (UE) 2022/2554 jenħtieġ li jkunu ffukati fuq dawk l-oqsma u l-elementi essenzjali li, fid-dawl tal-iskala, tar-riskju, tad-daqs u tal-kumplessità ta' dawk l-entitajiet finanzjarji, huma bħala minimu meħtieġa biex jiġu żgurati l-kunfidenzjalità, l-integrità, id-disponibbiltà u l-awtenticità tad-*data* u tas-servizzi ta' dawk l-entitajiet finanzjarji. F'dak il-kuntest, jenħtieġ li dawk l-entitajiet finanzjarji jkollhom stabbilit qafas ta' governanza u kontroll intern b'responsabbiltajiet ċari biex jippermettu qafas tal-ġestjoni tar-riskju effettiv u sod. Barra minn hekk, biex jitnaqqas il-piż amministrattiv u operazzjonali, jenħtieġ li dawk l-entitajiet finanzjarji jiżviluppaw u jiddokumentaw politika waħda biss, li hija politika ta' sigurtà tal-informazzjoni, li tispeċifika l-prinċipji u r-regoli ta' livell għoli meħtieġa biex jiġu protetti l-kunfidenzjalità, l-integrità, id-disponibbiltà u l-awtenticità tad-*data* u tas-servizzi ta' dawk l-entitajiet finanzjarji.

(27) Id-dispożizzjonijiet ta' dan ir-Regolament huma relatati mal-qasam tal-qafas tal-ġestjoni tar-riskju tal-ICT, billi jagħtu dettalji dwar l-elementi speċifiċi applikabbli għall-entitajiet finanzjarji f'konformità mal-Artikolu 15 tar-Regolament (UE) 2022/2554 u billi jfasslu l-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT għall-entitajiet finanzjarji stabbilit fl-Artikolu 16(1) ta' dak ir-Regolament. Biex tiġi żgurata l-koerenza bejn il-qafas ordinarju u dak issimplifikat tal-ġestjoni tar-riskju tal-ICT, u meta jitqies li dawk id-dispożizzjonijiet jenħtieġ li jsiru applikabbli fl-istess ħin, huwa xieraq li dawk id-dispożizzjonijiet jiġu inklużi f'att leġiżlattiv wieħed.

(28) Dan ir-Regolament huwa bbażat fuq l-abbozz tal-istandards tekniċi regolatorji ppreżentati lill-Kummissjoni mill-Awtorità Bankarja Ewropea, l-Awtorità Ewropea tal-Assigurazzjoni u l-Pensjonijiet tax-Xogħol u l-Awtorità Ewropea tat-Titoli u s-Swieq (l-Awtoritajiet Superviżorji Ewropej), f'konsultazzjoni mal-Aġenzija tal-Unjoni Ewropea għaċ-Ċibersigurtà (ENISA).

([3]) Ir-Regolament (UE) Nru 648/2012 tal-Parlament Ewropew u tal-Kunsill tal-4 ta' Lulju 2012 dwar derivati OTC, kontropartijiet ċentrali u repożitorji tad-*data* dwar it-tranżazzjonijiet (ĠU L 201, 27.7.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Ir-Regolament (UE) Nru 600/2014 tal-Parlament Ewropew u tal-Kunsill tal-15 ta' Mejju 2014 dwar is-swieq tal-istrumenti finanzjarji u li jemenda r-Regolament (UE) Nru 648/2012 (ĠU L 173, 12.6.2014, p. 84 ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Ir-Regolament (UE) Nru 909/2014 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Lulju 2014 dwar titjib fis-saldu tat-titoli fl-Unjoni Ewropea u dwar depożitorji ċentrali tat-titoli u li jemenda d-Direttivi 98/26/KE u 2014/65/UE u r-Regolament (UE) Nru 236/2012 (ĠU L 257, 28.8.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Il-Kumitat Konġunt tal-Awtoritajiet Superviżorji Ewropej imsemmi fl-Artikolu 54 tar-Regolament (UE) Nru 1093/2010 tal-Parlament Ewropew u tal-Kunsill ([6]), fl-Artikolu 54 tar-Regolament (UE) Nru 1094/2010 tal-Parlament Ewropew u tal-Kunsill ([7]) u fl-Artikolu 54 tar-Regolament (UE) Nru 1095/2010 tal-Parlament Ewropew u tal-Kunsill ([8]) wettaq konsultazzjonijiet pubbliċi miftuħa dwar l-abbozz ta' standards tekniċi regolatorji li fuqhom huwa bbażat dan ir-Regolament, analizza l-kostijiet u l-benefiċċji potenzjali tal-istandards proposti u talab il-parir tal-Grupp tal-Partijiet Bankarji Interessati stabbilit f'konformità mal-Artikolu 37 tar-Regolament (UE) Nru 1093/2010, tal-Grupp tal-Partijiet Interessati tal-Oqsma tal-Assigurazzjoni u tar-Riassigurazzjoni u l-Grupp tal-Partijiet Interessati tal-Qasam tal-Pensjonijiet tax-Xogħol stabbiliti f'konformità mal-Artikolu 37 tar-Regolament (UE) Nru 1094/2010, u tal-Grupp tal-Partijiet Interessati tat-Titoli u s-Swieq stabbilit f'konformità mal-Artikolu 37 tar-Regolament (UE) Nru 1095/2010.

(30) Sa fejn l-ipproċessar ta' *data* personali huwa meħtieġ li jikkonforma mal-obbligi stabbiliti f'dan l-Att, jenħtieġ li r-Regolamenti (UE) 2016/679 ([9]) u (UE) 2018/1725 ([10]) tal-Parlament Ewropew u tal-Kunsill japplikaw bis-sħiħ. Pereżempju, il-prinċipju tal-minimizzazzjoni tad-*data* jenħtieġ li jiġi rrispettat meta tinġabar *data* personali biex tiġi żgurata individwazzjoni xierqa tal-inċidenti. Il-Kontrollur Ewropew għall-Protezzjoni tad-*Data* ġie kkonsultat ukoll dwar l-abbozz tat-test ta' dan l-Att,

ADOTTAT DAN IR-REGOLAMENT:

TITOLU I

PRINĊIPJU ĠENERALI

Artikolu 1

Profil tar-riskju ġenerali u kumplessità

Meta jiġu żviluppati u implimentati l-politiki, il-proċeduri, il-protokolli u l-għodod tas-sigurtà tal-ICT imsemmija fit-Titolu II u l-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT imsemmi fit-Titolu III, għandhom jitqiesu d-daqs u l-profil tar-riskju ġenerali tal-entità finanzjarja, u n-natura, l-iskala u l-elementi ta' kumplessità akbar jew imnaqqsa tas-servizzi, tal-attivitajiet u tal-operazzjonijiet tagħha, inklużi l-elementi relatati ma':

(a) kriptaġġ u kriptografija;

(b) sigurtà tal-operazzjonijiet tal-ICT;

(c) sigurtà tan-network;

([6]) 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, ELI: https://eur-lex.europa.eu/eli/reg/2010/1093/oj).

([7]) Ir-Regolament (UE) Nru 1094/2010 tal-Parlament Ewropew u tal-Kunsill tal-24 ta' Novembru 2010 li jistabbilixxi Awtorità Superviżorja Ewropea (Awtorità Ewropea tal-Assigurazzjoni u l-Pensjonijiet tax-Xogħol), u li jemenda d-Deċiżjoni Nru 716/2009/KE u li jħassar id-Deċiżjoni tal-Kummissjoni 2009/79/KE (ĠU L 331, 15.12.2010, p. 48, ELI: https://eur-lex.europa.eu/eli/reg/2010/1094/oj).

([8]) Ir-Regolament (UE) Nru 1095/2010 tal-Parlament Ewropew u tal-Kunsill tal-24 ta' Novembru 2010 li jistabbilixxi Awtorità Superviżorja Ewropea (Awtorità Ewropea tat-Titoli u s-Swieq) u li jemenda d-Deċiżjoni Nru 716/2009/KE u jħassar id-Deċiżjoni tal-Kummissjoni 2009/77/KE (ĠU L 331, 15.12.2010, p. 84, ELI: https://eur-lex.europa.eu/eli/reg/2010/1095/oj).

([9]) Ir-Regolament (UE) 2016/679 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Ir-Regolament (UE) 2018/1725 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Ottubru 2018 dwar il-protezzjoni ta' persuni fiżiċi fir-rigward tal-ipproċessar ta' *data* personali mill-istituzzjonijiet, korpi, uffiċċji u aġenziji tal-Unjoni u dwar il-moviment liberu ta' tali *data*, u li jħassar ir-Regolament (KE) Nru 45/2001 u d-Deċiżjoni Nru 1247/2002/KE (ĠU L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(d) ġestjoni tal-proġetti tal-ICT u tat-tibdil tagħhom;

(e) l-impatt potenzjali tar-riskju tal-ICT fuq il-kunfidenzjalità, l-integrità u d-disponibbiltà tad-*data*, u tat-tfixkil fuq il-kontinwità u d-disponibbiltà tal-attivitajiet tal-entità finanzjarja.

TITOLU II

AKTAR ARMONIZZAZZJONI TAL-GĦODOD, TAL-METODI, TAL-PROĊESSI U TAL-POLITIKI TAL-ĠESTJONI TAR-RISKJU TAL-ICT F'KONFORMITÀ MAL-ARTIKOLU 15 TAR-REGOLAMENT (UE) 2022/2554

KAPITOLU I

Politiki, proċeduri, protokolli, u għodod ta' sigurtà tal-ICT

Taqsima 1

Artikolu 2

Elementi ġenerali tal-politiki, proċeduri, protokolli u għodda ta' sigurtà tal-ICT

1. L-entitajiet finanzjarji għandhom jiżguraw li l-politiki tas-sigurtà tal-ICT, is-sigurtà tal-informazzjoni u l-proċeduri, il-protokolli u l-għodod relatati tagħhom kif imsemmija fl-Artikolu 9(2) tar-Regolament (UE) 2022/2554 ikunu inkorporati fil-qafas tal-ġestjoni tar-riskju tal-ICT tagħhom. L-entitajiet finanzjarji għandhom jistabbilixxu l-politiki, il-proċeduri, il-protokolli u l-għodod tas-sigurtà tal-ICT stabbiliti f'dan il-Kapitolu li:

(a) jiżguraw is-sigurtà tan-networks;

(b) fihom salvagwardji kontra l-intrużjonijiet u l-użu ħażin tad-*data*;

(c) jippreżervaw id-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data*, inkluż permezz tal-użu ta' tekniki kriptografiċi;

(d) jiggarantixxu trażmissjoni tad-*data* akkurata u fil-pront mingħajr interruzzjonijiet kbar u dewmien bla bżonn.

2. L-entitajiet finanzjarji għandhom jiżguraw li l-politiki ta' sigurtà tal-ICT imsemmija fil-paragrafu 1:

(a) huma allinjati mal-objettivi tas-sigurtà tal-informazzjoni tal-entità finanzjarja inklużi fl-istrateġija tar-reżiljenza operazzjonali diġitali msemmija fl-Artikolu 6(8) tar-Regolament (UE) 2022/2554;

(b) jindikaw id-data tal-approvazzjoni formali tal-politiki tas-sigurtà tal-ICT mill-korp maniġerjali;

(c) jinkludu indikaturi u miżuri biex:

(i) jimmonitorjaw l-implimentazzjoni tal-politiki, tal-proċeduri, tal-protokolli u tal-għodod tas-sigurtà tal-ICT;

(ii) jirreġistraw eċċezzjonijiet minn dik l-implimentazzjoni

(iii) jiżguraw li tiġi żgurata r-reżiljenza operazzjonali diġitali tal-entità finanzjarja f'każ ta' eċċezzjonijiet kif imsemmi fil-punt (ii);

(d) jispeċifikaw ir-responsabbiltajiet tal-persunal fil-livelli kollha biex tiġi żgurata s-sigurtà tal-ICT tal-entità finanzjarja;

(e) jispeċifikaw il-konsegwenzi tan-nuqqas ta' konformità mill-persunal tal-entità finanzjarja mal-politiki tas-sigurtà tal-ICT, fejn id-dispożizzjonijiet għal dak l-għan ma jkunux stabbiliti f'politiki oħrajn tal-entità finanzjarja;

(f) jelenkaw id-dokumentazzjoni li għandha tinżamm;

(g) jispeċifikaw is-segregazzjoni tal-arranġamenti tad-dmirijiet fil-kuntest tat-tliet linji tal-mudell ta' difiża jew ta' mudell intern ieħor ta' ġestjoni u kontroll tar-riskju, kif applikabbli, biex jiġu evitati kunflitti ta' interess;

(h) jikkunsidraw prattiki ewlenin u, meta applikabbli, standards kif iddefiniti fl-Artikolu 2, il-punt (1) tar-Regolament (UE) Nru 1025/2012;

(i) jidentifikaw ir-rwoli u r-responsabbiltajiet għall-iżvilupp, għall-implimentazzjoni u għaż-żamma tal-politiki, tal-proċeduri, tal-protokolli u tal-għodod tas-sigurtà tal-ICT;

(j) huma rrieżaminati f'konformità mal-Artikolu 6(5) tar-Regolament (UE) 2022/2554;

(k) iqisu t-tibdiliet materjali li jikkonċernaw l-entità finanzjarja, inklużi t-tibdiliet materjali fl-attivitajiet jew fil-proċessi tal-entità finanzjarja, fix-xenarju tat-theddid ċibernetiku, jew fl-obbligi legali applikabbli.

Taqsima 2

Artikolu 3

Ġestjoni tar-riskju tal-ICT

L-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politiki u proċeduri tal-ġestjoni tar-riskju tal-ICT li għandu jkun fihom dawn kollha li ġejjin:

(a) indikazzjoni tal-approvazzjoni tal-livell ta' tolleranza tar-riskju għar-riskju tal-ICT stabbilit f'konformità mal-Artikolu 6(8), il-punt (b) tar-Regolament (UE) 2022/2554;

(b) proċedura u metodoloġija għat-twettiq tal-valutazzjoni tar-riskju tal-ICT, li tidentifika:

(i) il-vulnerabbiltajiet u t-theddid li jaffettwaw jew li jistgħu jaffettwaw il-funzjonijiet tan-negozju appoġġati, is-sistemi tal-ICT u l-assi tal-ICT li jappoġġaw dawk il-funzjonijiet;

(ii) l-indikaturi kwantitattivi jew kwalitattivi biex jitkejlu l-impatt u l-probabbiltà tal-vulnerabbiltajiet u t-theddid imsemmija fil-punt (i);

(c) il-proċedura biex jiġu identifikati, implimentati u ddokumentati miżuri għat-trattament tar-riskju tal-ICT għar-riskji tal-ICT identifikati u vvalutati, inkluża d-determinazzjoni tal-miżuri għat-trattament tar-riskju tal-ICT meħtieġa biex ir-riskju tal-ICT jinġieb fil-livell tat-tolleranza tar-riskju msemmi fil-punt (a);

(d) għar-riskji residwali tal-ICT li jkunu għadhom preżenti wara l-implimentazzjoni tal-miżuri tat-trattament tar-riskju tal-ICT imsemmija fil-punt (c):

(i) dispożizzjonijiet dwar l-identifikazzjoni ta' dawk ir-riskji residwali tal-ICT;

(ii) l-assenjazzjoni tar-rwoli u tar-responsabbiltajiet fir-rigward ta':

(1) l-aċċettazzjoni tar-riskji residwali tal-ICT li jaqbżu l-livell ta' tolleranza tar-riskju tal-entità finanzjarja msemmi fil-punt (a);

(2) għall-proċess ta' rieżami msemmi fil-punt (iv) ta' dan il-punt (d);

(iii) l-iżvilupp ta' inventarju tar-riskji residwali tal-ICT aċċettati, inkluża ġustifikazzjoni għall-aċċettazzjoni tagħhom;

(iv) dispożizzjonijiet dwar ir-rieżami tar-riskji residwali tal-ICT aċċettati mill-anqas darba fis-sena, inklużi:

(1) l-identifikazzjoni ta' kwalunkwe tibdil fir-riskji residwali tal-ICT;

(2) il-valutazzjoni tal-miżuri ta' mitigazzjoni disponibbli;

(3) il-valutazzjoni ta' jekk ir-raġunijiet li jiġġustifikaw l-aċċettazzjoni tar-riskji residwali tal-ICT jkunux għadhom validi u applikabbli fid-data tar-rieżami;

(e) dispożizzjonijiet dwar il-monitoraġġ ta':

(i) kwalunkwe tibdil fix-xenarju tar-riskju tal-ICT u tat-theddid ċibernetiku;

(ii) vulnerabbiltajiet u theddid interni u esterni:

(iii) ir-riskju tal-ICT tal-entità finanzjarja li jippermetti l-individwazzjoni fil-pront ta' tibdiliet li jistgħu jaffettwaw il-profil tar-riskju tal-ICT tagħha;

(f) dispożizzjonijiet dwar proċess biex jiġi żgurat li jitqies kwalunkwe tibdil fl-istrateġija tan-negozju u fl-istrateġija tar-reżiljenza operazzjonali diġitali tal-entità finanzjarja.

Għall-finijiet tal-ewwel paragrafu, il-punt (c), il-proċedura msemmija f'dak il-punt għandha tiżgura:

(a) il-monitoraġġ tal-effettività tal-miżuri għat-trattament tar-riskju tal-ICT implimentati;

(b) il-valutazzjoni ta' jekk intlaħqux il-livelli ta' tolleranza tar-riskju stabbiliti tal-entità finanzjarja;

(c) il-valutazzjoni ta' jekk l-entità finanzjarja tkunx ħadet azzjonijiet biex tikkoreġi jew ittejjeb dawk il-miżuri meta meħtieġ.

Taqsima 3

Ġestjoni tal-assi tal-ICT

Artikolu 4

Politika tal-ġestjoni tal-assi tal-ICT

1. Bħala parti mill-politiki, mill-proċeduri, mill-protokolli u mill-għodod ta' sigurtà tal-ICT msemmija fl-Artikolu 9(2) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politika dwar il-ġestjoni tal-assi tal-ICT.

2. Il-politika dwar il-ġestjoni tal-assi tal-ICT msemmija fil-paragrafu 1 għandha:

(a) tippreskrivi l-monitoraġġ u l-ġestjoni taċ-ċiklu tal-ħajja tal-assi tal-ICT identifikati u kklassifikati f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554;

(b) tippreskrivi li l-entità finanzjarja żżomm rekords ta' dawn kollha li ġejjin:

(i) l-identifikatur uniku ta' kull assi tal-ICT;

(ii) informazzjoni dwar il-post, fiżiku jew loġiku, tal-assi kollha tal-ICT;

(iii) il-klassifikazzjoni tal-assi kollha tal-ICT, kif imsemmi fl-Artikolu 8(1) tar-Regolament (UE) 2022/2254;

(iv) l-identità tas-sidien tal-assi tal-ICT;

(v) il-funzjonijiet jew is-servizzi tan-negozju appoġġati mill-assi tal-ICT;

(vi) ir-rekwiżiti tal-kontinwità tal-operat tal-ICT, inklużi l-objettivi tal-ħin ta' rkupru u l-objettivi tal-punt ta' rkupru;

(vii) jekk l-assi tal-ICT jistax ikun jew huwiex espost għal networks esterni, inkluż l-Internet;

(viii) ir-rabtiet u l-interdipendenzi fost l-assi tal-ICT u l-funzjonijiet tan-negozju bl-użu ta' kull assi tal-ICT;

(ix) meta applikabbli, għall-assi kollha tal-ICT, id-dati tat-tmiem tas-servizzi ta' appoġġ regolari, estiż u personalizzat tal-fornitur terz ta' servizzi tal-ICT li warajhom dawk l-assi tal-ICT ma jibqgħux appoġġati mill-fornitur tagħhom jew minn fornitur terz ta' servizzi tal-ICT;

(c) għall-entitajiet finanzjarji għajr il-mikrointrapriżi, tippreskrivi li dawk l-entitajiet finanzjarji jżommu rekords tal-informazzjoni meħtieġa biex titwettaq valutazzjoni speċifika tar-riskju tal-ICT fis-sistemi tal-ICT miruta kollha msemmija fl-Artikolu 8(7) tar-Regolament (UE) 2022/2554.

Artikolu 5

Proċedura tal-ġestjoni tal-assi tal-ICT

1. L-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċedura għall-ġestjoni tal-assi tal-ICT.

2. Il-proċedura għall-ġestjoni tal-assi tal-ICT imsemmija fil-paragrafu 1 għandha tispeċifika l-kriterji għat-twettiq tal-valutazzjoni tal-kritikalità tal-assi tal-informazzjoni u tal-assi tal-ICT li jappoġġaw il-funzjonijiet tan-negozju. Dik il-valutazzjoni għandha tqis:

(a) ir-riskju tal-ICT relatat ma' dawk il-funzjonijiet tan-negozju u d-dipendenzi tagħhom fuq l-assi tal-informazzjoni jew l-assi tal-ICT;

(b) kif it-telf ta' kunfidenzjalità, integrità u disponibbiltà ta' dawn l-assi ta' informazzjoni u l-assi tal-ICT jaffettwa l-proċessi u l-attivitajiet tan-negozju tal-entitajiet finanzjarji.

Taqsima 4

Kriptaġġ u kriptografija

Artikolu 6

Kriptaġġ u kontrolli kriptografiċi

1. Bħala parti mill-politiki, mill-proċeduri, mill-protokolli u mill-għodod tas-sigurtà tal-ICT tagħhom imsemmija fl-Artikolu 9(2) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politika dwar il-kriptaġġ u l-kontrolli kriptografiċi.

2. L-entitajiet finanzjarji għandhom ifasslu l-politika dwar il-kriptaġġ u l-kontrolli kriptografiċi msemmija fil-paragrafu 1 abbażi tar-riżultati ta' klassifikazzjoni tad-*data* approvata u valutazzjoni tar-riskju tal-ICT. Dik il-politika għandu jkun fiha regoli għal dan kollu li ġej:

(a) il-kriptaġġ tad-*data* waqt li tkun wieqfa u fi tranżitu;

(b) il-kriptaġġ tad-*data* waqt l-użu, meta meħtieġ;

(c) il-kriptaġġ ta' konnessjonijiet u traffiku interni tan-network ma' partijiet esterni;

(d) il-ġestjoni tal-kjavi kriptografika msemmija fl-Artikolu 7, li tistabbilixxi regoli dwar l-użu korrett, il-protezzjoni u ċ-ċiklu tal-ħajja ta' kjavi kriptografiċi.

Għall-finijiet tal-punt (b), meta l-kriptaġġ tad-*data* waqt l-użu ma jkunx possibbli, l-entitajiet finanzjarji għandhom jipproċessaw id-*data* waqt l-użu f'ambjent isseparat u protett, jew jieħdu miżuri ekwivalenti biex jiżguraw il-kunfidenzjalità, l-integrità, l-awtentiċità u d-disponibbiltà tad-*data*.

3. L-entitajiet finanzjarji għandhom jinkludu fil-politika dwar il-kriptaġġ u l-kontrolli kriptografiċi msemmija fil-paragrafu 1 kriterji għall-għażla ta' tekniki u prattiki tal-użu kriptografiċi, filwaqt li jqisu l-prattiki ewlenin, u l-istandards kif iddefiniti fl-Artikolu 2, il-punt (1) tar-Regolament (UE) Nru 1025/2012 u l-klassifikazzjoni tal-assi rilevanti tal-ICT stabbiliti f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554. L-entitajiet finanzjarji li ma jkunux jistgħu iżommu mal-prattiki jew l-istandards ewlenin, jew li ma jkunux jistgħu jużaw l-aktar tekniki affidabbli, għandhom jadottaw miżuri ta' mitigazzjoni u ta' monitoraġġ li jiżguraw ir-reżiljenza kontra t-theddid ċibernetiku.

4. L-entitajiet finanzjarji għandhom jinkludu fil-politika dwar il-kriptaġġ u l-kontrolli kriptografiċi msemmija fil-paragrafu 1 id-dispożizzjonijiet għall-aġġornament jew għat-tibdil, fejn meħtieġ, tat-teknoloġija kriptografika abbażi tal-iżviluppi fil-kriptanaliżi. Dawk l-aġġornamenti jew il-bidliet għandhom jiżguraw li t-teknoloġija kriptografika tibqa' reżiljenti kontra t-theddid ċibernetiku, kif meħtieġ mill-Artikolu 10(2), il-punt (a). L-entitajiet finanzjarji li ma jkunux jistgħu jaġġornaw jew ibiddlu t-teknoloġija kriptografika għandhom jadottaw miżuri ta' mitigazzjoni u ta' monitoraġġ li jiżguraw ir-reżiljenza kontra t-theddid ċibernetiku.

5. L-entitajiet finanzjarji għandhom jinkludu fil-politika dwar il-kriptaġġ u l-kontrolli kriptografiċi msemmija fil-paragrafu 1 rekwiżit biex jirreġistraw l-adozzjoni ta' miżuri ta' mitigazzjoni u ta' monitoraġġ adottati f'konformità mal-paragrafi 3 u 4 u jipprovdu spjegazzjoni mmotivata għalfejn jagħmlu dan.

Artikolu 7

Ġestjoni tal-kjavi kriptografiċi

1. Fil-politika ta' ġestjoni tal-kjavi kriptografiċi msemmija fl-Artikolu 6(2), il-punt (d), l-entitajiet finanzjarji għandhom jinkludu rekwiżiti għall-ġestjoni ta' kjavi kriptografiċi matul iċ-ċiklu tal-ħajja kollu tagħhom, inklużi l-ġenerazzjoni, it-tiġdid, il-ħżin, il-backup, l-arkivjar, l-irkupru, it-trażmissjoni, l-irtirar, ir-revoka u l-qerda ta' dawk il-kjavi kriptografiċi.

2. L-entitajiet finanzjarji għandhom jidentifikaw u jimplimentaw kontrolli biex jipproteġu l-kjavi kriptografiċi permezz taċ-ċiklu tal-ħajja kollu tagħhom kontra t-telf, l-aċċess mhux awtorizzat, id-divulgazzjoni u l-modifika. L-entitajiet finanzjarji għandhom ifasslu dawk il-kontrolli abbażi tar-riżultati tal-klassifikazzjoni tad-*data* approvata u l-valutazzjoni tar-riskju tal-ICT.

3. L-entitajiet finanzjarji għandhom jiżviluppaw u jimplimentaw metodi biex jissostitwixxu l-kjavi kriptografiċi f'każ ta' telf jew fejn dawk il-kjavi jiġu kompromessi jew issirilhom ħsara.

4. L-entitajiet finanzjarji għandhom joħolqu u jżommu reġistru għaċ-ċertifikati u għall-apparati għall-ħżin taċ-ċertifikati kollha mill-anqas għal assi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti. L-entitajiet finanzjarji għandhom iżommu dak ir-reġistru aġġornat.

5. L-entitajiet finanzjarji għandhom jiżguraw it-tiġdid fil-pront taċ-ċertifikati qabel l-iskadenza tagħhom.

Taqsima 5

Sigurtà tal-operazzjonijiet tal-ICT

Artikolu 8

Politiki u proċeduri għall-operazzjonijiet tal-ICT

1. Bħala parti mill-politiki, mill-proċeduri, mill-protokolli u mill-għodod tas-sigurtà tal-ICT imsemmija fl-Artikolu 9(2) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politiki u proċeduri għall-ġestjoni tal-operazzjonijiet tal-ICT. Dawk il-politiki u l-proċeduri għandhom jispeċifikaw kif l-entitajiet finanzjarji joperaw, jimmonitorjaw, jikkontrollaw u jirrestawraw l-assi tal-ICT tagħhom, inkluża d-dokumentazzjoni tal-operazzjonijiet tal-ICT.

2. Il-politiki u l-proċeduri għall-operazzjonijiet tal-ICT imsemmija fil-paragrafu 1 għandhom jinkludu dawn kollha li ġejjin:

(a) deskrizzjoni tal-assi tal-ICT, inklużi dawn kollha li ġejjin:

  (i) ir-rekwiżiti dwar l-installazzjoni, il-manutenzjoni, il-konfigurazzjoni u d-deinstallazzjoni siguri ta' sistema tal-ICT;

  (ii) ir-rekwiżiti dwar il-ġestjoni tal-assi tal-informazzjoni użati mill-assi tal-ICT, inklużi l-ipproċessar u l-immaniġġar tagħhom, kemm awtomatizzati kif ukoll manwali;

  (iii) ir-rekwiżiti dwar l-identifikazzjoni u l-kontroll tas-sistemi tal-ICT miruta;

(b) il-kontrolli u l-monitoraġġ tas-sistemi tal-ICT, inklużi dawn kollha li ġejjin:

  (i) backup u restawr tar-rekwiżiti tas-sistemi tal-ICT;

  (ii) rekwiżiti ta' skedar, filwaqt li jitqiesu l-interdipendenzi fost is-sistemi tal-ICT;

  (iii) protokolli għall-informazzjoni tar-rekord tal-awditjar u tar-reġistru tas-sistema;

  (iv) rekwiżiti biex jiġi żgurat li t-twettiq tal-awditjar intern u ttestjar ieħor jimminimizza t-tfixkil fl-operazzjonijiet kummerċjali;

  (v) rekwiżiti dwar is-separazzjoni tal-ambjenti ta' produzzjoni tal-ICT mill-ambjenti tal-iżvilupp, tal-ittestjar u minn ambjenti oħrajn mhux tal-produzzjoni;

  (vi) rekwiżiti għat-twettiq tal-iżvilupp u l-ittestjar f'ambjenti li jkunu separati mill-ambjent ta' produzzjoni;

  (vii) rekwiżiti għat-twettiq tal-iżvilupp u l-ittestjar fl-ambjenti ta' produzzjoni;

(c) it-trattament tal-iżbalji li jikkonċernaw is-sistemi tal-ICT, inklużi dawn kollha li ġejjin:

(i) proċeduri u protokolli għat-trattament tal-iżbalji;

(ii) kuntatti ta' appoġġ u eskalazzjoni, inklużi kuntatti ta' appoġġ estern f'każ ta' kwistjonijiet operazzjonali jew tekniċi mhux mistennija;

(iii) bidu mill-ġdid tas-sistema tal-ICT, it-treġija lura u l-proċeduri ta' rkupru għall-użu f'każ ta' tfixkil fis-sistema tal-ICT.

Għall-finijiet tal-punt (b)(v), is-separazzjoni għandha tqis il-komponenti kollha tal-ambjent, inklużi l-kontijiet, id-*data* jew il-konnessjonijiet, kif meħtieġ mill-Artikolu 13, l-ewwel subartikolu, il-punt (a).

Għall-finijiet tal-punt (b)(vii), il-politiki u l-proċeduri msemmija fil-paragrafu 1 għandhom jipprevedu li l-każijiet li fihom jitwettaq l-ittestjar f'ambjent ta' produzzjoni jkunu identifikati b'mod ċar, immotivati, ikunu għal perjodi ta' żmien limitati u jiġu approvati mill-funzjoni rilevanti f'konformità mal-Artikolu 16(6). L-entitajiet finanzjarji għandhom jiżguraw id-disponibbiltà, il-kunfidenzjalità, l-integrità u l-awtenticità tas-sistemi tal-ICT u tad-*data* tal-produzzjoni matul l-iżvilupp u l-attivitajiet ta' ttestjar fl-ambjent ta' produzzjoni.

Artikolu 9

Ġestjoni tal-kapaċità u tal-prestazzjoni

1. Bħala parti mill-politiki, mill-proċeduri, mill-protokolli u mill-għodod tas-sigurtà tal-ICT imsemmija fl-Artikolu 9(2) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċeduri ta' ġestjoni tal-kapaċità u tal-prestazzjoni għal dawn li ġejjin:

(a) l-identifikazzjoni tar-rekwiżiti tal-kapaċità tas-sistemi tal-ICT tagħhom;

(b) l-applikazzjoni tal-ottimizzazzjoni tar-riżorsi;

(c) il-proċeduri ta' monitoraġġ għall-manutenzjoni u t-titjib ta':

(i) id-disponibbiltà tas-sistemi tad-*data* u tal-ICT;

(ii) l-effiċjenza tas-sistemi tal-ICT;

(iii) il-prevenzjoni ta' nuqqas ta' kapaċità tal-ICT.

2. Il-proċeduri ta' ġestjoni tal-kapaċità u tal-prestazzjoni msemmija fil-paragrafu 1 għandhom jiżguraw li l-entitajiet finanzjarji jieħdu miżuri li huma xierqa biex jissodisfaw l-ispeċifiċitajiet tas-sistemi tal-ICT bi proċessi twal jew kumplessi ta' akkwist jew ta' approvazzjoni jew sistemi tal-ICT li huma intensivi fl-użu tar-riżorsi.

Artikolu 10

Ġestjoni tal-vulnerabbiltà u tal-patches

1. Bħala parti mill-politiki, mill-proċeduri, mill-protokolli u mill-għodod tas-sigurtà tal-ICT imsemmija fl-Artikolu 9(2) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċeduri ta' ġestjoni tal-vulnerabbiltà.

2. Il-proċeduri ta' ġestjoni tal-vulnerabbiltà msemmija fil-paragrafu 1 għandhom:

(a) jidentifikaw u jaġġornaw riżorsi ta' informazzjoni rilevanti u affidabbli biex jibnu u jsostnu s-sensibilizzazzjoni dwar il-vulnerabbiltajiet;

(b) jiżguraw it-twettiq ta' skennjar u valutazzjonijiet awtomatizzati għall-vulnerabbiltajiet fuq l-assi tal-ICT, li permezz tagħhom il-frekwenza u l-ambitu ta' dawk l-attivitajiet għandhom ikunu proporzjonati għall-klassifikazzjoni stabbilita f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554 u l-profil tar-riskju ġenerali tal-assi tal-ICT;

(c) jivverifikaw jekk:

(i) Il-fornituri terzi ta' servizzi tal-ICT jittrattawx il-vulnerabbiltajiet relatati mas-servizzi tal-ICT pprovduti lill-entità finanzjarja;

(ii) jekk dawk il-fornituri ta' servizzi jirrapportawx lill-entità finanzjarja mill-inqas il-vulnerabbiltajiet kritiċi u l-istatistika u x-xejriet f'waqtu;

(d) jittraċċaw l-użu ta':

(i) libreriji ta' partijiet terzi, inklużi libreriji b'sors miftuħ, użati minn servizzi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti;

(ii) servizzi tal-ICT żviluppati mill-entità finanzjarja nnifisha jew speċifikament personalizzati jew żviluppati għall-entità finanzjarja minn fornitur terz ta' servizzi tal-ICT;

(e) jistabbilixxu proċeduri għad-divulgazzjoni responsabbli tal-vulnerabbiltajiet lill-klijenti, lill-kontropartijiet u lill-pubbliku;

(f) jagħtu prijorità lill-varar tal-patches u ta' miżuri oħrajn ta' mitigazzjoni biex jiġu indirizzati l-vulnerabbiltajiet identifikati;

(g) jimmonitorjaw u jivverifikaw ir-rimedju tal-vulnerabbiltajiet;

(h) jirrikjedu r-reġistrazzjoni ta' kwalunkwe vulnerabbiltà individwata li taffettwa s-sistemi tal-ICT u l-monitoraġġ tar-riżoluzzjoni tagħhom.

Għall-finijiet tal-punt (b), l-entitajiet finanzjarji għandhom iwettqu mill-inqas darba fil-ġimgħa skennjar u valutazzjonijiet awtomatizzati għall-vulnerabbiltajiet fuq l-assi tal-ICT għall-assi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti.

Għall-finijiet tal-punt (c), l-entitajiet finanzjarji għandhom jitolbu li l-fornituri terzi ta' servizzi tal-ICT jinvestigaw il-vulnerabbiltajiet rilevanti, jiddeterminaw il-kawżi ewlenin u jimplimentaw azzjoni ta' mitigazzjoni xierqa.

Għall-finijiet tal-punt (d), l-entitajiet finanzjarji għandhom, meta jkun xieraq f'kollaborazzjoni mal-fornitur terz ta' servizzi tal-ICT, jimmonitorjaw il-verżjoni u l-aġġornamenti possibbli tal-libreriji ta' partijiet terzi. Fil-każ ta' assi tal-ICT lesti għall-użu (kummerċjalment disponibbli) jew komponenti tal-assi tal-ICT miksuba u użati fl-operat ta' servizzi tal-ICT li ma jappoġġawx funzjonijiet kritiċi jew importanti, l-entitajiet finanzjarji għandhom jintraċċaw l-użu sa fejn ikun possibbli ta' libreriji ta' partijiet terzi, inklużi libreriji b'sors miftuħ.

Għall-finijiet tal-punt (f), l-entitajiet finanzjarji għandhom iqisu l-kritikalità tal-vulnerabbiltà, il-klassifikazzjoni stabbilita f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554, u l-profil tar-riskju tal-assi tal-ICT affettwati mill-vulnerabbiltajiet identifikati.

3. Bħala parti mill-politiki, mill-proċeduri, mill-protokolli u mill-għodod tas-sigurtà tal-ICT imsemmija fl-Artikolu 9(2) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċeduri tal-ġestjoni tal-patches.

4. Il-proċeduri tal-ġestjoni tal-patches imsemmija fil-paragrafu 3 għandhom:

(a) sa fejn ikun possibbli, jidentifikaw u jevalwaw is-software u l-hardware patches disponibbli u l-aġġornamenti bl-użu ta' għodod awtomatizzati;

(b) jidentifikaw proċeduri ta' emerġenza għall-patching u għall-aġġornament tal-assi tal-ICT;

(c) jittestjaw u jvaraw is-software u l-hardware patches u l-aġġornamenti msemmija fl-Artikolu 8(2), il-punti (b)(v), (vi) u (vii);

(d) jistabbilixxu skadenzi għall-installazzjoni ta' software u hardware patches u proċeduri ta' eskalazzjoni f'każ li dawk l-iskadenzi ma jkunux jistgħu jiġu ssodisfati.

Artikolu 11

Sigurtà tad-*data* u tas-sistema

1. Bħala parti mill-politiki, mill-proċeduri, mill-protokolli u mill-għodod tas-sigurtà tal-ICT imsemmija fl-Artikolu 9(2) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċedura ta' sigurtà tad-*data* u tas-sistema.

2. Il-proċedura ta' sigurtà tad-*data* u tas-sistema msemmija fil-paragrafu 1 għandu jkun fiha l-elementi kollha li ġejjin relatati mas-sigurtà tad-*data* u tas-sistema tal-ICT, f'konformità mal-klassifikazzjoni stabbilita f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554:

(a) ir-restrizzjonijiet fuq l-aċċess imsemmija fl-Artikolu 21 ta' dan ir-Regolament, li jappoġġaw ir-rekwiżiti ta' protezzjoni għal kull livell ta' klassifikazzjoni;

(b) l-identifikazzjoni ta' linja bażi ta' konfigurazzjoni sigura għall-assi tal-ICT li jimminimizzaw l-esponiment ta' dawk l-assi tal-ICT għat-theddid ċibernetiku u l-miżuri biex jiġi vverifikat regolarment li dawk il-linji bażi jintużaw b'mod effettiv;

(c) l-identifikazzjoni ta' miżuri ta' sigurtà biex jiġi żgurat li jiġi installat biss software awtorizzat fis-sistemi tal-ICT u fl-apparati tal-punt tat-tmiem;

(d) l-identifikazzjoni ta' miżuri ta' sigurtà kontra kodiċijiet malizzjużi;

(e) l-identifikazzjoni ta' miżuri ta' sigurtà biex jiġi żgurat li jintużaw biss mezzi għall-ħżin tad-*data*, sistemi u apparati ta' punt tat-tmiem awtorizzati għat-trasferiment u l-ħżin tad-*data* tal-entità finanzjarja;

(f) ir-rekwiżiti li ġejjin biex jiġi żgurat l-użu ta' apparati ta' punt tat-tmiem portabbli u ta' apparati ta' punt tat-tmiem privati mhux portabbli:

  (i) ir-rekwiżit li tintuża soluzzjoni ta' ġestjoni għall-ġestjoni mill-bogħod tal-apparati tal-punt tat-tmiem u biex id-*data* tal-entità finanzjarja titħassar mill-bogħod;

  (ii) ir-rekwiżit li jintużaw mekkaniżmi ta' sigurtà li ma jistgħux jiġu mmodifikati, jitneħħew jew jiġu evitati mill-membri tal-persunal jew mill-fornituri terzi ta' servizzi tal-ICT b'mod mhux awtorizzat;

  (iii) ir-rekwiżit li jintużaw apparati għall-ħżin tad-*data* li jistgħu jitneħħew biss meta r-riskju residwali tal-ICT jibqa' fil-livell ta' tolleranza tar-riskju tal-entità finanzjarja msemmi fl-Artikolu 3, l-ewwel subparagrafu, il-punt (a);

(g) il-proċess biex titħassar b'mod sigur id-*data*, preżenti fil-bini tal-entità finanzjarja jew maħżuna esternament, li l-entità finanzjarja ma għadhiex teħtieġ li tiġbor jew taħżen;

(h) il-proċess għar-rimi jew id-dekummissjonar b'mod sigur ta' apparati għall-ħżin tad-*data* preżenti fil-bini tal-entità finanzjarja jew maħżuna esternament li jkun fihom informazzjoni kunfidenzjali;

(i) l-identifikazzjoni u l-implimentazzjoni ta' miżuri ta' sigurtà għall-prevenzjoni tat-telf u l-iżvelar tad-*data* u għas-sistemi u għall-apparati tal-punt tat-tmiem;

(j) l-implimentazzjoni ta' miżuri ta' sigurtà biex jiġi żgurat li t-telexogħol u l-użu ta' apparati ta' punt tat-tmiem privati ma jkollhomx impatt negattiv fuq is-sigurtà tal-ICT tal-entità finanzjarja;

(k) għall-assi jew għas-servizzi tal-ICT operati minn fornitur terz ta' servizzi tal-ICT, l-identifikazzjoni u l-implimentazzjoni ta' rekwiżiti biex tinżamm ir-reżiljenza operazzjonali diġitali, f'konformità mar-riżultati tal-klassifikazzjoni tad-*data* u tal-valutazzjoni tar-riskju tal-ICT.

Għall-finijiet tal-punt (b), il-linja bażi ta' konfigurazzjoni sigura msemmija f'dak il-punt għandha tqis il-prattiki ewlenin u t-tekniki xierqa stabbiliti fl-istandards iddefiniti fl-Artikolu 2, il-punt (1) tar-Regolament (UE) Nru 1025/2012.

Għall-finijiet tal-punt (k), l-entitajiet finanzjarji għandhom iqisu dan li ġej:

(a) l-implimentazzjoni tas-settings rakkomandati mill-bejjiegħ dwar l-elementi operati mill-entità finanzjarja;

(b) allokazzjoni ċara tar-rwoli u tar-responsabbiltajiet tas-sigurtà tal-informazzjoni bejn l-entità finanzjarja u l-fornitur terz ta' servizzi tal-ICT, f'konformità mal-prinċipju tar-responsabbiltà sħiħa tal-entità finanzjarja fuq il-fornitur terz ta' servizzi tal-ICT tagħha msemmi fl-Artikolu 28(1), il-punt (a), tar-Regolament (UE) 2022/2554, u għall-entitajiet finanzjarji msemmija fl-Artikolu 28(2) ta' dak ir-Regolament, u f'konformità mal-politika tal-entità finanzjarja dwar l-użu ta' servizzi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti;

(c) il-ħtieġa li jiġu żgurati u miżmuma kompetenzi adegwati fl-entità finanzjarja fil-ġestjoni u s-sigurtà tas-servizz użat;

(d) miżuri tekniċi u organizzazzjonali biex jimminimizzaw ir-riskji relatati mal-infrastruttura użata mill-fornitur terz ta' servizzi tal-ICT għas-servizzi tal-ICT tiegħu, filwaqt li jitqiesu l-prattiki ewlenin u l-istandards kif iddefiniti fl-Artikolu 2, il-punt (1) tar-Regolament (UE) Nru 1025/2012.

Artikolu 12

Reġistrazzjoni

1. L-entitajiet finanzjarji għandhom, bħala parti mis-salvagwardji kontra l-intrużjonijiet u l-użu ħażin tad-*data*, jiżviluppaw, jiddokumentaw, u jimplimentaw proċeduri, protokolli u għodod ta' reġistrazzjoni.

2. Il-proċeduri, il-protokolli, u l-għodod tar-reġistrazzjoni msemmija fil-paragrafu 1 għandhom jinkludu dawn kollha li ġejjin:

(a) l-identifikazzjoni tal-avvenimenti li għandhom jiġu rreġistrati, il-perjodu ta' żamma tar-reġistri, u l-miżuri biex tiġi żgurata u mmaniġġjata d-*data* tar-reġistri, filwaqt li jitqies l-iskop li għalih jinħolqu r-reġistri;

(b) l-allinjament tal-livell ta' dettall tar-reġistri mal-iskop u l-użu tagħhom biex tkun tista' ssir id-detezzjoni effettiva ta' attivitajiet anomali kif imsemmi fl-Artikolu 24;

(c) ir-rekwiżit li jiġu rreġistrati l-avvenimenti relatati ma' dawn kollha li ġejjin:

(i) il-kontroll loġiku u fiżiku tal-aċċess, kif imsemmi fl-Artikolu 21, u l-ġestjoni tal-identità;

(ii) il-ġestjoni tal-kapaċità;

(iii) il-ġestjoni tat-tibdil;

(iv) l-operazzjonijiet tal-ICT, inklużi attivitajiet tas-sistema tal-ICT;

(v) l-attivitajiet tat-traffiku tan-network, inkluża l-prestazzjoni tan-network tal-ICT;

(d) miżuri għall-protezzjoni ta' sistemi ta' reġistrazzjoni u ta' informazzjoni tar-reġistru minn tbagħbis, tħassir u aċċess mhux awtorizzat waqt li jkunu wieqfa, fi tranżitu, u, meta rilevanti, waqt l-użu;

(e) miżuri biex jiġi individwat falliment tas-sistemi ta' reġistrazzjoni;

(f) mingħajr preġudizzju għal kwalunkwe rekwiżit regolatorju applikabbli skont id-dritt tal-Unjoni jew id-dritt nazzjonali, is-sinkronizzazzjoni tal-arloġġi ta' kull waħda mis-sistemi tal-ICT tal-entità finanzjarja fuq sors tal-ħin ta' referenza affidabbli ddokumentat.

Għall-finijiet tal-punt (a), l-entitajiet finanzjarji għandhom jistabbilixxu l-perjodu ta' żamma, filwaqt li jqisu l-objettivi tas-sigurtà tan-negozju u tal-informazzjoni, ir-raġuni għar-reġistrazzjoni tal-avveniment fir-reġistri u r-riżultati tal-valutazzjoni tar-riskju tal-ICT.

Taqsima 6

Sigurtà tan-network

Artikolu 13

Ġestjoni tas-sigurtà tan-network

L-entitajiet finanzjarji għandhom, bħala parti mis-salvagwardji li jiżguraw is-sigurtà tan-networks kontra l-intrużjonijiet u l-użu ħażin tad-*data*, jiżviluppaw, jiddokumentaw u jimplimentaw politiki, proċeduri, protokolli u għodod dwar il-ġestjoni tas-sigurtà tan-network, inklużi dawn kollha li ġejjin:

(a) is-segregazzjoni u s-segmentazzjoni tas-sistemi u tan-networks tal-ICT filwaqt li jitqiesu:

(i) il-kritikalità jew l-importanza tal-funzjoni li jappoġġaw dawk is-sistemi u n-networks tal-ICT;

(ii) il-klassifikazzjoni stabbilita f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554;

(iii) il-profil tar-riskju kumplessiv tal-assi tal-ICT bl-użu ta' dawk is-sistemi u networks;

(b) id-dokumentazzjoni tal-konnessjonijiet tan-network u l-flussi tad-*data* kollha tal-entità finanzjarja;

(c) l-użu ta' network separat u ddedikat għall-amministrazzjoni tal-assi tal-ICT;

(d) l-identifikazzjoni u l-implimentazzjoni ta' kontrolli tal-aċċess għan-network biex jiġu evitati u identifikati konnessjonijiet man-network tal-entità finanzjarja minn kwalunkwe apparat jew sistema mhux awtorizzati, jew kwalunkwe punt tat-tmiem li ma jissodisfax ir-rekwiżiti ta' sigurtà tal-entità finanzjarja;

(e) il-kriptaġġ tal-konnessjonijiet tan-network li jgħaddu minn fuq in-networks korporattivi, in-networks pubbliċi, in-networks domestiċi, in-networks ta' partijiet terzi, u n-networks mingħajr fili, għall-protokolli ta' komunikazzjoni użati, filwaqt li jitqiesu r-riżultati tal-klassifikazzjoni tad-*data* approvata, ir-riżultati tal-valutazzjoni tar-riskju tal-ICT u l-kriptaġġ tal-konnessjonijiet tan-network imsemmija fl-Artikolu 6(2);

(f) id-disinn ta' networks f'konformità mar-rekwiżiti tas-sigurtà tal-ICT stabbiliti mill-entità finanzjarja, filwaqt li jitqiesu l-prattiki ewlenin biex jiġu żgurati l-kunfidenzjalità, l-integrità u d-disponibbiltà tan-network;

(g) l-iżgurar tat-traffiku tan-network bejn in-networks interni u l-Internet u konnessjonijiet esterni oħrajn;

(h) l-identifikazzjoni tar-rwoli u tar-responsabbiltajiet u tal-passi għall-ispeċifikazzjoni, għall-implimentazzjoni, għall-approvazzjoni, għat-tibdil u għar-rieżami tar-regoli dwar il-firewalls u tal-filtri tal-konnessjonijiet;

(i) il-prestazzjoni tar-rieżamijiet tal-arkitettura tan-network u tad-disinn tas-sigurtà tan-network darba fis-sena, u perjodikament għall-mikrointraprizi, biex jiġu identifikati l-vulnerabbiltajiet potenzjali;

(j) il-miżuri biex jiġu iżolati temporanjament, meta meħtieġ, is-subnetworks, u l-komponenti u l-apparati tan-network;

(k) l-implimentazzjoni ta' linja bażi ta' konfigurazzjoni sigura tal-komponenti kollha tan-network, u t-twebbis tan-network u tal-apparati tan-network f'konformità ma' kwalunkwe struzzjoni tal-bejjiegħ, u, meta applikabbli, standards, kif iddefiniti fl-Artikolu 2, il-punt (1) tar-Regolament (UE) Nru 1025/2012, u prattiki ewlenin;

(l) il-proċeduri biex jiġu llimitati, imblokkati u tterminati s-sistema u s-sessjonijiet mill-boghod wara perjodu speċifikat ta' inattività;

(m) għall-ftehimiet dwar is-servizzi tan-network:

(i) l-identifikazzjoni u l-ispeċifikazzjoni tal-miżuri tas-sigurtà tal-ICT u tal-informazzjoni, tal-livelli ta' servizz u tar-rekwiżiti ta' ġestjoni tas-servizzi kollha tan-network;

(ii) jekk dawk is-servizzi humiex ipprovduti minn fornitur ta' servizzi intragrupp tal-ICT jew minn fornituri terz ta' servizzi tal-ICT.

Għall-finijiet tal-punt (h), l-entitajiet finanzjarji għandhom iwettqu r-rieżami tar-regoli dwar il-firewall u tal-filtri tal-konnessjonijiet fuq bażi regolari f'konformità mal-klassifikazzjoni stabbilita f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554 u mal-profil tar-riskju ġenerali tas-sistemi tal-ICT involuti. Għas-sistemi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti, l-entitajiet finanzjarji għandhom jivverifikaw l-adegwatezza tar-regoli eżistenti dwar il-firewall u l-filtri ta' konnessjoni mill-anqas kull 6 xhur.

Artikolu 14

Żgurar tal-informazzjoni fi tranżitu

1. Bħala parti mis-salvagwardji biex jiġu ppreżervati d-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data*, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw il-politiki, il-proċeduri, il-protokolli u l-għodod għall-protezzjoni tal-informazzjoni fi tranżitu. L-entitajiet finanzjarji għandhom b'mod partikolari jiżguraw dan kollu li ġej:

(a) id-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data* matul it-trażmissjoni tan-network u l-istabbiliment ta' proċeduri biex tiġi vvalutata l-konformità ma' dawk ir-rekwiżiti;

(b) il-prevenzjoni u l-individwazzjoni ta' żvelar tad-*data* u t-trasferiment sigur ta' informazzjoni bejn l-entità finanzjarja u l-partijiet esterni;

(c) li r-rekwiżiti dwar il-kunfidenzjalità jew l-arranġamenti ta' nondivulgazzjoni li jirriflettu l-ħtiġijiet tal-entità finanzjarja għall-protezzjoni tal-informazzjoni kemm għall-persunal tal-entità finanzjarja kif ukoll għal partijiet terzi jiġu implimentati, iddokumentati u rrieżaminati regolarment.

2. L-entitajiet finanzjarji għandhom ifasslu l-politiki, il-proċeduri, il-protokolli u l-għodod għall-protezzjoni tal-informazzjoni fi tranżitu msemmija fil-paragrafu 1 abbażi tar-riżultati tal-klassifikazzjoni tad-*data* approvata u tal-valutazzjoni tar-riskju tal-ICT.

Taqsima 7

Ġestjoni tal-proġetti tal-ICT u tat-tibdil tagħhom

Artikolu 15

Ġestjoni tal-proġetti tal-ICT

1. Bħala parti mis-salvagwardji biex jiġu ppreżervati d-disponibbiltà, l-awtenticità, l-integrità u l-kunfidenzjalità tad-*data*, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politika ta' ġestjoni tal-proġetti tal-ICT.

2. Il-politika ta' ġestjoni tal-proġetti tal-ICT imsemmija fil-paragrafu 1 għandha tispeċifika l-elementi li jiżguraw il-ġestjoni effettiva tal-proġetti tal-ICT relatati mal-akkwiżizzjoni, mal-manutenzjoni u, meta applikabbli, mal-iżvilupp tas-sistemi tal-ICT tal-entità finanzjarja.

3. Il-politika ta' ġestjoni tal-proġetti tal-ICT imsemmija fil-paragrafu 1 għandha tinkludi dan kollu li ġej:

(a) l-objettivi tal-proġetti tal-ICT;

(b) il-governanza tal-proġetti tal-ICT, inklużi r-rwoli u r-responsabbiltajiet;

(c) l-ippjanar, il-perjodu ta' żmien u l-passi tal-proġetti tal-ICT;

(d) valutazzjoni tar-riskju tal-proġetti tal-ICT;

(e) stadji importanti rilevanti;

(f) rekwiżiti tal-ġestjoni tat-tibdil;

(g) l-ittestjar tar-rekwiżiti kollha, inklużi r-rekwiżiti tas-sigurtà u l-proċess ta' approvazzjoni rispettiv meta tintuża sistema tal-ICT fl-ambjent ta' produzzjoni.

4. Il-politika ta' ġestjoni tal-proġetti tal-ICT imsemmija fil-paragrafu 1 għandha tiżgura l-implimentazzjoni sigura tal-proġetti tal-ICT permezz tal-għoti tal-informazzjoni u l-għarfien espert meħtieġa mill-qasam tan-negozju jew mill-funzjonijiet affettwati mill-proġett tal-ICT.

5. F'konformità mal-valutazzjoni tar-riskju tal-proġetti tal-ICT imsemmija fil-paragrafu 3, il-punt (d), il-politika ta' ġestjoni tal-proġetti tal-ICT imsemmija fil-paragrafu 1 għandha tipprevedi li l-istabbiliment u l-progress tal-proġetti tal-ICT li jkollhom impatt fuq funzjonijiet kritiċi jew importanti tal-entità finanzjarja u r-riskji assoċjati tagħhom jiġu rrapportati lill-korp maniġerjali kif ġej:

(a) individwalment jew f'aggregazzjoni, skont l-importanza u d-daqs tal-proġetti tal-ICT;

(b) perjodikament u, meta meħtieġ, fuq bażi mmexxija minn avvenimenti.

Artikolu 16

Akkwiżizzjoni, żvilupp u manutenzjoni tas-sistemi tal-ICT

1. Bħala parti mis-salvagwardji biex jiġu ppreżervati d-disponibbiltà, l-awtenticità, l-integrità u l-kunfidenzjalità tad-*data*, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politika li tirregola l-akkwiżizzjoni, l-iżvilupp u l-manutenzjoni tas-sistemi tal-ICT. Dik il-politika għandha:

(a) tidentifika prattiki u metodoloġiji tas-sigurtà relatati mal-akkwiżizzjoni, mal-iżvilupp u mal-manutenzjoni tas-sistemi tal-ICT;

(b) tirrikjedi l-identifikazzjoni ta':

(i) speċifikazzjonijiet tekniċi u speċifikazzjonijiet tekniċi tal-ICT, kif iddefiniti fl-Artikolu 2, il-punti (4) u (5) tar-Regolament (UE) Nru 1025/2012;

(ii) rekwiżiti relatati mal-akkwiżizzjoni, mal-iżvilupp u mal-manutenzjoni tas-sistemi tal-ICT, b'enfasi partikolari fuq ir-rekwiżiti tas-sigurtà tal-ICT u fuq l-approvazzjoni tagħhom mill-funzjoni kummerċjali rilevanti u mis-sid tal-assi tal-ICT f'konformità mal-arranġamenti ta' governanza interna tal-entità finanzjarja;

(c) tispeċifika l-miżuri biex jiġi mmitigat ir-riskju ta' tibdil mhux intenzjonat jew ta' manipulazzjoni intenzjonata tas-sistemi tal-ICT matul l-iżvilupp, il-manutenzjoni u l-varar ta' dawk is-sistemi tal-ICT fl-ambjent ta' produzzjoni.

2. L-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċedura ta' akkwiżizzjoni, żvilupp u manutenzjoni tas-sistemi tal-ICT għall-ittestjar u l-approvazzjoni tas-sistemi kollha tal-ICT qabel l-użu tagħhom u wara l-manutenzjoni, f'konformità mal-Artikolu 8(2), il-punt (b), il-punti (v), (vi) u (vii). Il-livell ta' ttestjar għandu jkun proporzjonat għall-kritikalità tal-proċeduri kummerċjali u tal-assi tal-ICT ikkonċernati. L-ittestjar għandu jkun iddisinjat biex jivverifika li sistemi ġodda tal-ICT ikunu adegwati biex jaħdmu kif maħsub, inkluża l-kwalità tas-software żviluppat internament.

Il-kontropartijiet ċentrali għandhom, minbarra r-rekwiżiti stabbiliti fl-ewwel subparagrafu, jinvolvu, kif xieraq, fid-disinn u fit-twettiq tal-ittestjar imsemmi fl-ewwel subparagrafu:

(a) il-membri tal-ikklerjar u klijenti;

(b) il-kontropartijiet ċentrali interoperabbli;

(c) partijiet interessati oħrajn.

Id-depożitorji ċentrali tat-titoli għandhom, minbarra r-rekwiżiti stabbiliti fl-ewwel subparagrafu, jinvolvu, kif xieraq, fid-disinn u fit-twettiq tal-ittestjar imsemmi fl-ewwel subparagrafu:

(a) l-utenti;

(b) il-forniturі ta' utilitajiet kritiċi u servizzi kritiċi;

(c) depożitorji ċentrali tat-titoli oħrajn;

(d) infrastrutturi tas-suq oħrajn;

(e) kwalunkwe istituzzjoni oħra li magħha d-depożitorji ċentrali tat-titoli identifikaw interdipendenzi fil-politika ta' kontinwità tal-operat tagħhom.

3. Il-proċedura msemmija fil-paragrafu 2 għandu jkun fiha t-twettiq tar-rieżamijiet tal-kodiċi tas-sors li jkopru kemm l-ittestjar statiku kif ukoll dak dinamiku. Dak l-ittestjar għandu jkun fih ittestjar tas-sigurtà għal sistemi u applikazzjonijiet esposti għall-Internet f'konformità mal-Artikolu 8(2), il-punt (b), il-punti (v), (vi) u (vii). L-entitajiet finanzjarji għandhom:

(a) jidentifikaw u janalizzaw il-vulnerabbiltajiet u l-anomaliji fil-kodiċi tas-sors;

(b) jadottaw pjan ta' azzjoni biex jindirizzaw dawk il-vulnerabbiltajiet u l-anomaliji;

(c) jimmonitorjaw l-implimentazzjoni ta' dak il-pjan ta' azzjoni.

4. Il-proċedura msemmija fil-paragrafu 2 għandu jkun fiha ttestjar tas-sigurtà ta' pakketti ta' software mhux aktar tard mill-fażi ta' integrazzjoni, f'konformità mal-Artikolu 8(2), il-punti (b)(v), (vi) u (vii).

5. Il-proċeduri msemmija fil-paragrafu 2 għandhom jipprevedu li:

(a) l-ambjenti mhux tal-produzzjoni jaħżnu biss *data* anonimizzata, psewdonimizzata jew *data* tal-produzzjoni aleatorja;

(b) l-entitajiet finanzjarji għandhom jipproteġu l-integrità u l-kunfidenzjalità tad-*data* f'ambjenti mhux tal-produzzjoni.

6. B'deroga mill-paragrafu 5, il-proċedura msemmija fil-paragrafu 2 tista' tipprevedi li d-*data* tal-produzzjoni tinħażen biss għal okkażjonijiet speċifiċi ta' ttestjar, għal perjodi ta' żmien limitati u wara l-approvazzjoni mill-funzjoni rilevanti u r-rapportar ta' dawn l-okkażjonijiet lill-funzjoni tal-ġestjoni tar-riskju tal-ICT.

7. Il-proċedura msemmija fil-paragrafu 2 għandu jkun fiha l-implimentazzjoni ta' kontrolli biex tiġi protetta l-integrità tal-kodiċi tas-sors tas-sistemi tal-ICT li jiġu żviluppati internament jew minn fornitur terz ta' servizzi tal-ICT u li jiġu kkonsenjati lill-entità finanzjarja minn fornitur terz ta' servizzi tal-ICT.

8. Il-proċedura msemmija fil-paragrafu 2 għandha tipprevedi li software proprjetarju u, meta fattibbli, il-kodiċi tas-sors ipprovduti mill-forniturі terzi ta' servizzi tal-ICT jew li ġejjin minn proġetti ta' sors miftuħ, jridu jiġu analizzati u ttestjati f'konformità mal-paragrafu 3 qabel l-użu tagħhom fl-ambjent ta' produzzjoni.

9. Il-paragrafi 1 sa 8 ta' dan l-Artikolu għandhom japplikaw ukoll għas-sistemi tal-ICT żviluppati jew ġestiti minn utenti barra l-funzjoni tal-ICT, bl-użu ta' approċċ ibbażat fuq ir-riskju.

Artikolu 17

Ġestjoni tat-tibdil fl-ICT

1. Bħala parti mis-salvagwardji biex jiġu ppreżervati d-disponibbiltà, l-awtenticità, l-integrità u l-kunfidenzjalità tad-*data*, l-entitajiet finanzjarji għandhom jinkludu fil-proċeduri ta' ġestjoni tat-tibdil fl-ICT imsemmija fl-Artikolu 9(4), il-punt (e), tar-Regolament (UE) 2022/2554, fir-rigward tat-tibdiliet kollha fis-software, fil-hardware, fil-komponenti tal-firmware, fis-sistemi, jew fil-parametri tas-sigurtà, l-elementi kollha li ġejjin:

(a) verifika ta' jekk ir-rekwiżiti tas-sigurtà tal-ICT ġewx issodisfati;

(b) mekkaniżmi biex tiġi żgurata l-indipendenza tal-funzjonijiet li japprovaw it-tibdiliet u l-funzjonijiet responsabbli għat-talba u għall-implimentazzjoni ta' dawk it-tibdiliet;

(c) deskrizzjoni ċara tar-rwoli u tar-responsabbiltajiet biex jiġi żgurat li:

(i) it-tibdiliet ikunu speċifikati u ppjanati;

(ii) tkun iddisinjata tranżizzjoni adegwata;

(iii) it-tibdiliet jiġu ttestjati u ffinalizzati b'mod ikkontrollat;

(iv) ikun hemm assigurazzjoni tal-kwalità effettiva;

(d) id-dokumentazzjoni u l-komunikazzjoni tad-dettalji tat-tibdil, inklużi:

(i) l-għan u l-ambitu tat-tibdil;

(ii) l-iskeda ta' żmien għall-implimentazzjoni tat-tibdil;

(iii) l-eżiti mistennija;

(e) l-identifikazzjoni tal-proċeduri u tar-responsabbiltajiet ta' riżerva, inklużi l-proċeduri u r-responsabbiltajiet għat-twaqqif ta' tibdiliet jew għall-irkupru minn tibdiliet li ma ġewx implimentati b'suċċess;

(f) il-proċeduri, il-protokolli u l-għodod għall-ġestjoni ta' tibdiliet ta' emerġenza li jipprovdu salvagwardji adegwati;

(g) il-proċeduri għad-dokumentazzjoni, għall-evalwazzjoni mill-ġdid, għall-valutazzjoni u għall-approvazzjoni ta' tibdiliet ta' emerġenza wara l-implimentazzjoni tagħhom, inklużi alternattivi u patches;

(h) l-identifikazzjoni tal-impatt potenzjali ta' tibdil fuq il-miżuri eżistenti tas-sigurtà tal-ICT u valutazzjoni ta' jekk dan it-tibdil jirrikjedix l-adozzjoni ta' miżuri addizzjonali tas-sigurtà tal-ICT.

2. Wara li jkunu għamlu tibdiliet sinifikanti fis-sistemi tal-ICT tagħhom, il-kontropartijiet ċentrali u d-depożitorji ċentrali tat-titoli għandhom jissottomettu s-sistemi tal-ICT tagħhom għal ittestjar strett billi jissimulaw kundizzjonijiet ta' stress.

Il-kontropartijiet ċentrali għandhom jinvolvu, kif xieraq, fid-disinn u fit-twettiq tal-ittestjar imsemmi fl-ewwel subparagrafu:

(a) il-membri tal-ikklerjar u klijenti;

(b) il-kontropartijiet ċentrali interoperabbli;

(c) partijiet interessati oħrajn;

Id-depożitorji ċentrali tat-titoli għandhom, kif xieraq, jinvolvu fid-disinn u fit-twettiq tal-ittestjar imsemmi fl-ewwel subparagrafu:

(a) l-utenti;

(b) il-forniturі ta' utilitajiet kritiċi u servizzi kritiċi;

(c) depożitorji ċentrali tat-titoli oħrajn;

(d) infrastrutturi tas-suq oħrajn;

(e) kwalunkwe istituzzjoni oħra li magħha d-depożitorji ċentrali tat-titoli identifikaw interdipendenzi fil-politika tagħhom dwar il-kontinwità tal-operat tal-ICT.

Taqsima 8

Artikolu 18

Sigurtà fiżika u ambjentali

1. Bħala parti mis-salvagwardji biex jiġu ppreżervati d-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data*, l-entitajiet finanzjarji għandhom jispeċifikaw, jiddokumentaw u jimplimentaw politika ta' sigurtà fiżika u ambjentali. L-entitajiet finanzjarji għandhom jiddisinjaw dik il-politika fid-dawl tax-xenarju tat-theddid ċibernetiku, f'konformità mal-klassifikazzjoni stabbilita f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554, u fid-dawl tal-profil tar-riskju ġenerali tal-assi tal-ICT u tal-assi ta' informazzjoni aċċessibbli.

2. Il-politika tas-sigurtà fiżika u ambjentali msemmija fil-paragrafu 1 għandha tinkludi dan kollu li ġej:

(a) referenza għat-taqsima tal-politika dwar il-kontroll tad-drittijiet tal-ġestjoni tal-aċċess imsemmija fl-Artikolu 21, l-ewwel paragrfu, il-punt (g);

(b) miżuri għall-protezzjoni mill-attakki, mill-aċċidenti u mit-theddid u l-perikli ambjentali, il-bini, iċ-ċentri tad-*data* tal-entità finanzjarja u ż-żoni ddeżinjati sensittivi identifikati mill-entità finanzjarja, fejn hemm l-assi tal-ICT u l-assi tal-informazzjoni;

(c) miżuri biex jiġu żgurati l-assi tal-ICT, kemm fil-bini tal-entità finanzjarja kif ukoll barra minnu, filwaqt li jitqiesu r-riżultati tal-valutazzjoni tar-riskju tal-ICT relatata mal-assi rilevanti tal-ICT;

(d) miżuri biex jiġu żgurati d-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tal-assi tal-ICT, tal-assi tal-informazzjoni u tal-apparati ta' kontroll fiżiku tal-aċċess tal-entità finanzjarja permezz tal-manutenzjoni xierqa;

(e) miżuri biex jiġu ppreżervati d-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data*, inklużi:

(i) politika ta' skrivanija żbarazzata għad-dokumenti;

(ii) politika ċara ta' skrin vojt għall-faċilitajiet tal-ipproċessar tal-informazzjoni.

Għall-finijiet tal-punt (b), il-miżuri għall-protezzjoni mit-theddid u mill-perikli ambjentali għandhom ikunu proporzjonati mal-importanza tal-bini, taċ-ċentri tad-*data*, taż-żoni ddeżinjati sensittivi u mal-kritikalità tal-operazzjonijiet jew tas-sistemi tal-ICT li jinsabu fihom.

Għall-finijiet tal-punt (c), il-politika tas-sigurtà fiżika u ambjentali msemmija fil-paragrafu 1 għandu jkun fiha miżuri biex tiġi pprovduta protezzjoni xierqa għall-assi tal-ICT li jitħallew waħedhom.

KAPITOLU II

Politika tar-riżorsi umani u kontroll tal-aċċess

Artikolu 19

Politika tar-riżorsi umani

Fil-politika tagħhom dwar ir-riżorsi umani jew politiki rilevanti oħrajn, l-entitajiet finanzjarji għandhom jinkludu l-elementi kollha li ġejjin relatati mas-sigurtà tal-ICT:

(a) l-identifikazzjoni u l-assenjazzjoni ta' kwalunkwe responsabbiltà speċifika għas-sigurtà tal-ICT;

(b) rekwiżiti għall-persunal tal-entità finanzjarja u tal-fornituri terzi ta' servizzi tal-ICT li jużaw jew jaċċessaw l-assi tal-ICT tal-entità finanzjarja biex:

(i) jiġu informati dwar il-politiki, il-proċeduri u l-protokolli tas-sigurtà tal-ICT tal-entità finanzjarja u jaderixxu magħhom;

(ii) ikunu konxji dwar il-kanali ta' rapportar stabbiliti mill-entità finanzjarja għall-individwazzjoni ta' mġiba anomala, inklużi, meta applikabbli, il-kanali ta' rapportar stabbiliti f'konformità mad-Direttiva (UE) 2019/1937 tal-Parlament Ewropew u tal-Kunsill ([11]);

(iii) għall-persunal, li jirritorna lill-entità finanzjarja, mat-terminazzjoni tal-impjieg, l-assi tal-ICT u l-assi ta' informazzjoni tanġibbli kollha fil-pussess tiegħu li jappartjenu għall-entità finanzjarja.

Artikolu 20

Ġestjoni tal-identità

1. Bħala parti mill-kontroll tagħhom tad-drittijiet ta' ġestjoni tal-aċċess, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politiki u proċeduri ta' ġestjoni tal-identità li jiżguraw l-identifikazzjoni u l-awtentikazzjoni uniċi tal-persuni fiżiċi u tas-sistemi li jaċċessaw l-informazzjoni tal-entitajiet finanzjarji biex jippermettu l-assenjament tad-drittijiet ta' aċċess tal-utenti f'konformità mal-Artikolu 21.

2. Il-politiki u l-proċeduri tal-ġestjoni tal-identità msemmija fil-paragrafu 1 għandhom jinkludu dawn kollha li ġejjin:

(a) mingħajr preġudizzju għall-Artikolu 21, l-ewwel paragrafu, il-punt (c), identità unika li tikkorrispondi għal kont tal-utent uniku għandha tiġi assenjata lil kull membru tal-persunal tal-entità finanzjarja jew tal-persunal tal-fornituri terzi ta' servizzi tal-ICT li jaċċessaw l-assi tal-informazzjoni u l-assi tal-ICT tal-entità finanzjarja;

(b) proċess ta' ġestjoni taċ-ċiklu tal-ħajja għall-identitajiet u l-kontijiet li jimmaniġġaw il-ħolqien, it-tibdil, ir-rieżami u l-aġġornament, id-diżattivazzjoni temporanja u t-terminazzjoni tal-kontijiet kollha.

Għall-finijiet tal-punt (a), l-entitajiet finanzjarji għandhom iżommu rekords tal-kompiti kollha ta' identità. Dawk ir-rekords għandhom jinżammu wara riorganizzazzjoni tal-entità finanzjarja jew wara t-tmiem tar-relazzjoni kuntrattwali mingħajr preġudizzju għar-rekwiżiti taż-żamma stabbiliti fid-dritt tal-Unjoni u d-dritt nazzjonali applikabbli.

Għall-finijiet tal-punt (b), l-entitajiet finanzjarji għandhom, meta fattibbli u xieraq, jużaw soluzzjonijiet awtomatizzati għall-proċess tal-ġestjoni tal-identità taċ-ċiklu tal-ħajja.

Artikolu 21

Kontroll tal-aċċess

Bħala parti mill-kontroll tagħhom tad-drittijiet ta' ġestjoni tal-aċċess, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politika li jkun fiha dawn kollha li ġejjin:

(a) l-assenjazzjoni tad-drittijiet ta' aċċess għall-assi tal-ICT abbażi tal-prinċipji tal-ħtieġa ta' tagħrif, tal-ħtieġa ta' użu u tal-anqas privileġġ, inkluż għal aċċess mill-bogħod u ta' emerġenza;

(b) is-segregazzjoni tad-dmirijiet imfassla biex jipprevjenu aċċess mhux iġġustifikat għal *data* kritika jew biex jipprevjenu l-allokazzjoni ta' kombinazzjonijiet ta' drittijiet ta' aċċess li jistgħu jintużaw biex jiġu evitati l-kontrolli;

(c) dispożizzjoni dwar l-akkontabilità tal-utent, billi jiġi llimitat sa fejn ikun possibbli l-użu ta' kontijiet tal-utenti ġeneriċi u kondiviżi u jiġi żgurat li l-utenti jkunu identifikabbli għall-azzjonijiet imwettqa fis-sistemi tal-ICT f'kull ħin;

([11]) Id-Direttiva (UE) 2019/1937 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Ottubru 2019 dwar il-protezzjoni ta' persuni li jirrapportaw dwar ksur tal-liġi tal-Unjoni (ĠU L 305, 26.11.2019, p. 17, ELI: https://eur-lex.europa.eu/eli/dir/2019/1937/oj).

(d) dispożizzjoni dwar ir-restrizzjonijiet tal-aċċess għall-assi tal-ICT, li tistabbilixxi kontrolli u għodod biex jiġi pprevenut aċċess mhux awtorizzat;

(e) proċeduri ta' ġestjoni tal-kontijiet għall-għoti, għat-tibdil jew għar-revoka tad-drittijiet ta' aċċess għall-kontijiet tal-utenti u l-kontijiet ġeneriċi, inklużi l-kontijiet tal-amministraturi ġeneriċi, u wkoll dispożizzjoni dwar dawn kollha li ġejjin:

(i) l-assenjazzjoni tar-rwoli u tar-responsabbiltajiet għall-għoti, għar-rieżami u għar-revoka tad-drittijiet ta' aċċess;

(ii) l-assenjazzjoni ta' aċċess privileġġat, ta' emerġenza u ta' amministratur fuq bażi ta' ħtieġa ta' użu jew fuq bażi *ad hoc* għas-sistemi kollha tal-ICT;

(iii) l-irtirar tad-drittijiet ta' aċċess mingħajr dewmien żejjed mat-terminazzjoni tal-impjieg jew meta l-aċċess ma jkunx għadu meħtieġ;

(iv) aġġornament tad-drittijiet ta' aċċess fejn ikunu meħtieġa tibdiliet u mill-anqas darba fis-sena għas-sistemi kollha tal-ICT, għajr għas-sistemi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti u mill-anqas kull 6 xhur għas-sistemi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti;

(f) metodi ta' awtentikazzjoni, inklużi dawn kollha li ġejjin:

(i) l-użu ta' metodi ta' awtentikazzjoni proporzjonati għall-klassifikazzjoni stabbilita f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554 u għall-profil tar-riskju ġenerali tal-assi tal-ICT u filwaqt li jitqiesu prattiki ewlenin;

(ii) l-użu ta' metodi ta' awtentikazzjoni b'saħħithom f'konformità ma' prattiki u tekniki ewlenin għall-aċċess mill-bogħod għan-network tal-entità finanzjarja, għal aċċess privileġġat, għal aċċess għall-assi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti jew assi tal-ICT li huma aċċessibbli għall-pubbliku;

(g) miżuri ta' kontroll għall-aċċess fiżiku li jinkludu:

(i) l-identifikazzjoni u r-reġistrazzjoni ta' persuni fiżiċi li huma awtorizzati jaċċessaw il-bini, iċ-ċentri tad-*data* u ż-żoni ddeżinjati sensittivi identifikati mill-entità finanzjarja fejn hemm l-assi tal-ICT u tal-informazzjoni;

(ii) l-għoti ta' drittijiet ta' aċċess fiżiku għal assi kritiċi tal-ICT lil persuni awtorizzati biss, f'konformità mal-prinċipji tal-ħtieġa ta' tagħrif u tal-anqas privileġġ, u fuq bażi *ad hoc*;

(iii) il-monitoraġġ tal-aċċess fiżiku għall-bini, għaċ-ċentri tad-*data* u għal żoni ddeżinjati sensittivi identifikati mill-entità finanzjarja fejn ikun hemm l-assi tal-ICT u tal-informazzjoni jew it-tnejn li huma;

(iv) ir-rieżami tad-drittijiet ta' aċċess fiżiku biex jiġi żgurat li d-drittijiet ta' aċċess mhux meħtieġa jiġu rrevokati minnufih.

Għall-finijiet tal-punt (e)(i), l-entitajiet finanzjarji għandhom jistabbilixxu l-perjodu ta' żamma filwaqt li jqisu l-objettivi tas-sigurtà tan-negozju u tal-informazzjoni, ir-raġunijiet għar-reġistrazzjoni tal-avveniment fir-reġistri u r-riżultati tal-valutazzjoni tar-riskju tal-ICT.

Għall-finijiet tal-punt (e)(ii), l-entitajiet finanzjarji għandhom, meta possibbli, jużaw kontijiet iddedikati għat-twettiq ta' kompiti amministrattivi fuq is-sistemi tal-ICT. Meta jkun fattibbli u xieraq, l-entitajiet finanzjarji għandhom jużaw soluzzjonijiet awtomatizzati għall-ġestjoni tal-aċċess għall-privileġġ.

Għall-finijiet tal-punt (g)(i), l-identifikazzjoni u r-reġistrazzjoni għandhom ikunu proporzjonati mal-importanza tal-bini, taċ-ċentri tad-*data*, taż-żoni ddeżinjati sensittivi u mal-kritikalità tal-operazzjonijiet jew tas-sistemi tal-ICT li jinsabu fihom.

Għall-finijiet tal-punt (g)(iii), il-monitoraġġ għandu jkun proporzjonat mal-klassifikazzjoni stabbilita f'konformità mal-Artikolu 8(1) tar-Regolament (UE) 2022/2554 u għall-kritikalità taż-żona aċċessata.

KAPITOLU III

Individwazzjoni ta' inċidenti relatati mal-ICT u r-rispons għalihom

Artikolu 22

Politika ta' ġestjoni tal-inċidenti relatati mal-ICT

Bħala parti mill-mekkaniżmi biex jiġu individwati attivitajiet anomali, inklużi kwistjonijiet ta' prestazzjoni tan-network tal-ICT u inċidenti relatati mal-ICT, l-entitajiet finanzjarji għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politika ta' inċidenti relatata mal-ICT li permezz tagħha għandhom:

(a) jiddokumentaw il-proċess ta' ġestjoni tal-inċidenti relatati mal-ICT imsemmi fl-Artikolu 17 tar-Regolament (UE) 2022/2554;

(b) jistabbilixxu lista ta' kuntatti rilevanti ma' funzjonijiet interni u partijiet ikkonċernati esterni li huma involuti direttament fis-sigurtà tal-operazzjonijiet tal-ICT, inkluż dwar:

(i) l-individwazzjoni u l-monitoraġġ tat-theddid ċibernetiku;

(ii) l-individwazzjoni ta' attivitajiet anomali;

(iii) il-ġestjoni tal-vulnerabbiltà;

(c) jistabbilixxu, jimplimentaw u joperaw mekkaniżmi tekniċi, organizzazzjonali u operazzjonali biex jappoġġaw il-proċess ta' ġestjoni tal-inċidenti relatati mal-ICT, inklużi mekkaniżmi li jippermettu individwazzjoni fil-pront ta' attivitajiet u mġiba anomali f'konformità mal-Artikolu 23 ta' dan ir-Regolament;

(d) iżommu l-evidenza kollha relatata ma' inċidenti relatati mal-ICT għal perjodu li ma għandux ikun itwal milli meħtieġ għall-finijiet li għalihom tinġabar id-*data*, proporzjonali mal-kritikalità tal-funzjonijiet tan-negozju affettwati, tal-proċessi ta' appoġġ u tal-assi tal-ICT u tal-informazzjoni, f'konformità mal-[Artikolu [15] tar-Regolament Delegat tal-Kummissjoni (UE) 2024/1772 ([12]) u ma' kwalunkwe rekwiżit ta' żamma applikabbli skont id-dritt tal-Unjoni;

(e) jistabbilixxu u jimplimentaw mekkaniżmi biex janalizzaw inċidenti u xejriet sinifikanti jew rikorrenti relatati mal-ICT fl-għadd u fl-okkorrenza ta' inċidenti relatati mal-ICT.

Għall-finijiet tal-punt (d), l-entitajiet finanzjarji għandhom iżommu l-evidenza msemmija f'dak il-punt b'mod sigur.

Artikolu 23

Individwazzjoni ta' attivitajiet anomali u kriterji għall-individwazzjoni ta' inċidenti relatati mal-ICT u r-rispons għalihom

1. L-entitajiet finanzjarji għandhom jistabbilixxu rwoli u responsabbiltajiet ċari għall-individwazzjoni effettiva ta' inċidenti relatati mal-ICT u ta' attivitajiet anomali, u r-rispons effettiv għalihom.

2. Il-mekkaniżmu biex jiġu individwati fil-pront attivitajiet anomali, inklużi kwistjonijiet ta' prestazzjoni tan-network tal-ICT u inċidenti relatati mal-ICT, kif imsemmi fl-Artikolu 10(1) tar-Regolament (UE) 2022/2554, għandu jippermetti lill-entitajiet finanzjarji:

(a) jiġbru, jimmonitorjaw u janalizzaw dawn kollha li ġejjin:

(i) il-fatturi interni u esterni, inklużi mill-anqas ir-reġistri miġbura f'konformità mal-Artikolu 12 ta' dan ir-Regolament, informazzjoni mill-funzjonijiet tan-negozju u tal-ICT, u kwalunkwe problema rrapportata mill-utenti tal-entità finanzjarja;

(ii) it-theddid ċibernetiku intern u estern potenzjali, filwaqt li jitqiesu x-xenarji użati b'mod komuni minn atturi u xenarji ta' theddid ibbażati fuq attività ta' intelligence tat-theddid;

([12]) Ir-Regolament Delegat tal-Kummissjoni (UE) 2024/1772 tat-13 ta' Marzu 2024 li jissupplimenta r-Regolament (UE) 2022/2554 tal-Parlament Ewropew u tal-Kunsill fir-rigward ta' standards tekniċi regolatorji li jispeċifikaw il-kriterji għall-klassifikazzjoni ta' inċidenti relatati mal-ICT u theddid ċibernetiku, li jistabbilixxi livelli limitu ta' materjalità u li jispeċifika d-dettalji tar-rapporti ta' inċidenti kbar (ĠU L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(iii) notifika ta' inċident relatat mal-ICT minn fornitur terz ta' servizzi tal-ICT tal-entità finanzjarja individwat fis-sistemi u n-networks tal-ICT tal-fornitur terz ta' servizzi tal-ICT u li jista' jaffettwa lill-entità finanzjarja;

(b) jidentifikaw attivitajiet u mġiba anomali, u jimplimentaw għodod li jiġġeneraw allerti għal attivitajiet u mġiba anomali, mill-anqas għall-assi tal-ICT u għall-assi ta' informazzjoni li jappoġġaw funzjonijiet kritiċi jew importanti;

(c) jagħtu prijorità lill-allerti imsemmija fil-punt (b) biex jippermettu l-ġestjoni tal-inċidenti relatati mal-ICT individwati fil-ħin ta' riżoluzzjoni mistenni, kif speċifikat mill-entitajiet finanzjarji, kemm matul kif ukoll barra l-ħinijiet tax-xogħol;

(d) jirreġistraw, janalizzaw u jevalwaw kwalunkwe informazzjoni rilevanti dwar l-attivitajiet u l-imġiba anomali kollha b'mod awtomatiku jew manwali.

Għall-finijiet tal-punt (b), l-għodod imsemmija f'dak il-punt għandu jkun fihom l-għodod li jipprovdu allerti awtomatizzati bbażati fuq regoli predefiniti biex jiġu identifikati l-anomaliji li jaffettwaw il-kompletezza u l-integrità tas-sorsi tad-*data* jew il-ġbir tar-reġistri.

3. L-entitajiet finanzjarji għandhom jipproteġu kwalunkwe reġistrazzjoni tal-attivitajiet anomali kontra t-tbagħbis u l-aċċess mhux awtorizzat waqt li jkunu wieqfa, fi tranżitu u, meta rilevanti, waqt l-użu.

4. L-entitajiet finanzjarji għandhom jirreġistraw l-informazzjoni rilevanti kollha għal kull attività anomala individwata li tippermetti:

(a) l-identifikazzjoni tad-data u l-ħin tal-okkorrenza tal-attività anomala;

(b) l-identifikazzjoni tad-data u l-ħin tal-individwazzjoni tal-attività anomala;

(c) l-identifikazzjoni tat-tip tal-attività anomala.

5. L-entitajiet finanzjarji għandhom iqisu l-kriterji kollha li ġejjin biex jiskattaw il-proċessi ta' individwazzjoni ta' inċidenti relatati mal-ICT, u ta' rispons għalihom, imsemmija fl-Artikolu 10(2) tar-Regolament (UE) 2022/2554:

(a) indikazzjonijiet li setgħet twettqet attività malizzjuża f'sistema jew f'network tal-ICT, jew li din is-sistema jew network tal-ICT setgħu ġew kompromessi;

(b) telf ta' *data* individwat b'rabta mad-disponibbiltà, mal-awtenticità, mal-integrità u mal-kunfidenzjalità tad-*data*;

(c) impatt negattiv individwat fuq it-tranżazzjonijiet u l-operazzjonijiet tal-entità finanzjarja;

(d) nuqqas ta' disponibbiltà ta' sistemi u networks tal-ICT;

6. Għall-finijiet tal-paragrafu 5, l-entitajiet finanzjarji għandhom iqisu wkoll il-kritikalità tas-servizzi affettwati.

KAPITOLU IV

Ġestjoni tal-kontinwità tal-operat tal-ICT

Artikolu 24

Komponenti tal-politika dwar il-kontinwità tal-operat tal-ICT

1. L-entitajiet finanzjarji għandhom jinkludu fil-politika tagħhom dwar il-kontinwità tal-operat tal-ICT imsemmija fl-Artikolu 11(1) tar-Regolament (UE) 2022/2554 dawn kollha li ġejjin:

(a) deskrizzjoni ta':

(i) l-objettivi tal-politika dwar il-kontinwità tal-operat tal-ICT, inkluża l-interrelazzjoni tal-ICT u l-kontinwità tal-operat ġenerali, u filwaqt li jitqiesu r-riżultati tal-valutazzjoni tal-impatt fuq in-negozju (BIA) msemmija fl-Artikolu 11(5) tar-Regolament (UE) 2022/2554;

(ii) l-ambitu tal-arranġamenti, tal-pjanijiet, tal-proċeduri u tal-mekkaniżmi tal-kontinwità tal-operat tal-ICT, inklużi l-limitazzjonijiet u l-esklużjonijiet;

(iii) il-perjodu ta' żmien li għandu jiġi kopert mill-arranġamenti, mill-pjanijiet, mill-proċeduri u mill-mekkaniżmi tal-kontinwità tal-operat tal-ICT;

(iv) il-kriterji biex jiġu attivati u diżattivati l-pjanijiet ta' kontinwità tal-operat tal-ICT, il-pjanijiet ta' rispons u rkupru tal-ICT, u l-pjanijiet ta' komunikazzjoni f'każ ta' kriżi;

(b) dispożizzjonijiet dwar:

(i) il-governanza u l-organizzazzjoni biex tiġi implimentata l-politika dwar il-kontinwità tal-operat tal-ICT, inklużi r-rwoli, ir-responsabbiltajiet u l-proċeduri ta' eskalazzjoni li jiżguraw li jkunu disponibbli riżorsi suffiċjenti;

(ii) l-allinjament bejn il-pjanijiet ta' kontinwità tal-operat tal-ICT u l-pjanijiet ġenerali ta' kontinwità tal-operat, li jikkonċerna mill-anqas dawn kollha li ġejjin:

(1) xenarji potenzjali ta' falliment, inklużi x-xenarji msemmija fl-Artikolu 26(2) ta' dan ir-Regolament;

(2) objettivi ta' rkupru, li jispeċifikaw li l-entità finanzjarja għandha tkun tista' tirkupra l-operazzjonijiet tal-funzjonijiet kritiċi jew importanti tagħha wara tfixkil f'objettiv ta' ħin ta' rkupru u objettiv ta' punt ta' rkupru;

(iii) l-iżvilupp ta' pjanijiet ta' kontinwità tal-operat tal-ICT għal tfixkil serju fin-negozju bħala parti minn dawk il-pjanijiet, u l-prijoritizzazzjoni ta' azzjonijiet ta' kontinwità tal-operat tal-ICT bl-użu ta' approċċ ibbażat fuq ir-riskju;

(iv) l-iżvilupp, l-ittestjar u r-rieżami tal-pjanijiet ta' rispons u ta' rkupru tal-ICT, f'konformità mal-Artikoli 25 u 26 ta' dan ir-Regolament;

(v) ir-rieżami tal-effettività tal-arranġamenti, tal-pjanijiet, tal-proċeduri u tal-mekkaniżmi ta' kontinwità tal-operat tal-ICT implimentati, f'konformità mal-Artikolu 26 ta' dan ir-Regolament;

(vi) l-allinjament tal-politika dwar il-kontinwità tal-operat tal-ICT ma':

(1) il-politika dwar il-komunikazzjoni kif imsemmija fl-Artikolu 14(2) tar-Regolament (UE) 2022/2554;

(2) l-azzjonijiet ta' komunikazzjoni u ta' komunikazzjoni tal-kriżijiet imsemmija fl-Artikolu 11(2), il-punt (e) tar-Regolament (UE) 2022/2554.

2. Minbarra r-rekwiżiti msemmija fil-paragrafu 1, il-kontropartijiet ċentrali għandhom jiżguraw li l-politika dwar il-kontinwità tal-operat tal-ICT tagħhom:

(a) ikun fiha ħin massimu ta' rkupru għall-funzjonijiet kritiċi tagħhom li ma jkunx itwal minn sagħtejn;

(b) tqis ir-rabtiet esterni u l-interdipendenzi fl-infrastrutturi finanzjarji, inklużi ċ-ċentri tan-negozjar approvati mill-kontroparti ċentrali, is-saldu tat-titoli u s-sistemi ta' pagament, u l-istituzzjonijiet ta' kreditu użati mill-kontroparti ċentrali jew minn kontroparti ċentrali konnessa;

(c) tirrikjedi li jkun hemm arranġamenti stabbiliti biex:

(i) jiżguraw il-kontinwità ta' funzjonijiet kritiċi jew importanti tal-kontroparti ċentrali abbażi ta' xenarji ta' diżastri;

(ii) iżommu sit tal-ipproċessar sekondarju li kapaċi jiżgura l-kontinwità ta' funzjonijiet kritiċi jew importanti tal-kontroparti ċentrali identiċi għas-sit primarju;

(iii) iżommu jew ikollhom aċċess immedjat għal sit ta' negozju sekondarju, biex jippermettu lill-persunal jiżgura l-kontinwità tas-servizz jekk il-post primarju tan-negozju ma jkunx disponibbli;

(iv) iqisu l-ħtieġa ta' siti addizzjonali ta' pproċessar, b'mod partikolari jekk id-diversità tal-profili tar-riskji tas-siti primarji u sekondarji ma tipprovdix biżżejjed kunfidenza li l-objettivi ta' kontinwità tal-operat tal-kontroparti ċentrali se jintlaħqu fix-xenarji kollha.

Għall-finijiet tal-punt (a), il-kontropartijiet ċentrali għandhom ilestu l-proċeduri u l-pagamenti ta' tmiem il-jum fil-ħin u fil-jum meħtieġa fiċ-ċirkostanzi kollha.

Għall-finijiet tal-punt (c)(i), l-arranġamenti msemmija f'dak il-punt għandhom jindirizzaw id-disponibbiltà ta' riżorsi umani adegwati, il-ħin ta' qtugħ tas-servizz massimu għal funzjonijiet kritiċi u l-kommutazzjoni awtomatika u l-irkupru ta' sit sekondarju.

Għall-finijiet tal-punt (c)(ii), is-sit tal-ipproċessar sekondarju msemmi f'dak il-punt għandu jkollu profil tar-riskju ġeografiku li jkun distint minn dak tas-sit primarju.

3. Minbarra r-rekwiżiti msemmija fil-paragrafu 1, id-depożitorji ċentrali tat-titoli għandhom jiżguraw li l-politika ta' kontinwità tal-operat tal-ICT tagħhom:

(a) tqis kwalunkwe rabta u interdipendenza mal-utenti, mal-utilitajiet kritiċi u mal-forniturі kritiċi tas-servizzi, depożitorji ċentrali tat-titoli oħrajn u infrastrutturi tas-suq oħrajn;

(b) tirrikjedi li l-arranġamenti tagħha għall-kontinwità tal-operat tal-ICT jiżguraw li l-objettiv tal-ħin tal-irkupru għall-funzjonijiet kritiċi jew importanti tagħhom ma jkunx itwal minn sagħtejn.

4. Minbarra r-rekwiżiti msemmija fil-paragrafu 1, iċ-ċentri tan-negozjar għandhom jiżguraw li l-politika ta' kontinwità tal-operat tal-ICT tagħhom tiżgura li:

(a) in-negozjar jista' jerġa' jinbeda wara sagħtejn jew kważi sagħtejn minn inċident ta' tfixkil;

(b) l-ammont massimu ta' *data* li tista' tintilef minn kwalunkwe servizz tal-IT taċ-ċentru tan-negozjar wara inċident ta' tfixkil ikun qrib iż-żero.

Artikolu 25

Ittestjar tal-pjanijiet ta' kontinwità tal-operat tal-ICT

1. Meta jittestjaw il-pjanijiet ta' kontinwità tal-operat tal-ICT f'konformità mal-Artikolu 11(6) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom iqisu l-valutazzjoni tal-impatt fuq in-negozju (BIA) tal-entità finanzjarja u l-valutazzjoni tar-riskju tal-ICT imsemmija fl-Artikolu 3(1), il-punt (b) ta' dan ir-Regolament.

2. L-entitajiet finanzjarji għandhom jivvalutaw permezz tal-ittestjar tal-pjanijiet ta' kontinwità tal-operat tal-ICT tagħhom imsemmija fil-paragrafu 1 jekk ikunux kapaċi jiżguraw il-kontinwità tal-funzjonijiet kritiċi jew importanti tal-entità finanzjarja. Dak l-ittestjar għandu:

(a) jitwettaq abbażi ta' xenarji ta' ttestjar li jissimulaw tfixkil potenzjali, inkluż sett adegwat ta' xenarji severi iżda plawżibbli;

(b) jinkludi l-ittestjar tas-servizzi tal-ICT ipprovduti mill-forniturі terzi ta' servizzi tal-ICT, meta applikabbli;

(c) għall-entitajiet finanzjarji, minbarra l-mikrointrapriżi, kif imsemmi fl-Artikolu 11(6), it-tieni subparagrafu tar-Regolament (UE) 2022/2554, ikun fih xenarji ta' tibdil mill-infrastruttura primarja tal-ICT għall-kapaċità żejda, il-backups u l-faċilitajiet żejda;

(d) ikun imfassal biex jisfida s-suppożizzjonijiet li fuqhom ikunu bbażati l-pjanijiet ta' kontinwità tal-operat, inklużi l-arranġamenti ta' governanza u l-pjanijiet ta' komunikazzjoni dwar il-kriżijiet;

(e) jinkludi proċeduri biex tiġi vverifikata l-kapaċità tal-persunal tal-entitajiet finanzjarji, tal-forniturі terzi ta' servizzi tal-ICT, tas-sistemi tal-ICT u tas-servizzi tal-ICT li jwieġbu b'mod adegwat għax-xenarji debitament meqjusa f'konformità mal-Artikolu 26(2).

Għall-finijiet tal-punt (a), l-entitajiet finanzjarji dejjem għandhom jinkludu fl-ittestjar ix-xenarji meqjusa għall-iżvilupp tal-pjanijiet ta' kontinwità tal-operat.

Għall-finijiet tal-punt (b), l-entitajiet finanzjarji għandhom iqisu debitament ix-xenarji marbuta mal-insolvenza jew il-fallimenti tal-forniturі terzi ta' servizzi tal-ICT jew marbuta mar-riskji politiċi fil-ġuriżdizzjonijiet tal-forniturі terzi ta' servizzi tal-ICT, meta rilevanti.

Għall-finijiet tal-punt (c), l-ittestjar għandu jivverifika jekk mill-anqas funzjonijiet kritiċi jew importanti jistgħux jitħaddmu kif xieraq għal perjodu ta' żmien suffiċjenti, u jekk il-funzjonament normali jistax jerġa' jiġi rrestawrat.

3. Minbarra r-rekwiżiti msemmija fil-paragrafu 2, il-kontropartijiet ċentrali għandhom jinvolvu fl-ittestjar tal-pjanijiet ta' kontinwità tal-operat tal-ICT tagħhom imsemmija fil-paragrafu 1:

(a) il-membri tal-ikklerjar;

(b) il-forniturі esterni;

(c) l-istituzzjonijiet rilevanti fl-infrastruttura finanzjarja li magħhom il-kontropartijiet ċentrali identifikaw interdipendenzi fil-politiki tagħhom dwar il-kontinwità tal-operat.

4. Minbarra r-rekwiżiti msemmija fil-paragrafu 2, id-depożitorji ċentrali tat-titoli għandhom jinvolvu fl-ittestjar tal-pjanijiet ta' kontinwità tal-operat tal-ICT tagħhom imsemmija fil-paragrafu 1, kif xieraq:

(a) l-utenti tad-depożitorji ċentrali tat-titoli;

(b) il-forniturі ta' utilitajiet kritiċi u servizzi kritiċi;

(c) depożitorji ċentrali tat-titoli oħrajn;

(d) infrastrutturi tas-suq oħrajn;

(e) kwalunkwe istituzzjoni oħra li magħha d-depożitorji ċentrali tat-titoli identifikaw interdipendenzi fil-politika ta' kontinwità tal-operat tagħhom.

5. L-entitajiet finanzjarji għandhom jiddokumentaw ir-riżultati tal-ittestjar imsemmi fil-paragrafu 1. Kwalunkwe nuqqas identifikat li jirriżulta minn dak l-ittestjar għandu jiġi analizzat, indirizzat u rrapportat lill-korp maniġerjali.

Artikolu 26

Pjanijiet ta' rispons u ta' rkupru tal-ICT

1. Meta jiżviluppaw il-pjanijiet ta' rispons u ta' rkupru tal-ICT imsemmija fl-Artikolu 11(3) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji għandhom iqisu r-riżultati tal-valutazzjoni tal-impatt fuq in-negozju (BIA) tal-entità finanzjarja. Dawk il-pjanijiet ta' rispons u ta' rkupru tal-ICT għandhom:

(a) jispeċifikaw il-kundizzjonijiet li jwasslu għall-attivazzjoni jew għad-diżattivazzjoni tagħhom, u kwalunkwe eċċezzjoni għal din l-attivazzjoni jew diżattivazzjoni;

(b) jiddeskrivu liema azzjonijiet għandhom jittieħdu biex jiġu żgurati d-disponibbiltà, l-integrità, il-kontinwità u l-irkupru ta' mill-anqas sistemi u servizzi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti tal-entità finanzjarja;

(c) ikunu mfassla biex jissodisfaw l-objettivi ta' rkupru tal-operazzjonijiet tal-entitajiet finanzjarji;

(d) jiġu ddokumentati u jsiru disponibbli għall-persunal involut fl-eżekuzzjoni tal-pjanijiet ta' rispons u ta' rkupru tal-ICT u jkunu faċilment aċċessibbli f'każ ta' emerġenza;

(e) jipprevedu kemm opzjonijiet ta' rkupru fuq perjodu ta' żmien qasir kif ukoll fuq perjodu ta' żmien twil, inkluż l-irkupru parzjali tas-sistemi;

(f) jistabbilixxu l-objettivi tal-pjanijiet ta' rispons u ta' rkupru tal-ICT u l-kundizzjonijiet biex tiġi ddikjarata l-eżekuzzjoni b'suċċess ta' dawk il-pjanijiet.

Għall-finijiet tal-punt (d), l-entitajiet finanzjarji għandhom jispeċifikaw b'mod ċar ir-rwoli u r-responsabbiltajiet.

2. Il-pjanijiet ta' rispons u ta' rkupru tal-ICT imsemmija fil-paragrafu 1 għandhom jidentifikaw ix-xenarji rilevanti, inklużi xenarji ta' tfixkil serju fin-negozju u probabbiltà akbar ta' okkorrenza ta' tfixkil. Dawk il-pjanijiet għandhom jiżviluppaw xenarji bbażati fuq informazzjoni kurrenti dwar it-theddid u dwar it-tagħlimiet meħuda minn okkorrenzi preċedenti ta' tfixkil fin-negozju. L-entitajiet finanzjarji għandhom iqisu debitament ix-xenarji kollha li ġejjin:

(a) attakki ċibernetiċi u kommutazzjonijiet bejn l-infrastruttura primarja tal-ICT u l-kapaċità żejda, il-backups u l-faċilitajiet żejda;

(b) xenarji li fihom il-kwalità tal-forniment ta' funzjoni kritika jew importanti tiddeterjora għal livell inaċċettabbli jew tfalli, u jitqies debitament l-impatt potenzjali tal-insolvenza, jew fallimenti oħrajn, ta' kwalunkwe fornitur terz ta' servizzi terzi tal-ICT rilevanti;

(c) falliment parzjali jew totali tal-bini, inkluż il-bini tal-uffiċċju u tan-negozju, u ċ-ċentri tad-*data*;

(d) falliment sostanzjali tal-assi tal-ICT jew tal-infrastruttura tal-komunikazzjoni;

(e) in-nuqqas ta' disponibbiltà ta' għadd kritiku ta' persunal jew ta' membri tal-persunal responsabbli biex jiggarantixxu l-kontinwità tal-operazzjonijiet;

(f) l-impatt tat-tibdil fil-klima u ta' avvenimenti relatati mad-degradazzjoni tal-ambjent, diżastri naturali, pandemiji u attakki fiżiċi, inklużi intrużjonijiet u attakki terroristiċi;

(g) attakki minn ġewwa;

(h) instabbiltà politika u soċjali, inkluż, meta rilevanti, fil-ġuriżdizzjoni tal-fornitur terz ta' servizzi tal-ICT u fil-post fejn id-*data* tinħażen u tiġi pproċessata;

(i) qtugħ ta' dawl mifrux.

3. Meta l-miżuri ta' rkupru primarju jistgħu ma jkunux fattibbli fuq perjodu ta' żmien qasir minħabba kostijiet, riskji, loġistika jew ċirkostanzi mhux previsti, il-pjanijiet ta' rispons u ta' rkupru tal-ICT imsemmija fil-paragrafu 1 għandhom iqisu għażliet alternattivi.

4. Bħala parti mill-pjanijiet ta' rispons u ta' rkupru tal-ICT imsemmija fil-paragrafu 1, l-entitajiet finanzjarji għandhom iqisu u jimplimentaw miżuri ta' kontinwità biex jimmitigaw il-fallimenti ta' fornituri terzi ta' servizzi tal-ICT ta' servizzi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti tal-entità finanzjarja.

KAPITOLU V

Rapport dwar ir-rieżami tal-qafas tal-ġestjoni tar-riskju tal-ICT

Artikolu 27

Format u kontenut tar-rapport dwar ir-rieżami tal-qafas tal-ġestjoni tar-riskju tal-ICT

1. L-entitajiet finanzjarji għandhom jissottomettu r-rapport dwar ir-rieżami tal-qafas tal-ġestjoni tar-riskju tal-ICT imsemmi fl-Artikolu 6(5) tar-Regolament (UE) 2022/2554 f'format elettroniku li jippermetti t-tiftix.

2. L-entitajiet finanzjarji għandhom jinkludu l-informazzjoni kollha li ġejja fir-rapport imsemmi fil-paragrafu 1:

(a) taqsima introduttorja li:

(i) tidentifika b'mod ċar l-entità finanzjarja li hija s-suġġett tar-rapport, u tiddeskrivi l-istruttura tal-grupp tagħha, meta rilevanti;

(ii) tiddeskrivi l-kuntest tar-rapport f'termini tan-natura, tal-iskala u tal-kumplessità tas-servizzi, tal-attivitajiet u tal-operazzjonijiet tal-entità finanzjarja, l-organizzazzjoni tagħha, il-funzjonijiet kritiċi identifikati, l-istrateġija, il-proġetti jew l-attivitajiet ewlenin li għaddejjin bħalissa, ir-relazzjonijiet u d-dipendenza tagħha fuq servizzi u sistemi tal-ICT interni u kkuntrattati jew l-implikazzjonijiet li telf totali jew degradazzjoni serja ta' sistemi bħal dawn ikollha f'termini ta' funzjonijiet kritiċi jew importanti u l-effiċjenza tas-suq;

(iii) tiġbor fil-qosor it-tibdiliet ewlenin fil-qafas tal-ġestjoni tar-riskju tal-ICT minn meta ġie ppreżentat ir-rapport preċedenti;

(iv) tipprovdi sommarju fil-livell eżekuttiv tal-profil tar-riskju tal-ICT kurrenti u qrib it-terminu, ix-xenarju tat-theddid, l-effettività vvalutata tal-kontrolli tagħha u l-pożizzjoni tas-sigurtà tal-entità finanzjarja;

(b) id-data tal-approvazzjoni tar-rapport mill-korp maniġerjali tal-entità finanzjarja;

(c) deskrizzjoni tar-raġuni għar-rieżami tal-qafas tal-ġestjoni tar-riskju tal-ICT f'konformità mal-Artikolu 6(5) tar-Regolament (UE) 2022/2554;

(d) id-dati tal-bidu u tat-tmiem tal-perjodu ta' rieżami;

(e) indikazzjoni tal-funzjoni responsabbli għar-rieżami;

(f) deskrizzjoni tat-tibdiliet u tat-titjib ewlenin fil-qafas tal-ġestjoni tar-riskju tal-ICT mir-rieżami preċedenti;

(g) sommarju tas-sejbiet tar-rieżami u tal-analiżi ddettaljata u valutazzjoni tas-severità tad-dgħufijiet, tan-nuqqasijiet u tal-lakuni fil-qafas tal-ġestjoni tar-riskju tal-ICT matul il-perjodu ta' rieżami;

(h) deskrizzjoni tal-miżuri biex jiġu indirizzati d-dgħufijiet, in-nuqqasijiet u l-lakuni identifikati, inklużi dawn kollha li ġejjin:

(i) sommarju tal-miżuri meħuda biex jiġu rrimedjati d-dgħufijiet, in-nuqqasijiet u l-lakuni identifikati;

(ii) data mistennija għall-implimentazzjoni tal-miżuri u d-dati relatati mal-kontroll intern tal-implimentazzjoni, inkluża informazzjoni dwar l-istat tal-progress tal-implimentazzjoni ta' dawk il-miżuri fid-data tal-abbozzar tar-rapport, li tispjega, meta applikabbli, jekk ikun hemm riskju li l-iskadenzi ma jkunux jistgħu jiġu rrispettati;

(iii) l-għodod li għandhom jintużaw, u l-identifikazzjoni tal-funzjoni responsabbli għat-twettiq tal-miżuri, bid-dettalji dwar jekk l-għodod u l-funzjonijiet humiex interni jew esterni;

(iv) deskrizzjoni tal-impatt tat-tibdiliet previsti fil-miżuri fuq ir-riżorsi baġitarji, umani u materjali tal-entità finanzjarja, inklużi r-riżorsi ddedikati għall-implimentazzjoni ta' kwalunkwe miżura korrettiva;

(v) informazzjoni dwar il-proċess biex l-awtorità kompetenti tiġi infurmata, meta jkun xieraq;

(vi) meta d-dgħufijiet, in-nuqqasijiet jew il-lakuni identifikati ma jkunux soġġetti għal miżuri korrettivi, spjegazzjoni ddettaljata tal-kriterji użati għall-analiżi tal-impatt ta' dawk id-dgħufijiet, in-nuqqasijiet jew il-lakuni, biex jiġi evalwat ir-riskju residwali tal-ICT relatat u tal-kriterji użati biex jiġi aċċettat ir-riskju residwali relatat;

(i) informazzjoni dwar żviluppi ulterjuri ppjanati tal-qafas tal-ġestjoni tar-riskju tal-ICT;

(j) konklużjonijiet li jirriżultaw mir-rieżami tal-qafas tal-ġestjoni tar-riskju tal-ICT;

(k) informazzjoni dwar ir-rieżamijiet tal-passat, inklużi:

(i) lista ta' rieżamijiet tal-passat sal-lum;

(ii) meta applikabbli, stat ta' implimentazzjoni tal-miżuri korrettivi identifikati mill-aħħar rapport;

(iii) fejn il-miżuri korrettivi proposti fir-rieżamijiet tal-passat urew li ma kinux effettivi jew ħolqu sfidi mhux mistennija, deskrizzjoni ta' kif dawk il-miżuri korrettivi jistgħu jittejbu jew ta' dawk l-isfidi mhux mistennija;

(l) sorsi ta' informazzjoni użati fit-tħejjija tar-rapport, inklużi dawn kollha li ġejjin:

(i) għall-entitajiet finanzjarji għajr il-mikrointrapriżi kif imsemmi fl-Artikolu 6(6) tar-Regolament (UE) 2022/2554, ir-riżultati tal-awditi interni;

(ii) ir-riżultati tal-valutazzjonijiet tal-konformità;

(iii) ir-riżultati tal-ittestjar tar-reżiljenza operazzjonali diġitali, u meta applikabbli r-riżultati tal-ittestjar avvanzat, abbażi tal-ittestjar tal-penetrazzjoni bbażat fuq it-theddid (TLPT), tal-għodod, tas-sistemi u tal-proċessi tal-ICT;

(iv) sorsi esterni.

Għall-finijiet tal-punt (c), fejn ir-rieżami jkun inbeda wara struzzjonijiet superviżorji, jew il-konklużjonijiet idderivati mill-ittestjar tar-reżiljenza operazzjonali diġitali jew mill-proċessi tal-awditjar rilevanti, ir-rapport għandu jkun fih referenzi espliċiti għal dawn l-istruzzjonijiet jew konklużjonijiet, li jippermettu l-identifikazzjoni tar-raġuni għall-bidu tar-rieżami. Meta r-rieżami jkun ingħata bidu wara inċidenti relatati mal-ICT, ir-rapport għandu jkun fih il-lista tal-inċidenti kollha relatati mal-ICT b'analiżi tal-kawżi ewlenin tal-inċidenti.

Għall-finijiet tal-punt (f), id-deskrizzjoni għandu jkun fiha analiżi tal-impatt tat-tibdiliet fuq l-istrateġija tar-reżiljenza operazzjonali diġitali tal-entità finanzjarja, fuq il-qafas ta' kontroll intern tal-ICT tal-entità finanzjarja u fuq il-governanza tal-ġestjoni tar-riskju tal-ICT tal-entità finanzjarja.

TITOLU III

QAFAS ISSIMPLIFIKAT TAL-ĠESTJONI TAR-RISKJU TAL-ICT GĦALL-ENTITAJIET FINANZJARJI MSEMMIJA FL-ARTIKOLU 16(1) TAR-REGOLAMENT (UE) 2022/2554

KAPITOLU I

Qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT

Artikolu 28

Governanza u organizzazzjoni

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandu jkollhom stabbilit qafas ta' governanza u kontroll intern li jiżgura ġestjoni effettiva u prudenti tar-riskju tal-ICT biex jinkiseb livell għoli ta' reżiljenza operazzjonali diġitali.

2. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom, bħala parti mill-qafas issimplifikat tagħhom għall-ġestjoni tar-riskju tal-ICT, jiżguraw li l-korp maniġerjali tagħhom:

(a) ikollu r-responsabbiltà ġenerali li jiżgura li l-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT jippermetti l-kisba tal-istrateġija tan-negozju tal-entità finanzjarja f'konformità mal-predispożizzjoni għar-riskju ta' dik l-entità finanzjarja, u jiżgura li r-riskju tal-ICT jitqies f'dak il-kuntest;

(b) jistabbilixxi rwoli u responsabbiltajiet ċari għall-kompiti kollha relatati mal-ICT;

(c) jistabbilixxi objettivi tas-sigurtà tal-informazzjoni u rekwiżiti tal-ICT;

(d) japprova, jissorvelja u jirrieżamina perjodikament:

(i) il-klassifikazzjoni tal-assi tal-informazzjoni tal-entità finanzjarja kif imsemmi fl-Artikolu 30(1) ta' dan ir-Regolament, il-lista tar-riskji ewlenin identifikati u l-valutazzjoni tal-impatt fuq in-negozju u l-politiki relatati;

(ii) il-pjanijiet ta' kontinwità tal-operat tal-entità finanzjarja, u l-miżuri ta' rispons u ta' rkupru msemmija fl-Artikolu 16(1), il-punt (f) tar-Regolament (UE) 2022/2554;

(e) jalloka u jirrieżamina mill-anqas darba fis-sena l-baġit meħtieġ biex jissodisfa l-ħtiġijiet ta' reżiljenza operazzjonali diġitali tal-entità finanzjarja fir-rigward tat-tipi kollha ta' riżorsi, inklużi programmi rilevanti ta' sensibilizzazzjoni dwar is-sigurtà tal-ICT u taħriġ fir-reżiljenza operazzjonali diġitali u ħiliet fl-ICT għall-persunal kollu;

(f) jispeċifika u jimplimenta l-politiki u l-miżuri inklużi fil-Kapitoli I, II u III ta' dan it-Titolu biex jidentifika, jivvaluta u jimmaniġġa r-riskju tal-ICT li l-entità finanzjarja tkun esposta għalih;

(g) jidentifika u jimplimenta proċeduri, protokolli tal-ICT u għodod li huma meħtieġa biex jiġu protetti l-assi kollha tal-informazzjoni u l-assi tal-ICT;

(h) jiżgura li l-persunal tal-entità finanzjarja jinżamm aġġornat b'għarfien u b'ħiliet suffiċjenti biex jifhem u jivvaluta r-riskju tal-ICT u l-impatt tiegħu fuq l-operazzjonijiet tal-entità finanzjarja, proporzjonali għar-riskju tal-ICT li jkun qed jiġi ġestit;

(i) jistabbilixxi arranġamenti ta' rapportar, inklużi l-frekwenza, il-forma u l-kontenut tar-rapportar lill-korp maniġerjali dwar is-sigurtà tal-informazzjoni u r-reżiljenza operazzjonali diġitali.

3. L-entitajiet finanzjarji msemmija fil-paragrafu 1 jistgħu, f'konformità mad-dritt settorjali tal-Unjoni u d-dritt nazzjonali, jissottokuntrattaw il-kompiti ta' verifika tal-konformità mar-rekwiżiti tal-ġestjoni tar-riskju tal-ICT lil fornituri terzi jew intragrupp ta' servizzi tal-ICT. Fil-każ ta' esternalizzazzjoni bħal din, l-entitajiet finanzjarji għandhom jibqgħu jerfgħu r-responsabbiltà sħiħa għall-verifika tal-konformità mar-rekwiżiti tal-ġestjoni tar-riskju tal-ICT.

4. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jiżguraw segregazzjoni xierqa u l-indipendenza tal-funzjonijiet ta' kontroll u tal-funzjonijiet tal-awditjar intern.

5. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jiżguraw li l-qafas issimplifikat tagħhom tal-ġestjoni tar-riskju tal-ICT ikun soġġett għal awditu intern mill-awdituri, f'konformità mal-pjan tal-awditjar tal-entitajiet finanzjarji. L-awdituri għandu jkollhom biżżejjed għarfien, ħiliet u għarfien espert fir-riskju tal-ICT, u għandhom ikunu indipendenti. Il-frekwenza u l-enfasi tal-awditi tal-ICT għandhom ikunu proporzjonati mar-riskji tal-ICT tal-entità finanzjarja.

6. Abbażi tal-eżitu tal-awditu msemmi fil-paragrafu 5, l-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jiżguraw il-verifika u r-rimedju f'waqthom tas-sejbiet kritiċi tal-awditjar tal-ICT.

Artikolu 29

Politika u miżuri dwar is-sigurtà tal-informazzjoni

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jiżviluppaw, jiddokumentaw u jimplimentaw politika dwar is-sigurtà tal-informazzjoni fil-kuntest tal-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT. Din il-politika dwar is-sigurtà tal-informazzjoni għandha tispeċifika l-prinċipji u r-regoli ta' livell għoli biex jiġu protetti l-kunfidenzjalità, l-integrità, id-disponibbiltà u l-awtentiċità tad-*data* u tas-servizzi li jipprovdu dawk l-entitajiet finanzjarji.

2. Abbażi tal-politika tagħhom dwar is-sigurtà tal-informazzjoni msemmija fil-paragrafu 1, l-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jistabbilixxu u jimplimentaw miżuri ta' sigurtà tal-ICT biex jimmitigaw l-esponiment tagħhom għar-riskju tal-ICT, inklużi miżuri ta' mitigazzjoni implimentati mill-fornituri terzi ta' servizzi tal-ICT.

Il-miżuri ta' sigurtà tal-ICT għandhom jinkludu l-miżuri kollha msemmija fl-Artikoli 30 sa 38.

Artikolu 30

Klassifikazzjoni tal-assi tal-informazzjoni u tal-assi tal-ICT

1. Bħala parti mill-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT imsemmi fl-Artikolu 16(1), il-punt (a) tar-Regolament (UE) 2022/2554, l-entitajiet finanzjarji msemmija fil-paragrafu 1 ta' dak l-Artikolu għandhom jidentifikaw, jikklassifikaw u jiddokumentaw il-funzjonijiet kritiċi jew importanti kollha, l-assi tal-informazzjoni u l-assi tal-ICT li jappoġġaw lilhom u l-interdipendenzi tagħhom. L-entitajiet finanzjarji għandhom jirrieżaminaw dik l-identifikazzjoni u l-klassifikazzjoni kif meħtieġ.

2. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jidentifikaw il-funzjonijiet kritiċi jew importanti kollha appoġġati mill-fornituri terzi ta' servizzi tal-ICT.

Artikolu 31

Ġestjoni tar-riskju tal-ICT

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jinkludu fil-qafas issimplifikat tagħhom tal-ġestjoni tar-riskju tal-ICT dawn kollha li ġejjin:

(a) determinazzjoni tal-livelli ta' tolleranza tar-riskju għar-riskju tal-ICT, f'konformità mal-predispożizzjoni għar-riskju tal-entità finanzjarja;

(b) l-identifikazzjoni u l-valutazzjoni tar-riskji tal-ICT li għalihom hija esposta l-entità finanzjarja;

(c) l-ispeċifikazzjoni tal-istrateġiji ta' mitigazzjoni tal-anqas għar-riskji tal-ICT li ma humiex fil-livelli ta' tolleranza tar-riskju tal-entità finanzjarja;

(d) il-monitoraġġ tal-effettività tal-istrateġiji ta' mitigazzjoni msemmija fil-punt (c);

(e) l-identifikazzjoni u l-valutazzjoni ta' kwalunkwe riskju għas-sigurtà tal-ICT u tal-informazzjoni li jirriżulta minn kwalunkwe tibdil kbir fis-sistema tal-ICT jew fis-servizzi, fil-proċessi jew fil-proċeduri tal-ICT, u mir-riżultati tal-ittestjar tas-sigurtà tal-ICT u wara kwalunkwe inċident kbir relatat mal-ICT.

2. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom iwettqu u jiddokumentaw il-valutazzjoni tar-riskju tal-ICT perjodikament skont il-profil tar-riskju tal-ICT tal-entitajiet finanzjarji.

3. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jimmonitorjaw kontinwament it-theddid u l-vulnerabbiltajiet li huma rilevanti għall-funzjonijiet kritiċi jew importanti tagħhom, u l-assi ta' informazzjoni u l-assi tal-ICT, u għandhom jirrieżaminaw regolarment ix-xenarji ta' riskju li jħallu impatt fuq dawk il-funzjonijiet kritiċi jew importanti.

4. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jistabbilixxu limiti ta' allerti u kriterji biex jiskattaw u jibdew proċessi ta' rispons għal inċidenti relatati mal-ICT.

Artikolu 32

Sigurtà fiżika u ambjentali

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jidentifikaw u jimplimentaw miżuri fiżiċi ta' sigurtà ddisinjati abbażi tax-xenarju tat-theddid u f'konformità mal-klassifikazzjoni msemmija fl-Artikolu 30(1) ta' dan ir-Regolament, il-profil tar-riskju ġenerali tal-assi tal-ICT, u assi ta' informazzjoni aċċessibbli.

2. Il-miżuri msemmija fil-paragrafu 1 għandhom jipproteġu l-bini tal-entitajiet finanzjarji u, meta applikabbli, iċ-ċentri tad-*data* tal-entitajiet finanzjarji fejn hemm l-assi tal-ICT u l-assi tal-informazzjoni minn aċċess mhux awtorizzat, attakki u aċċidenti, u minn theddid u perikli ambjentali.

3. Il-protezzjoni mit-theddid u mill-perikli ambjentali għandha tkun proporzjonata mal-importanza tal-bini kkonċernat u, meta applikabbli, taċ-ċentri tad-*data* u l-kritikalità tal-operazzjonijiet jew tas-sistemi tal-ICT li jinsabu fihom.

KAPITOLU II

Aktar elementi ta' sistemi, protokolli u għodod biex jiġi mminimizzat l-impatt tar-riskju tal-ICT

Artikolu 33

Kontroll tal-Aċċess

L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċeduri għall-kontroll loġiku u fiżiku tal-aċċess għandhom jinfurzaw, jimmonitorjaw u jirrieżaminaw perjodikament dawk il-proċeduri. Dawk il-proċeduri għandu jkun fihom l-elementi ta' kontroll loġiku u fiżiku tal-aċċess li ġejjin:

(a) id-drittijiet ta' aċċess għal assi tal-informazzjoni, għal assi tal-ICT u għall-funzjonijiet appoġġati tagħhom, u għal postijiet kritiċi ta' operazzjoni tal-entità finanzjarja, huma ġestiti fuq bażi ta' ħtieġa ta' tagħrif, ħtieġa ta' użu u tal-anqas privileġġi, inkluż għal aċċess mill-bogħod u ta' emerġenza;

(b) l-akkontabilità tal-utent, li tiżgura li l-utenti jkunu jistgħu jiġu identifikati għall-azzjonijiet imwettqa fis-sistemi tal-ICT;

(c) proċeduri ta' ġestjoni tal-kontijiet għall-għoti, it-tibdil jew ir-revoka tad-drittijiet ta' aċċess għall-kontijiet tal-utenti u l-kontijiet ġeneriċi, inklużi l-kontijiet ta' amministraturi ġeneriċi;

(d) metodi ta' awtentikazzjoni li huma proporzjonati għall-klassifikazzjoni msemmija fl-Artikolu 30(1) u għall-profil tar-riskju ġenerali tal-assi tal-ICT, u li huma bbażati fuq prattiki ewlenin;

(e) id-drittijiet ta' aċċess jiġu rrieżaminati perjodikament u jiġu rtirati meta ma jibqgħux meħtieġa.

Għall-finijiet tal-punt (c), l-entità finanzjarja għandha tassenja aċċess privileġġat, ta' emerġenza u ta' amministratur fuq bażi tal-ħtieġa tal-użu jew fuq bażi *ad hoc* għas-sistemi kollha tal-ICT, u għandha tiġi rreġistrata f'konformità mal-Artikolu 34, l-ewwel paragrafu, il-punt (f).

Għall-finijiet tal-punt (d), l-entitajiet finanzjarji għandhom jużaw metodi ta' awtentikazzjoni b'saħħithom li huma bbażati fuq prattiki ewlenin għall-aċċess mill-bogħod għan-network tal-entitajiet finanzjarji, għall-aċċess privileġġat, u għall-aċċess għall-assi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti li huma disponibbli għall-pubbliku.

Artikolu 34

Sigurtà tal-operazzjonijiet tal-ICT

L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom, bħala parti mis-sistemi, mill-protokolli u mill-għodod tagħhom, u għall-assi kollha tal-ICT:

(a) jimmonitorjaw u jimmaniġġaw iċ-ċiklu tal-ħajja tal-assi kollha tal-ICT;

(b) jimmonitorjaw jekk l-assi tal-ICT humiex appoġġati minn fornituri terzi ta' servizzi tal-ICT ta' entitajiet finanzjarji, meta applikabbli;

(c) jidentifikaw ir-rekwiżiti tal-kapaċità tal-assi u l-miżuri tal-ICT tagħhom biex iżommu u jtejbu d-disponibbiltà u l-effiċjenza tas-sistemi tal-ICT u jipprevjenu n-nuqqas ta' kapaċitajiet tal-ICT qabel ma jimmaterjalizzaw;

(d) iwettqu skennjar u valutazzjonijiet awtomatizzati għall-vulnerabbiltajiet fuq l-assi tal-ICT proporzjonati għall-klassifikazzjoni tagħhom kif imsemmi fl-Artikolu 30(1) u għall-profil tar-riskju ġenerali tal-assi tal-ICT, u jużaw is-software korrettiv biex jirrimedjaw il-vulnerabbiltajiet identifikati;

(e) jimmaniġġaw ir-riskji relatati ma' assi tal-ICT skaduti, mhux appoġġati jew miruta;

(f) jirreġistraw avvenimenti relatati mal-kontroll loġiku u fiżiku tal-aċċess, mal-operazzjonijiet tal-ICT, inklużi l-attivitajiet tat-traffiku tas-sistema u tan-network, u l-ġestjoni tat-tibdil fl-ICT;

(g) jidentifikaw u jimplimentaw miżuri għall-monitoraġġ u l-analiżi ta' informazzjoni dwar attivitajiet u mġiba anomali għal operazzjonijiet kritiċi jew importanti tal-ICT;

(h) jimplimentaw miżuri għall-monitoraġġ ta' informazzjoni rilevanti u aġġornata dwar it-theddid ċibernetiku;

(i) jimplimentaw miżuri biex jidentifikaw tixrid possibbli ta' informazzjoni, kodiċi malizzjuż u theddid ieħor għas-sigurtà, u vulnerabbiltajiet magħrufa pubblikament fis-software u fil-hardware, u jivverifikaw aġġornamenti korrispondenti ġodda dwar is-sigurtà.

Għall-finijiet tal-punt (f), l-entitajiet finanzjarji għandhom jallinjaw il-livell ta' dettall tar-reġistri mal-iskop u l-użu tagħhom tal-assi tal-ICT li jipproduċi dawk ir-reġistri.

Artikolu 35

Sigurtà tad-data, tas-sistema u tan-network

L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom, bħala parti mis-sistemi, il-protokolli u l-għodod tagħhom, jiżviluppaw u jimplimentaw salvagwardji li jiżguraw is-sigurtà tan-networks kontra l-intrużjonijiet u l-użu ħażin tad-*data* u li jippreżervaw id-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data*. B'mod partikolari, l-entitajiet finanzjarji għandhom, filwaqt li jqisu l-klassifikazzjoni msemmija fl-Artikolu 30(1) ta' dan ir-Regolament, jistabbilixxu dan kollu li ġej:

(a) l-identifikazzjoni u l-implimentazzjoni ta' miżuri għall-protezzjoni tad-*data* waqt l-użu, fi tranżitu u waqt li tkun wieqfa;

(b) l-identifikazzjoni u l-implimentazzjoni ta' miżuri ta' sigurtà rigward l-użu ta' software, mezzi għall-ħżin tad-*data*, sistemi u apparati ta' punt tat-tmiem li jittrasferixxu u jaħżnu d-*data* tal-entità finanzjarja;

(c) l-identifikazzjoni u l-implimentazzjoni ta' miżuri biex jiġu pprevenuti u individwati konnessjonijiet mhux awtorizzati man-network tal-entità finanzjarja, u biex jiġi żgurat it-traffiku tan-network bejn in-networks interni tal-entità finanzjarja u l-Internet u konnessjonijiet esterni oħrajn;

(d) l-identifikazzjoni u l-implimentazzjoni ta' miżuri li jiżguraw id-disponibbiltà, l-awtentiċità, l-integrità u l-kunfidenzjalità tad-*data* matul it-trażmissjonijiet tan-network;

(e) proċess biex titħassar b'mod sigur id-*data* fil-bini, jew li tinħażen esternament, li l-entità finanzjarja ma għadhiex teħtieġ tiġbor jew taħżen;

(f) proċess biex l-apparati għall-ħżin tad-*data* fil-bini jew l-apparati għall-ħżin tad-*data* li jinħażnu esternament li jkun fihom informazzjoni kunfidenzjali jintremew b'mod sigur, jew jiġu ddekumissjonati;

(g) l-identifikazzjoni u l-implimentazzjoni ta' miżuri biex jiġi żgurat li t-telexogħol u l-użu ta' apparati ta' punt tat-tmiem privat ma jkollhomx impatt negattiv fuq il-kapaċità tal-entità finanzjarja li twettaq l-attivitajiet kritiċi tagħha b'mod adegwat, f'waqtu u sigur.

Artikolu 36

Ittestjar tas-sigurtà tal-ICT

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jistabbilixxu u jimplimentaw pjan ta' ttestjar tas-sigurtà tal-ICT biex jivvalidaw l-effettività tal-miżuri tas-sigurtà tal-ICT tagħhom żviluppati f'konformità mal-Artikoli 33, 34 u 35 u mal-Artikoli 37 u 38 ta' dan ir-Regolament. L-entitajiet finanzjarji għandhom jiżguraw li dak il-pjan iqis it-theddid u l-vulnerabbiltajiet identifikati bħala parti mill-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT imsemmi fl-Artikolu 31 ta' dan ir-Regolament.

2. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jirrieżaminaw, jivvalutaw u jittestjaw il-miżuri ta' sigurtà tal-ICT, filwaqt li jqisu l-profil tar-riskju ġenerali tal-assi tal-ICT tal-entità finanzjarja.

3. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jimmonitorjaw u jevalwaw ir-riżultati tat-testijiet tas-sigurtà u jaġġornaw il-miżuri tas-sigurtà tagħhom kif xieraq mingħajr dewmien żejjed fil-każ ta' sistemi tal-ICT li jappoġġaw funzjonijiet kritiċi jew importanti.

Artikolu 37

Akkwiżizzjoni, żvilupp u manutenzjoni tas-sistemi tal-ICT

L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jiddisinjaw u jimplimentaw, meta jkun xieraq, proċedura li tirregola l-akkwiżizzjoni, l-iżvilupp u l-manutenzjoni tas-sistemi tal-ICT wara approċċ ibbażat fuq ir-riskju. Dik il-proċedura għandha:

(a) tiżgura li, qabel ma sseħħ kwalunkwe akkwiżizzjoni jew żvilupp tas-sistemi tal-ICT, ir-rekwiżiti funzjonali u mhux funzjonali, inklużi r-rekwiżiti tas-sigurtà tal-informazzjoni, ikunu speċifikati u approvati b'mod ċar mill-funzjoni tan-negozju kkonċernata;

(b) tiżgura l-ittestjar u l-approvazzjoni tas-sistemi tal-ICT qabel l-ewwel użu tagħhom u qabel ma jiġu introdotti t-tibdiliet fl-ambjent ta' produzzjoni;

(c) tidentifika miżuri biex jiġi mmitigat ir-riskju ta' tibdil mhux intenzjonat jew ta' manipulazzjoni intenzjonata tas-sistemi tal-ICT matul l-iżvilupp u l-implimentazzjoni fl-ambjent ta' produzzjoni.

Artikolu 38

Ġestjoni tal-proġetti tal-ICT u tat-tibdil tagħhom

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċedura ta' ġestjoni tal-proġetti tal-ICT u għandhom jispeċifikaw ir-rwoli u r-responsabbiltajiet għall-implimentazzjoni tagħha. Dik il-proċedura għandha tkopri l-istadji kollha tal-proġetti tal-ICT mill-bidu tagħhom sal-għeluq tagħhom.

2. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jiżviluppaw, jiddokumentaw u jimplimentaw proċedura ta' ġestjoni tat-tibdil fl-ICT biex jiżguraw li t-tibdiliet kollha fis-sistemi tal-ICT jiġu rreġistrati, ittestjati, ivvalutati, approvati, implimentati u vverifikat b'mod ikkontrollat u bis-salvagwardji adegwati biex tiġi ppreżervata r-reżiljenza operazzjonali diġitali tal-entità finanzjarja.

KAPITOLU III

Ġestjoni tal-kontinwità tal-operat tal-ICT

Artikolu 39

Komponenti tal-pjan ta' kontinwità tal-operat tal-ICT

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jiżviluppaw il-pjanijiet ta' kontinwità tal-operat tal-ICT tagħhom filwaqt li jqisu r-riżultati tal-analiżi tal-iskoperturi tagħhom għal interruzzjonijiet u xenarji kummerċjali severi, u l-impatt potenzjali tagħhom, li għalihom jistgħu jkunu esposti l-assi tal-ICT tagħhom li jappoġġaw funzjonijiet kritiċi jew importanti, inkluż xenarju ta' attakk ċibernetiku.

2. Il-pjanijiet ta' kontinwità tal-operat tal-ICT imsemmija fil-paragrafu 1 għandhom:

(a) ikunu approvati mill-korp maniġerjali tal-entità finanzjarja;

(b) ikunu ddokumentati u faċilment aċċessibbli fil-każ ta' emerġenza jew kriżi;

(c) jallokaw riżorsi suffiċjenti għall-eżekuzzjoni tagħhom;

(d) jistabbilixxu livelli ta' rkupru ppjanati u perjodi ta' żmien għall-irkupru u t-tkomplija tal-funzjonijiet u d-dipendenzi interni u esterni ewlenin, inklużi fornituri terzi ta' servizzi tal-ICT;

(e) jidentifikaw il-kundizzjonijiet li jistgħu jwasslu għall-attivazzjoni tal-pjanijiet ta' kontinwità tal-operat tal-ICT u x'azzjonijiet għandhom jittieħdu biex jiġu żgurati d-disponibbiltà, il-kontinwità u l-irkupru tal-assi tal-ICT tal-entitajiet finanzjarji li jappoġġaw funzjonijiet kritiċi jew importanti;

(f) jidentifikaw il-miżuri ta' restawr u ta' rkupru għal funzjonijiet kummerċjali kritiċi jew importanti, proċessi ta' appoġġ, assi ta' informazzjoni u l-interdipendenzi tagħhom biex jiġu evitati effetti negattivi fuq il-funzjonament tal-entitajiet finanzjarji;

(g) jidentifikaw proċeduri u miżuri dwar il-backup li jispeċifikaw l-ambitu tad-*data* li tkun soġġetta għall-backup, u l-frekwenza minima tal-backup, abbażi tal-kritikalità tal-informazzjoni jew tas-sensittività tad-*data;*

(h) iqisu għażliet alternattivi fejn l-irkupru jista' ma jkunx fattibbli fuq perjodu ta' żmien qasir minħabba kostijiet, riskji, loġistika jew ċirkostanzi mhux previsti;

(i) jispeċifikaw l-arranġamenti ta' komunikazzjoni interni u esterni, inklużi l-pjanijiet ta' eskalazzjoni;

(j) ikunu aġġornati f'konformità mat-tagħlimiet meħuda minn inċidenti, testijiet, riskji ġodda u theddid identifikat, objettivi ta' rkupru mibdula, tibdiliet kbar fl-organizzazzjoni tal-entità finanzjarja u fl-assi tal-ICT li jappoġġaw funzjonijiet kritiċi jew kummerċjali.

Għall-finijiet tal-punt (f), il-miżuri msemmija f'dak il-punt għandhom jipprevedu l-mitigazzjoni tan-nuqqasijiet ta' fornituri terzi kritiċi.

Artikolu 40

Ittestjar tal-pjanijiet ta' kontinwità tal-operat

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jittestjaw il-pjanijiet ta' kontinwità tal-operat tagħhom imsemmija fl-Artikolu 39 ta' dan ir-Regolament, inklużi x-xenarji msemmija f'dak l-Artikolu, mill-anqas darba fis-sena għall-proċeduri ta' backup u ta' restawr, jew ma' kull tibdil kbir fil-pjan ta' kontinwità tal-operat.

2. L-ittestjar tal-pjanijiet ta' kontinwità tal-operat imsemmija fil-paragrafu 1 għandu juri li l-entitajiet finanzjarji msemmija f'dak il-paragrafu jistgħu jsostnu l-vijabbiltà tan-negozji tagħhom sakemm l-operazzjonijiet kritiċi jiġu stabbiliti mill-ġdid u jidentifikaw kwalunkwe nuqqas f'dawk il-pjanijiet.

3. L-entitajiet finanzjarji msemmija fil-paragrafu 1 għandhom jiddokumentaw ir-riżultati tal-ittestjar tal-pjanijiet ta' kontinwità tal-operat u kwalunkwe nuqqas identifikat li jirriżulta minn dak l-ittestjar għandu jiġi analizzat, indirizzat u rrapportat lill-korp maniġerjali.

KAPITOLU IV

Rapport dwar ir-rieżami tal-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT

Artikolu 41

Format u kontenut tar-rapport dwar ir-rieżami tal-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT

1. L-entitajiet finanzjarji msemmija fl-Artikolu 16(1) tar-Regolament (UE) 2022/2554 għandhom jippreżentaw ir-rapport dwar ir-rieżami tal-qafas tal-ġestjoni tar-riskju tal-ICT imsemmi fil-paragrafu 2 ta' dak l-Artikolu f'format elettroniku li jippermetti t-tiftix.

2. Ir-rapport imsemmi fil-paragrafu 1 għandu jinkludi l-informazzjoni kollha li ġejja:

(a) taqsima introduttorja li tipprovdi:

(i) deskrizzjoni tal-kuntest tar-rapport f'termini tan-natura, tal-iskala u tal-kumplessità tas-servizzi, tal-attivitajiet u tal-operazzjonijiet tal-entità finanzjarja, l-organizzazzjoni tal-entità finanzjarja, il-funzjonijiet kritiċi identifikati, l-istrateġija, il-proġetti jew l-attivitajiet ewlenin li għaddejjin, u r-relazzjonijiet, u d-dipendenza tal-entità finanzjarja fuq servizzi u sistemi tal-ICT interni u esternalizzati, jew l-implikazzjonijiet li telf totali jew degradazzjoni severa ta' dawn is-sistemi jkollhom fuq funzjonijiet kritiċi jew importanti u fuq l-effiċjenza tas-suq;

(ii) sommarju fil-livell eżekuttiv tar-riskju kurrenti u qrib it-terminu tal-ICT identifikat, ix-xenarju tat-theddid, l-effettività vvalutata tal-kontrolli tiegħu u l-pożizzjoni tas-sigurtà tal-entità finanzjarja;

(iii) informazzjoni dwar iż-żona rrapportata;

(iv) sommarju tat-tibdiliet ewlenin fil-qafas tal-ġestjoni tar-riskju tal-ICT mir-rapport preċedenti;

(v) sommarju u deskrizzjoni tal-impatt ta' tibdiliet kbar fil-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT mir-rapport preċedenti;

(b) meta applikabbli, id-data tal-approvazzjoni tar-rapport mill-korp maniġerjali tal-entità finanzjarja;

(c) deskrizzjoni tar-raġunijiet għar-rieżami, inklużi:

(i) meta r-rieżami jkun inbeda wara struzzjonijiet superviżorji, evidenza ta' dawn l-istruzzjonijiet;

(ii) meta r-rieżami jkun ingħata bidu wara l-okkorrenza ta' inċidenti relatati mal-ICT, il-lista ta' dawk l-inċidenti kollha relatati mal-ICT b'analiżi tal-kawżi ewlenin relatati mal-inċidenti;

(d) id-data tal-bidu u tat-tmiem tal-perjodu ta' rieżami;

(e) il-persuna responsabbli għar-rieżami;

(f) sommarju tas-sejbiet, u awtovalutazzjoni tas-severità tad-dgħufijiet, tan-nuqqasijiet u tal-lakuni identifikati fil-qafas tal-ġestjoni tar-riskju tal-ICT għall-perjodu ta' rieżami, inkluża analiżi ddettaljata tagħhom;

(g) miżuri ta' rimedju identifikati biex jiġu indirizzati dgħufijiet, nuqqasijiet u lakuni fil-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT, u d-data mistennija għall-implimentazzjoni ta' dawk il-miżuri, inkluż is-segwitu dwar id-dgħufijiet, in-nuqqasijiet u l-lakuni identifikati f'rapporti preċedenti, fejn dawk id-dgħufijiet, in-nuqqasijiet u n-nuqqasijiet għadhom ma ġewx irrimedjati;

(h) konklużjonijiet ġenerali dwar ir-rieżami tal-qafas issimplifikat tal-ġestjoni tar-riskju tal-ICT, inkluż kwalunkwe żvilupp ippjanat ieħor.

TITOLU IV

DISPOŻIZZJONIJIET FINALI

Artikolu 42

Dħul fis-seħħ

Dan ir-Regolament għandu jidħol fis-seħħ fl-għoxrin jum wara dak tal-pubblikazzjoni tiegħu f'*Il-Ġurnal Uffiċjali tal-Unjoni Ewropea*.

Dan ir-Regolament għandu jorbot fl-intier tiegħu u japplika direttament fl-Istati Membri kollha.

Magħmul fi Brussell, it-13 ta' Marzu 2024.

Għall-Kummissjoni
Il-President
Ursula VON DER LEYEN