Usmernenia

EBA/GL/2019/04

28. novembra 2019

Usmernenia EBA k riadeniu rizík v oblasti IKT a bezpečnosti

Povinnosti týkajúce sa dodržiavania súladu s predpismi a ohlasovacia povinnosť

Status týchto usmernení

1. Tento dokument obsahuje usmernenia vydané podľa článku 16 nariadenia (EÚ) č. 1093/2010[1]. Podľa článku 16 ods. 3 nariadenia (EÚ) č. 1093/2010 príslušné orgány a finančné inštitúcie musia vynaložiť všetko úsilie na dodržanie týchto usmernení.

2. V týchto usmerneniach sa uvádza stanovisko Európskeho orgánu pre bankovníctvo (EBA) k náležitým postupom dohľadu v rámci Európskeho systému finančného dohľadu alebo k spôsobu, akým sa má uplatňovať právo Európskej únie v konkrétnej oblasti. Príslušné orgány, ako sú vymedzené v článku 4 ods. 2 nariadenia (EÚ) č. 1093/2010 a na ktoré sa tieto usmernenia vzťahujú, by ich mali dodržiavať tak, že ich začlenia do svojich postupov dohľadu podľa potreby (napr. zmenou svojho právneho rámca alebo postupov dohľadu), a to aj v prípade, keď sú usmernenia určené predovšetkým inštitúciám.

Požiadavky na predkladanie správ

3. Podľa článku 16 ods. 3 nariadenia (EÚ) č. 1093/2010 musia príslušné orgány oznámiť EBA, či tieto usmernenia dodržiavajú alebo majú v úmysle dodržať, alebo v opačnom prípade musia uviesť dôvody ich nedodržania do ([dd. mm. rrrr]). Ak do tohto dátumu nebude doručené žiadne oznámenie, EBA sa bude domnievať, že ich príslušné orgány nedodržiavajú. Oznámenia sa majú zaslať prostredníctvom formulára dostupného na webovom sídle EBA na adresu compliance@eba.europa.eu s referenčným číslom „EBA/GL/2019/04“. Oznámenia majú predkladať osoby, ktoré sú oprávnené podávať správy o dodržiavaní usmernení v mene svojich príslušných orgánov. Akúkoľvek zmenu stavu dodržiavania usmernení treba takisto oznámiť orgánu EBA.

4. Oznámenia budú uverejnené na webovom sídle EBA v súlade s článkom 16 ods. 3.

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12).

Predmet úpravy, rozsah pôsobnosti a vymedzenie pojmov

Predmet úpravy

5. Tieto usmernenia sú založené na ustanoveniach článku 74 smernice 2013/36/EÚ (CRD) o vnútornej správe a riadení spoločnosti a sú odvodené od mandátu vydávať usmernenia, uvedeného v článku 95 ods. 3 smernice (EÚ) 2015/2366 (druhá smernica o platobných službách).

6. V týchto usmerneniach sú stanovené opatrenia v oblasti riadenia rizík, ktoré musia prijať finančné inštitúcie (vymedzené ďalej v odseku 9) v súlade s článkom 74 CRD, aby riadili svoje riziká v oblasti IKT a bezpečnosti pre všetky činnosti, a ktoré musia prijať poskytovatelia platobných služieb (PPS podľa vymedzenia ďalej v odseku 9) v súlade s článkom 95 ods. 1 druhej smernice o platobných službách, aby riadili prevádzkové a bezpečnostné riziká (zamýšľané ako „riziká v oblasti IKT a bezpečnosti“) v súvislosti s platobnými službami, ktoré poskytujú. Usmernenia zahŕňajú požiadavky na informačnú bezpečnosť vrátane kybernetickej bezpečnosti v takom rozsahu, v akom sú informácie uchovávané v IKT systémoch.

Rozsah pôsobnosti

7. Tieto usmernenia sa uplatňujú vo vzťahu k riadeniu rizík v oblasti IKT a bezpečnosti v rámci finančných inštitúcií (ako sú vymedzené v odseku 9). Na účely týchto usmernení sa pojem riziká v oblasti IKT a bezpečnosti týka prevádzkových a bezpečnostných rizík uvedených v článku 95 druhej smernice o platobných službách, pokiaľ ide o poskytovanie platobných služieb.

8. V prípade poskytovateľov platobných služieb (vymedzených v odseku 9) sa tieto usmernenia uplatňujú na ich poskytovanie platobných služieb, v súlade s rozsahom pôsobnosti a mandátu článku 95 druhej smernice o platobných službách. V prípade inštitúcií (vymedzených v odseku 9) sa tieto usmernenia uplatňujú na všetky činnosti, ktoré poskytujú.

Adresáti

9. Tieto usmernenia sú určené finančným inštitúciám, ktoré sú na účely týchto usmernení 1. poskytovatelia platobných služieb vymedzení v článku 4 ods. 11 druhej smernice o platobných službách, a 2. inštitúciám, t. j. úverovým inštitúciám a investičným spoločnostiam podľa vymedzenia v článku 4 ods. 1 bode 3 nariadenia (EÚ) č. 575/2013. Tieto usmernenia sa vzťahujú aj na príslušné orgány podľa vymedzenia v článku 4 ods. 1 bode 40 nariadenia (EÚ) č. 575/2013 vrátane Európskej centrálnej banky, pokiaľ ide o záležitosti súvisiace s úlohami, ktorými bola poverená na základe nariadenia (EÚ) č. 1024/2013, a na príslušné orgány podľa druhej smernice o platobných službách, ako sa uvádza v článku 4 ods. 2 bode i) nariadenia (EÚ) č. 1093/2010.

Vymedzenie pojmov

10. Pokiaľ nie je uvedené inak, pojmy použité a vymedzené v smernici 2013/36/EÚ (CRD), v nariadení (EÚ) č. 575/2013 (CRR) a v smernici (EÚ) 2015/2366 (druhej smernici o platobných službách) majú v týchto usmerneniach rovnaký význam. Na účely týchto usmernení sa okrem toho uplatňuje toto vymedzenie pojmov:

Riziko v oblasti IKT a bezpečnosti	Riziko strát z dôvodu porušenia dôvernosti, zlyhania integrity systémov a údajov, nevhodnosti alebo nedostupnosti systémov a údajov alebo neschopnosti v primeranom čase a za primerané náklady zmeniť informačné technológie (IT) v prípade zmeny environmentálnych alebo obchodných požiadaviek (t. j. agilita)[2]. Zahŕňa bezpečnostné riziká vyplývajúce z neprimeraných alebo zlyhaných interných postupov alebo externých udalostí vrátane kybernetických útokov alebo neprimeranej fyzickej bezpečnosti.
Riadiaci orgán	(a) V prípade úverových inštitúcií a investičných spoločností má tento pojem rovnaký význam ako vymedzenie pojmu v článku 3 ods. 1 bode 7 smernice 2013/36/EÚ. (b) V prípade platobných inštitúcií alebo inštitúcií elektronických peňazí sa pod týmto pojmom rozumejú členovia predstavenstva alebo osoby zodpovedné za riadenie platobných inštitúcií alebo inštitúcií elektronických peňazí a v relevantných prípadoch aj osoby zodpovedné za riadenie činností súvisiacich s platobnými službami platobných inštitúcií a inštitúcií elektronických peňazí. (c) V prípade poskytovateľov platobných služieb uvedených v článku 1 ods. 1 písm. c), e) a f) smernice (EÚ) 2015/2366 má tento pojem význam, ktorý mu priznáva platné právo Únie alebo vnútroštátne právo.
Prevádzkový alebo bezpečnostný incident	Jednorazová udalosť alebo rad navzájom súvisiacich udalostí, ktoré finančná inštitúcia neplánovala a ktoré majú alebo pravdepodobne budú mať nepriaznivý vplyv na integritu, dostupnosť, dôvernosť a/alebo autentickosť služieb.
Vrcholový manažment	(a) V prípade úverových inštitúcií a investičných spoločností má tento pojem rovnaký význam ako vymedzenie pojmu v článku 3 ods. 1 bode 9 smernice 2013/36/EÚ. (b) V prípade platobných inštitúcií a inštitúcií elektronických peňazí sa pod týmto pojmom rozumejú fyzické osoby, ktoré vykonávajú výkonné funkcie v rámci inštitúcie a ktoré sa

[2] Vymedzenie z Usmernení EBA o spoločných postupoch a metodikách postupu preskúmania a hodnotenia orgánmi dohľadu z 19. decembra 2014 (EBA/GL/2014/13), zmenených EBA/GL/2018/03.

	zodpovedajú riadiacemu orgánu za každodenné riadenie inštitúcie. (c) V prípade poskytovateľov platobných služieb uvedených v článku 1 ods. 1 písm. c), e) a f) smernice (EÚ) 2015/2366 má tento pojem význam, ktorý mu priznáva platné právo Únie alebo vnútroštátne právo.
Ochota podstupovať riziká	Súhrnná úroveň a typy rizika, ktoré sú poskytovatelia platobných služieb a inštitúcie ochotné prevziať v rámci svojej schopnosti znášať riziko v súlade so svojím obchodným modelom, aby dosiahli svoje strategické ciele.
Funkcia auditu	(a) V prípade úverových inštitúcií a investičných spoločností je funkcia auditu taká, ako je uvedené v oddiele 22 Usmernení EBA o vnútornom riadení (EBA/GL/2017/11). (b) V prípade iných poskytovateľov platobných služieb než úverové inštitúcie musí byť funkcia auditu nezávislá v rámci poskytovateľa platobných služieb alebo od neho a môže ísť o funkciu vnútorného a/alebo externého auditu.
Projekty IKT	Každý projekt alebo jeho časť, v ktorom sa menia, nahrádzajú, odstavujú alebo zavádzajú IKT systémy a služby. Projekty IKT môžu byť súčasťou všeobecnejších programov IKT alebo transformácie činnosti.
Tretia strana	Organizácia, ktorá vstúpila do obchodných vzťahov alebo uzavrela zmluvy so subjektom o poskytovaní produktu alebo služby[3].
Informačné aktívum	Súbor informácií, hmotný či nehmotný, ktorý je hodný ochrany.
IKT aktívum	Aktívum vo forme softvéru alebo hardvéru, ktoré sa nachádza v podnikateľskom prostredí.
IKT systémy[4]	IKT štruktúra ako súčasť mechanizmu alebo prepájacia sieť, ktorá slúži na podporu operácií finančnej inštitúcie.
IKT služby[5]	Služby poskytované IKT systémami jednému alebo viacerým interným alebo externým používateľom. Príkladmi sú služby týkajúce sa zadávania údajov, ich archivácie, spracovania a služby týkajúce sa vykazovania, ale aj monitorovacie služby a služby na podporu obchodovania a rozhodovania.

[3] Vymedzenie z G7 základných prvkov pre riadenie kybernetického rizika tretej strany vo finančnom sektore.
[4] Vymedzenie z Usmernení pre posudzovanie rizika súvisiaceho s informačnými a komunikačnými technológiami v rámci postupu preskúmania a hodnotenia orgánmi dohľadu (SREP) (EBA/GL/ 2017/05).
[5] tamže.

Vykonávanie

Dátum začiatku uplatňovania

11. Tieto usmernenia sa uplatňujú od 30. júna 2020.

Zrušenie

12. Usmernenia k bezpečnostným opatreniam vzťahujúcim sa na prevádzkové a bezpečnostné riziká (EBA/GL/2017/17) vydané v roku 2017 budú zrušené týmito usmerneniami k dátumu, kedy sa začnú uplatňovať tieto usmernenia.

Usmernenia o riadení rizík v oblasti IKT a bezpečnosti

1.1. Proporcionalita

1. Všetky finančné inštitúcie by mali dodržiavať ustanovenia stanovené v týchto usmerneniach takým spôsobom, ktorý je primeraný a v ktorom je zohľadnená veľkosť finančných inštitúcií, ich interná organizácia a povaha, rozsah, zložitosť a rizikovosť služieb a produktov, ktoré finančné inštitúcie poskytujú alebo zamýšľajú poskytovať.

1.2. Správa a stratégia

1.2.1. Správa

2. Riadiaci orgán by mal zabezpečiť, aby finančné inštitúcie mali primeranú vnútornú správu a rámec vnútornej kontroly, pokiaľ ide o ich riziká v oblasti IKT a bezpečnosti. Riadiaci orgán by mal stanoviť jasné úlohy a povinnosti pre IKT funkcie, riadenie rizík v oblasti informačnej bezpečnosti a kontinuity činnosti vrátane úloh a povinností riadiaceho orgánu a jeho výborov.
3. Riadiaci orgán by mal zabezpečiť, aby kvalita a zručnosti zamestnancov finančných inštitúcií boli primerané na podporu ich prevádzkových IKT potrieb a ich postupov riadenia rizík v oblasti IKT a bezpečnosti na priebežnom základe a zabezpečenie vykonávania stratégie v oblasti IKT. Riadiaci orgán by mal zabezpečiť, aby bol pridelený rozpočet primeraný na splnenie uvedených úloh. Okrem toho by finančné inštitúcie mali zabezpečiť, aby všetci zamestnanci vrátane držiteľov kľúčových funkcií na ročnom základe alebo v prípade potreby častejšie získavali primeranú odbornú prípravu o rizikách v oblasti IKT a bezpečnosti vrátane informačnej bezpečnosti (pozri tiež oddiel 1.4.7).

4. Riadiaci orgán nesie celkovú zodpovednosť za stanovenie, schválenie a dohľad nad vykonávaním stratégie v oblasti IKT finančných inštitúcií v rámci svojej celkovej obchodnej stratégie, ako aj za vytvorenie účinného rámca pre riadenie rizík pre riziká v oblasti IKT a bezpečnosti.

1.2.2. Stratégia

5. Stratégia v oblasti IKT by mala byť zladená s celkovou obchodnou stratégiou finančných inštitúcií a malo by v nej byť vymedzené:
    a) ako by sa mali vyvíjať IKT finančných inštitúcií, aby účinne podporovali ich obchodnú stratégiu a podieľali sa na nej vrátane vývoja organizačnej štruktúry, zmien IKT systémov a kľúčových prípadov závislosti od tretích strán;
    b) plánovaná stratégia a vývoj architektúry IKT vrátane prípadov závislostí od tretích strán;
    c) jasné ciele informačnej bezpečnosti so zameraním na IKT systémy a IKT služby, zamestnancov a postupy.

6. Finančné inštitúcie by mali vytvoriť súbory akčných plánov s opatreniami, ktoré treba prijať na dosiahnutie cieľa stratégie v oblasti IKT. O týchto súboroch by mali byť informovaní všetci relevantní zamestnanci (vrátane zmluvných dodávateľov a poskytovateľov, ktorí sú tretími stranami, ak je to vhodné a relevantné). Akčné plány by sa mali pravidelne preskúmať v záujme zabezpečenia ich relevantnosti a vhodnosti. Finančné inštitúcie by takisto mali stanoviť postupy na monitorovanie a meranie účinnosti vykonávania svojej stratégie v oblasti IKT.

1.2.3. Používanie poskytovateľov, ktorí sú tretími stranami

7. Bez toho, aby boli dotknuté Usmernenia EBA k outsourcingu (EBA/GL/2019/02) a článok 19 druhej smernice o platobných službách, by finančné inštitúcie mali zabezpečiť účinnosť opatrení na zmiernenie rizika, ako sú vymedzené v ich rámci pre riadenie rizík vrátane opatrení stanovených v týchto usmerneniach pri outsourcingu prevádzkových funkcií platobných služieb a/alebo IKT služieb a IKT systémov akejkoľvek činnosti, a to aj subjektom v skupine, alebo pri využívaní tretích strán.

8. S cieľom zabezpečiť kontinuitu IKT služieb a IKT systémov by finančné inštitúcie mali zabezpečiť, aby zmluvy a dohody o úrovni poskytovania služieb (a to za normálnych okolností, ako aj v prípade prerušenia služby – pozri tiež oddiel 1.7.2) s poskytovateľmi (poskytovatelia externého zabezpečovania činností, subjekty v skupine alebo poskytovatelia, ktorí sú tretími stranami) zahŕňali:
    a) vhodné a primerané ciele a opatrenia súvisiace s informačnou bezpečnosťou vrátane požiadaviek, ako sú minimálne požiadavky na kybernetickú bezpečnosť; špecifikácie životného cyklu údajov finančnej inštitúcie; akékoľvek požiadavky týkajúce sa postupov šifrovania údajov, bezpečnosti siete a monitorovania bezpečnosti a umiestnenia dátových centier;
    b) postupy na riešenie prevádzkových a bezpečnostných incidentov vrátane postúpenia nadriadeným a podávania správ.

9. Finančné inštitúcie by mali monitorovať a overovať, či títo poskytovatelia zaisťujú správnu úroveň bezpečnostných cieľov, bezpečnostných opatrení a výkonnostných cieľov finančnej inštitúcie.

1.3. Rámec pre riadenie rizík v oblasti IKT a bezpečnosti

1.3.1. Organizácia a ciele

10. Finančné inštitúcie by mali identifikovať a riadiť svoje riziká v oblasti IKT a bezpečnosti. IKT funkcia(-e) zodpovedná(-é) za IKT systémy, postupy a bezpečnostné operácie by mala(-i) mať zavedené vhodné postupy a kontroly na zabezpečenie toho, aby boli všetky riziká identifikované, analyzované, merané, monitorované, riadené, nahlásené a udržiavané v rámci obmedzení ochoty finančnej inštitúcie podstupovať riziká, a aby projekty a systémy, ktoré dodávajú, a činnosti, ktoré vykonávajú, boli v súlade s externými a internými požiadavkami.

11. Finančné inštitúcie by mali prideliť zodpovednosť za riadenie rizík v oblasti IKT a bezpečnosti a dohľad nad nimi kontrolnej funkcii a dodržiavať pritom požiadavky oddielu 19 Usmernení EBA o vnútornom riadení (EBA/GL/2017/11). Finančné inštitúcie by mali zabezpečiť nezávislosť a objektivitu tejto kontrolnej funkcie jej náležitým odčlenením od postupov prevádzok IKT. Táto kontrolná funkcia by sa mala zodpovedať priamo riadiacemu orgánu a mala by byť zodpovedná za monitorovanie a kontrolu dodržiavania rámca pre riadenie rizík v oblasti IKT a bezpečnosti. Mala by zabezpečiť, aby riziká v oblasti IKT a bezpečnosti boli identifikované, merané, posúdené, riadené, monitorované a nahlasované. Finančné inštitúcie by mali zabezpečiť, aby táto kontrolná funkcia nebola zodpovedná za vnútorný audit.

    Funkcia vnútorného auditu by sa mala riadiť prístupom založeným na rizikách a mať kapacitu na nezávislé preskúmanie a poskytnutie objektívneho uistenia o tom, že všetky činnosti a útvary finančnej spoločnosti súvisiace s IKT a bezpečnosťou sú v súlade s politikami a postupmi finančnej inštitúcie a s externými požiadavkami a dodržiavajú sa pritom požiadavky oddielu 22 Usmernení EBA o vnútornom riadení (EBA/GL/2017/11).

12. Finančné inštitúcie by mali vymedziť a prideliť kľúčové úlohy a zodpovednosti a príslušné hierarchické vzťahy v záujme toho, aby bol rámec pre riadenie rizík v oblasti IKT a bezpečnosti účinný. Tento rámec by mal byť úplne začlenený do postupov celkového riadenia rizík finančnej inštitúcie a mal by byť s nimi zosúladený.

13. Rámec pre riadenie rizík v oblasti IKT a bezpečnosti by mal zahŕňať postupy zavedené s cieľom:

    a) určiť ochotu podstupovať riziká, pokiaľ ide o riziká v oblasti IKT a bezpečnosti, v súlade s ochotou finančnej inštitúcie podstupovať riziká;
    b) určiť a posúdiť riziká v oblasti IKT a bezpečnosti, ktorým je finančná inštitúcia vystavená;
    c) vymedziť opatrenia na zmiernenie vrátane kontrol na zmiernenie rizík v oblasti IKT a bezpečnosti;
    d) monitorovať účinnosť týchto opatrení, ako aj počet nahlásených incidentov, v prípade poskytovateľov platobných služieb vrátane incidentov nahlásených v súlade s článkom 96 druhej smernice o platobných službách, ktoré majú vplyv na činnosti týkajúce sa IKT, a prijať opatrenie na nápravu opatrení v prípade potreby;
    e) podávať správu riadiacemu orgánu o rizikách a kontrolách v oblasti IKT a bezpečnosti;

f) identifikovať a posúdiť, či existujú nejaké riziká v oblasti IKT a bezpečnosti, ktoré vyplývajú z nejakej zásadnej zmeny v IKT systéme alebo IKT službách, postupoch alebo konaniach a/alebo po významnom prevádzkovom alebo bezpečnostnom incidente.

14. Finančné inštitúcie by mali zabezpečiť, aby bol rámec pre riadenie rizík v oblasti IKT a bezpečnosti zaznamenaný a priebežne zlepšovaný na základe poznatkov získaných počas jeho vykonávania a monitorovania. Rámec pre riadenie rizík v oblasti IKT a bezpečnosti by mal schvaľovať a aspoň raz ročne preskúmať riadiaci orgán.

1.3.2. Identifikácia funkcií, postupov a aktív

15. Finančné inštitúcie by mali identifikovať, stanoviť a udržiavať aktuálne mapovanie svojich obchodných funkcií, úloh a podporných procesov s cieľom určiť dôležitosť každého z nich a ich vzájomné závislosti v súvislosti s rizikami v oblasti IKT a bezpečnosti.

16. Okrem toho by finančné inštitúcie mali identifikovať, stanoviť a udržiavať aktuálne mapovanie informačných aktív podporujúcich ich obchodné funkcie a podporné procesy, ako sú IKT systémy, zamestnanci, dodávatelia, tretie strany a závislosti na iných interných a externých systémoch a procesoch, aby boli schopné riadiť minimálne tie informačné aktíva, ktoré podporujú ich kritické obchodné funkcie a procesy.

1.3.3. Klasifikácia a posúdenie rizík

17. Finančné inštitúcie by mali klasifikovať identifikované obchodné funkcie, podporné procesy a informačné aktíva uvedené v odsekoch 15 a 16 z hľadiska kritickej povahy.

18. Na vymedzenie kritickej povahy týchto identifikovaných obchodných funkcií, podporných procesov a informačných aktív by finančné inštitúcie mali zvážiť aspoň požiadavky na dôvernosť, integritu a dostupnosť. Za informačné aktíva by mala byť jasne pridelená povinnosť zodpovedať sa a zodpovednosť.

19. Finančné inštitúcie by mali preskúmať primeranosť klasifikácie informačných aktív a príslušnej dokumentácie pri vykonávaní posúdenia rizík.

20. Finančné inštitúcie by mali identifikovať riziká v oblasti IKT a bezpečnosti, ktoré majú vplyv na identifikované a klasifikované obchodné funkcie, podporné procesy a informačné aktíva v závislosti od ich kritickej povahy. Toto posúdenie rizík by sa malo vykonávať a zaznamenávať ročne alebo v kratších intervaloch v prípade potreby. Tieto posúdenia rizík by sa mali takisto vykonávať v prípade akýchkoľvek zásadných zmien v infraštruktúre, procesoch alebo postupoch, ktoré majú vplyv na obchodné funkcie, podporné procesy alebo informačné aktíva a v dôsledku toho by sa malo aktualizovať aktuálne posúdenie rizík finančných inštitúcií.

21. Finančné inštitúcie by mali zabezpečiť, aby sústavne monitorovali hrozby a zraniteľné stránky relevantné pre ich obchodné procesy, podporné funkcie a informačné aktíva a mali by pravidelne preskúmať rizikové scenáre, ktoré na ne majú vplyv.

1.3.4. Zmiernenie rizík

22. Na základe posúdení rizík by finančné inštitúcie mali určiť, ktoré opatrenia sú potrebné na zmiernenie identifikovaných rizík v oblasti IKT a bezpečnosti na prijateľné úrovne a či sú potrebné zmeny existujúcich obchodných procesov, kontrolných opatrení, IKT systémov a IKT služieb. Finančná inštitúcia by mala zvážiť čas potrebný na zavedenie týchto zmien a čas na prijatie vhodných predbežných opatrení na zmierenie, aby sa minimalizovali riziká v oblasti IKT a bezpečnosti tak, aby zostali v rámci ochoty finančnej inštitúcie podstupovať riziká v oblasti IKT a bezpečnosti.
23. Finančné inštitúcie by mali vymedziť a zaviesť opatrenia na zmiernenie identifikovaných rizík v oblasti IKT a bezpečnosti a na ochranu informačných aktív v súlade s ich klasifikáciou.

1.3.5. Podávanie správ

24. Finančné inštitúcie by mali jasne a včas informovať riadiaci orgán o výsledkoch posúdenia rizík. Týmto informovaním nie je dotknutá povinnosť poskytovateľa platobných služieb poskytnúť príslušným orgánom aktuálne a komplexné posúdenie rizík, ako je stanovené v článku 95 ods. 2 smernice (EÚ) 2015/2366.

1.3.6. Audit

25. Správa, systémy a procesy finančnej inštitúcie pre jej riziká v oblasti IKT a bezpečnosti by mali na pravidelnom základe podliehať auditu audítormi s dostatočnými vedomosťami, zručnosťami a odbornými znalosťami o rizikách v oblasti IKT a bezpečnosti a platbách (v prípade poskytovateľov platobných služieb), aby riadiacemu orgánu poskytli nezávislé uistenie o ich účinnosti. Audítori by mali byť nezávislí v rámci finančnej inštitúcie alebo od nej. Periodicita a zameranie týchto auditov by malo byť primerané príslušným rizikám v oblasti IKT a bezpečnosti.
26. Riadiaci orgán finančnej inštitúcie by mal schváliť plán auditu vrátane akýchkoľvek auditov IKT a ich akýchkoľvek podstatných úprav. Plán auditu a jeho vykonávanie vrátane periodicity auditu by mali zohľadňovať vlastné riziká v oblasti IKT a bezpečnosti vo finančnej inštitúcii a mali by im byť úmerné a pravidelne aktualizované.
27. Mal by sa stanoviť formálny nadväzujúci proces vrátane ustanovení na včasné overenie a opravu kritických zistení z IKT auditu.

1.4. Informačná bezpečnosť

1.4.1. Politika informačnej bezpečnosti

28. Finančné inštitúcie by mali vypracovať a zaznamenať politiku informačnej bezpečnosti, v ktorej by sa mali vymedziť zásady a pravidlá na vysokej úrovni na ochranu dôvernosti, integrity a dostupnosti údajov a informácií finančných inštitúcií a ich klientov. V prípade poskytovateľov platobných služieb je táto politika identifikovaná v dokumente o bezpečnostnej politike, ktorý sa prijme v súlade s článkom 5 ods. 1 písm. j) smernice (EÚ) 2015/2366. Politika informačnej

bezpečnosti by mala byť v súlade s cieľmi finančnej inštitúcie v oblasti informačnej bezpečnosti založená na príslušných výsledkoch postupu posúdenia rizík. Túto politiku by mal schvaľovať riadiaci orgán.

29. Táto politika by mala obsahovať opis hlavných úloh a povinností riadenia informačnej bezpečnosti a mali by v nej byť stanovené požiadavky pre zamestnancov a dodávateľov, procesy a technológiu v súvislosti s informačnou bezpečnosťou so zohľadnením toho, že zamestnanci a dodávatelia na všetkých úrovniach majú povinnosti v zabezpečovaní informačnej bezpečnosti finančných inštitúcií. Táto politika by mala zabezpečiť dôvernosť, integritu a dostupnosť kritických logických a fyzických aktív, zdrojov a citlivých údajov finančnej inštitúcie, či už sú tieto údaje v pokoji, v tranzite alebo sa používajú. O politike informačnej bezpečnosti by mali byť informovaní všetci zamestnanci a dodávatelia finančnej inštitúcie.

30. Na základe politiky informačnej bezpečnosti by finančné inštitúcie mali stanoviť a vykonávať bezpečnostné opatrenia na zmiernenie rizík v oblasti IKT a bezpečnosti, ktorým sú vystavené. Tieto opatrenia by mali obsahovať:

    a) organizáciu a riadenie v súlade s odsekmi 10 a 11;
    b) logickú bezpečnosť (oddiel 1.4.2);
    c) fyzickú bezpečnosť (oddiel 1.4.3);
    d) bezpečnosť prevádzok IKT (oddiel 1.4.4);
    e) monitorovanie bezpečnosti (oddiel 1.4.5);
    f) preskúmania, posúdenie a testovanie informačnej bezpečnosti (oddiel 1.4.6);
    g) odbornú prípravu a informovanosť v oblasti informačnej bezpečnosti (oddiel 1.4.7).

1.4.2. Logická bezpečnosť

31. Finančné inštitúcie by mali vymedziť, zaznamenať a zaviesť postupy na kontrolu logického prístupu (riadenie identity a prístupu). Tieto postupy by mali byť zavedené, presadzované, monitorované a pravidelne preskúmané. Tieto postupy by mali zahŕňať aj kontroly na monitorovanie anomálií. V týchto postupoch by sa mali zavádzať minimálne nasledujúce prvky, pričom pojem používateľ zahŕňa aj technických používateľov:

    (a) **Potreba poznať, minimálne práva a deľba povinností:** finančné inštitúcie by mali riadiť prístupové práva k informačným aktívam a ich podporným systémom na základe potreby poznať, a to aj v prípade vzdialeného prístupu. Používateľom by mali byť udelené minimálne prístupové práva, ktoré sú prísne nevyhnutné na vykonávanie ich povinností (zásada minimálnych práv), t. j. aby sa zabránilo neodôvodnenému prístupu k veľkému súboru údajov alebo aby sa zabránilo prideleniu kombinácií prístupových práv, ktoré je možné využiť na obchádzanie kontrol (zásada deľby povinností).
    (b) **Zodpovednosť používateľa:** finančné inštitúcie by mali v čo najväčšej miere obmedzovať používanie generických a spoločných používateľských účtov a zabezpečiť, aby mohli byť používatelia identifikovaní so zreteľom na akcie vykonané v IKT systémoch.
    (c) **Práva privilegovaného prístupu:** finančné inštitúcie by mali uplatňovať silné kontroly nad privilegovaným prístupom do systémov prísnym obmedzovaním a dôsledným dohľadom nad účtami so zvýšenými oprávneniami na prístup do systémov (napr. kontá správcu). S cieľom zabezpečiť bezpečnú komunikáciu a znížiť riziko by sa mal

správcovský prístup na diaľku ku kritickým IKT systémom poskytovať iba na základe potreby poznať a pri použití riešení prísneho overenia.

(d) **Zaznamenávanie aktivít používateľa:** mali by sa zaznamenávať a monitorovať minimálne všetky aktivity privilegovaných používateľov. Záznamy o prístupe by mali byť zabezpečené, aby sa zabránilo nepovolenej úprave alebo vymazaniu, a uchovávané počas obdobia zodpovedajúceho kritickosti identifikovaných obchodných činností, podporných procesov a informačných aktív v súlade s oddielom 1.3.3, aby boli dotknuté požiadavky na uchovávanie stanovené v práve Únie a vo vnútroštátnom práve. Finančná inštitúcia by mala tieto informácie použiť na uľahčenie identifikácie a vyšetrovania nezvyčajných činností zistených pri poskytovaní služieb.

(e) **Správa prístupu:** prístupové práva by mali byť udeľované, zrušené alebo zmenené včas, podľa vopred vymedzených tokov práce schvaľovania, ktoré zahŕňajú obchodného vlastníka informácií, ku ktorým sa pristupuje (vlastník informačného aktíva). V prípade ukončenia pracovného pomeru by mali byť prístupové práva ihneď zrušené.

(f) **Recertifikácia prístupu:** prístupové práva by mali byť pravidelne preskúmané s cieľom zabezpečiť, aby používatelia nemali nadmerné privilégiá a aby boli prístupové práva zrušené, ak už nie sú potrebné.

(g) **Metódy overovania:** finančné inštitúcie by mali presadzovať metódy overovania, ktoré sú dostatočne odolné, aby sa primerane a účinne zabezpečilo, že sa dodržiavajú politiky a postupy na kontrolu prístupu. Metódy overovania by mali byť primerané kritickej povahe IKT systémov, informácií alebo postupov, ku ktorým sa uskutočňuje prístup. Toto by malo zahŕňať minimálne zložité heslá alebo silnejšie metódy overovania (napríklad dvojprvkové overovanie) podľa príslušného rizika.

32. Elektronický prístup prostredníctvom aplikácií k údajom a IKT systémom by sa mal obmedziť na minimum, ktoré je potrebné na poskytovanie príslušnej služby.

1.4.3. Fyzická bezpečnosť

33. Mali by byť vymedzené, zaznamenané a vykonávané opatrenia fyzickej bezpečnosti finančných inštitúcií, aby sa chránili ich priestory, dátové centrá a citlivé oblasti pred neoprávneným prístupom a pred nebezpečenstvami prostredia.

34. Fyzický prístup k IKT systémom by sa mal povoliť iba oprávneným osobám. Oprávnenie by sa malo prideliť v súlade s úlohami a povinnosťami jednotlivca a obmedziť na osoby, ktoré sú primerane vyškolené a monitorované. Fyzický prístup by sa mal pravidelne preskúmať s cieľom zaistiť, aby boli prístupové práva, ktoré nie sú nevyhnutné, ihneď zrušené, keď nie sú potrebné.

35. Primerané opatrenia na ochranu pred nebezpečenstvami prostredia by mali byť úmerné dôležitosti budov a kritickej povahe operácií alebo IKT systémov nachádzajúcich sa v týchto budovách.

1.4.4. Bezpečnosť prevádzok IKT

36. Finančné inštitúcie by mali zaviesť postupy, aby predišli výskytu bezpečnostných problémov v IKT systémoch a IKT službách, a mali by minimalizovať ich vplyv na dodávanie IKT služieb. Tieto postupy by mali obsahovať nasledujúce opatrenia:

a) identifikácia možných zraniteľných miest, ktoré by mali byť vyhodnotené a napravené zabezpečením toho, aby bol softvér a mikroprogramové vybavenie aktuálne vrátane softvéru, ktorý finančné inštitúcie poskytujú svojim interným a externým používateľom, využívaním kritických bezpečnostných opráv alebo vykonávaním kompenzačných kontrol;
b) zavedenie zabezpečených konfiguračných základných stavov všetkých sieťových zložiek;
c) zavedenie sieťovej segmentácie, systémov na prevenciu straty údajov a šifrovanie sieťovej prevádzky (v súlade s klasifikáciou údajov);
d) zavedenie ochrany koncových bodov vrátane serverov, pracovných staníc a mobilných zariadení; finančné inštitúcie by mali posúdiť, či koncové body spĺňajú bezpečnostné normy, ktoré vymedzili, predtým, ako sa im udelí prístup do podnikovej siete;
e) zabezpečenie, aby boli zavedené mechanizmy na overovanie integrity softvéru, mikropočítačového vybavenia a údajov;
f) šifrovanie údajov v pokoji a v tranzite (v súlade s klasifikáciou údajov).

37. Okrem toho by finančné inštitúcie mali priebežne určovať, či zmeny v existujúcom prevádzkovom prostredí ovplyvňujú existujúce bezpečnostné opatrenia alebo si vyžadujú prijatie dodatočných opatrení na zmiernenie súvisiacich rizík náležitým spôsobom. Tieto zmeny by mali byť súčasťou formálneho procesu riadenia zmien finančných inštitúcií, ktorý by mal zabezpečiť správne naplánovanie, testovanie, zdokumentovanie, povolenie a využívanie zmien.

1.4.5. Monitorovanie bezpečnosti

38. Finančné inštitúcie by mali stanoviť a vykonávať politiky a postupy na zisťovanie nezvyčajných činností, ktoré môžu ovplyvniť informačnú bezpečnosť finančných inštitúcií, a správne na tieto udalosti reagovať. V rámci tohto nepretržitého monitorovania by finančné inštitúcie mali zaviesť vhodné a účinné spôsobilosti na detekciu a nahlasovanie fyzického alebo logického narušenia, ako aj porušenia dôvernosti, integrity a dostupnosti informačných aktív. Procesy nepretržitého monitorovania a odhaľovania by mali zahŕňať:

a) príslušné interné a externé faktory vrátane obchodných funkcií a správcovských funkcií IKT;
b) transakcie na zistenie zneužívania prístupu tretími stranami alebo inými subjektmi a interného zneužívania prístupu;
c) potenciálne vnútorné a vonkajšie hrozby.

39. Finančné inštitúcie by mali stanoviť a implementovať procesy a organizačné štruktúry, aby sa identifikovali a neustále monitorovali bezpečnostné hrozby, ktoré by mohli významne ovplyvniť ich schopnosti poskytovať služby. Finančné inštitúcie by mali aktívne monitorovať technologický vývoj s cieľom, aby boli informovaní o bezpečnostných rizikách. Finančné inštitúcie by mali zaviesť opatrenia na odhaľovanie, napríklad na identifikáciu možných únikov informácií, škodlivého kódu a iných bezpečnostných hrozieb, ako aj verejne známych zraniteľných miest v softvéri a hardvéri a mali by kontrolovať, či majú zodpovedajúce nové aktualizácie zabezpečenia.

40. Proces monitorovania bezpečnosti by mal finančnej inštitúcii takisto pomôcť pochopiť povahu prevádzkových alebo bezpečnostných incidentov, identifikovať trendy a podporiť prešetrovania organizácie.

1.4.6. Preskúmania, posúdenie a testovanie informačnej bezpečnosti

41. Finančné inštitúcie by mali vykonávať rozmanité preskúmania, posúdenia a testovanie informačnej bezpečnosti na zabezpečenie účinnej identifikácie zraniteľných miest vo svojich IKT systémoch a IKT službách. Finančné inštitúcie môžu napríklad vykonávať analýzu nedostatkov v porovnaní s normami informačnej bezpečnosti, preskúmania dodržiavania súladu s predpismi, vnútorné a externé audity informačných systémov alebo preskúmania fyzickej bezpečnosti. Okrem toho by inštitúcie mali zvážiť osvedčené postupy, napríklad preskúmania zdrojového kódu, posúdenia zraniteľných miest, penetračné testy a útoky červeného tímu.

42. Finančné inštitúcie by mali stanoviť a zaviesť rámec pre testovanie informačnej bezpečnosti, ktorým sa potvrdí spoľahlivosť a účinnosť ich opatrení v oblasti informačnej bezpečnosti a zabezpečí sa, že sú v tomto rámci zohľadnené hrozby a zraniteľné miesta, ktoré sú identifikované prostredníctvom monitorovania hrozieb a postupu posúdenia rizík v oblasti IKT a bezpečnosti.

43. Rámcom pre testovanie informačnej bezpečnosti by sa malo zabezpečiť, že testy:

    a) vykonávajú len nezávislí vykonávatelia testov s dostatočnými vedomosťami, zručnosťami a odbornými znalosťami v testovaní opatrení informačnej bezpečnosti a ktorí nie sú zapojení do vývoja opatrení informačnej bezpečnosti;
    b) zahŕňajú kontroly zraniteľných miest a penetračné testy (vrátane penetračného testovania riadeného hrozbami, ak je to potrebné a vhodné) úmerné k úrovni identifikovaného rizika v obchodných procesoch a systémoch.

44. Finančné inštitúcie by mali vykonávať priebežné a opakované skúšky bezpečnostných opatrení. V prípade všetkých kritických IKT systémov (odsek 17) by sa tieto testy mali vykonávať najmenej na ročnom základe a v prípade poskytovateľov platobných služieb budú súčasťou komplexného posúdenia bezpečnostných rizík súvisiacich s platobnou službou, ktorú poskytujú, v súlade s článkom 95 ods. 2 druhej smernice o platobných službách. Iné ako kritické systémy by sa mali pravidelne testovať pomocou prístupu založeného na rizikách, najmenej však každé 3 roky.

45. Finančné inštitúcie by mali zabezpečiť, aby sa testy bezpečnostných opatrení vykonávali v prípade zmien infraštruktúry, procesov alebo postupov, a ak sa vykonajú zmeny z dôvodu zásadných prevádzkových alebo bezpečnostných incidentov alebo z dôvodu vydania nových alebo významne zmenených kritických aplikácií na internete.

46. Finančné inštitúcie by mali monitorovať a vyhodnocovať výsledky bezpečnostných testov a aktualizovať podľa toho svoje bezpečnostné opatrenia v prípade kritických IKT systémov bez zbytočného odkladu.

47. V prípade poskytovateľov platobných služieb by rámec testovania mal zahŕňať aj bezpečnostné opatrenia týkajúce sa 1. platobných terminálov a zariadení používaných na poskytovanie platobných služieb; 2. platobných terminálov a zariadení používaných na autentifikáciu používateľa platobných služieb; a 3. zariadení a softvéru poskytnutých poskytovateľom platobných služieb používateľovi platobných služieb na účel generovania/prijatia autentifikačného kódu.

48. Na základe pozorovaných bezpečnostných hrozieb a vykonaných zmien by sa malo vykonať testovanie tak, aby zahrnulo scenáre relevantných a známych potenciálnych útokov.

1.4.7. Odborná príprava a informovanosť v oblasti informačnej bezpečnosti

49. Finančné inštitúcie by mali vytvoriť program odbornej prípravy vrátane pravidelných programov zvyšovania informovanosti o bezpečnosti pre všetkých zamestnancov a dodávateľov, aby zabezpečili ich prípravu na vykonávanie povinností a úloh v súlade s príslušnými bezpečnostnými politikami a postupmi v záujme zníženia počtu chýb spôsobených ľudským faktorom, krádeží, podvodov, zneužití alebo strát a toho, ako riešiť riziká týkajúce sa informačnej bezpečnosti. Finančné inštitúcie by mali zabezpečiť, aby program odbornej prípravy poskytoval odbornú prípravu pre všetkých zamestnancov a dodávateľov aspoň ročne.

1.5. Riadenie prevádzok IKT

50. Finančné inštitúcie by mali riadiť svoje prevádzky IKT na základe zaznamenaných a zavedených procesov a postupov [ktoré v prípade poskytovateľov platobných služieb zahŕňajú dokument o bezpečnostnej politike v súlade s článkom 5 ods. 1 písm. j) druhej smernice o platobných službách], ktoré sú schválené riadiacim orgánom. Pomocou tohto súboru listín by sa malo vymedziť, ako finančné inštitúcie prevádzkujú, monitorujú a kontrolujú svoje IKT systémy a služby vrátane zaznamenania kritických prevádzok IKT, a mali by finančným inštitúciám umožniť udržiavať aktuálny súpis IKT aktív.

51. Finančné inštitúcie by mali zabezpečiť, aby bolo vykonávanie ich prevádzok IKT zosúladené s ich obchodnými požiadavkami. Finančné inštitúcie by mali udržiavať a, ak je to možné, zlepšovať efektívnosť svojich prevádzok IKT, okrem iného vrátane potreby zvážiť spôsob minimalizovania možných chýb vyplývajúcich z vykonávania manuálnych úloh.

52. Finančné inštitúcie by mali zaviesť postupy zapisovania do denníka a monitorovania v prípade kritických prevádzok IKT, aby sa umožnilo zisťovanie, analýza a oprava chýb.

53. Finančné inštitúcie by mali udržiavať aktuálny súpis svojich IKT aktív (vrátane IKT systémov, sieťových zariadení, databáz atď.). Súpis IKT aktív by mal uchovávať konfiguráciu IKT aktív a súvislosti a vzájomné závislosti medzi rôznymi IKT aktívami, aby sa umožnila náležitá konfigurácia a proces riadenia zmien.

54. Súpis IKT aktív by mal byť dostatočne podrobný, aby umožnil rýchlu identifikáciu IKT aktíva, jeho umiestnenia, bezpečnostnú klasifikáciu a vlastníctvo. Mali by byť zaznamenané vzájomné závislosti medzi aktívami, aby sa prispelo v reakcii na bezpečnostné a prevádzkové incidenty vrátane kybernetických útokov.

55. Finančné inštitúcie by mali monitorovať a riadiť životné cykly IKT aktív s cieľom zabezpečiť, aby naďalej spĺňali a podporovali obchodné požiadavky a požiadavky na riadenie rizík. Finančné inštitúcie by mali monitorovať, či sú ich IKT aktíva podporované ich externými alebo internými predajcami a vývojovými pracovníkmi a či sa uplatnili všetky príslušné opravy a modernizácie na základe zaznamenaných procesov. Mali by sa posúdiť a zmierniť riziká vyplývajúce z neaktuálnych alebo nepodporovaných IKT aktív.

56. Finančné inštitúcie by mali realizovať plánovanie výkonnosti a kapacity a procesy monitorovania s cieľom predísť, odhaliť a reagovať na dôležité problémy vo výkonnosti IKT systémov a nedostatkov IKT kapacity včas.

57. Finančné inštitúcie by mali vymedziť a realizovať zálohovanie údajov a IKT systémov a postup obnovy s cieľom zabezpečiť, aby mohli byť obnovené podľa potreby. Rozsah a frekvencia zálohovania by mali byť stanovené v súlade s obchodnými požiadavkami na obnovu a kritickou povahou údajov a IKT systémov a hodnotené podľa vykonaného posúdenia rizík. Pravidelne by sa malo vykonávať testovanie postupov zálohovania a obnovy.

58. Finančné inštitúcie by mali zabezpečiť, aby sa zálohy údajov a IKT systémov uchovávali zabezpečené a aby boli dostatočne vzdialené od primárneho miesta, aby neboli vystavené rovnakým rizikám.

3.5.1 Riadenie IKT incidentov a problémov

59. Finančné inštitúcie by mali zaviesť a realizovať postup riadenia incidentov a problémov na monitorovanie a zaznamenávanie prevádzkových a bezpečnostných IKT incidentov a aby umožnili finančným situáciám pokračovať alebo znovu včas obnoviť kritické obchodné funkcie a procesy v prípade výskytu narušení. Finančné inštitúcie by mali určiť vhodné kritériá a prahové hodnoty na klasifikáciu udalostí ako prevádzkových alebo bezpečnostných incidentov, ako je stanovené vo Vymedzení pojmov týchto usmernení, ako aj ukazovatele včasného varovania, ktoré by mali slúžiť ako upozornenia umožňujúce včasné odhalenie týchto incidentov. Týmito kritériami a prahovými hodnotami nie je v prípade poskytovateľov platobných služieb dotknutá klasifikácia zásadných incidentov v súlade s článkom 96 druhej smernice o platobných službách a Usmernenia k oznamovaniu závažných incidentov podľa smernice (EÚ) 2015/2366 o platobných službách (PSD2) (EBA/GL/2017/10).

60. S cieľom minimalizovať vplyv nepriaznivých udalostí a umožniť včasnú obnovu by finančné inštitúcie mali stanoviť vhodné procesy a organizačné štruktúry na zabezpečenie jednotného a integrovaného monitorovania, zaobchádzania a nadväzných opatrení na prevádzkové a bezpečnostné incidenty a na zabezpečenie identifikácie a odstránenia základných príčin, aby sa zabránilo výskytu opakovaných incidentov. V procese riadenia incidentov a problémov by sa mali stanoviť:

    a) postupy na identifikáciu, zaznamenávanie, zapisovanie do denníka, kategorizovanie a klasifikovanie incidentov podľa priority na základe obchodnej kritickej povahy;
    b) úlohy a zodpovednosti za rôzne scenáre incidentov (napr. chyby, nesprávne fungovanie, kybernetické útoky);
    c) postupy riadenia problémov na identifikovanie, analyzovanie a riešenie základnej príčiny jedného alebo viacerých incidentov — finančná inštitúcia by mala vždy analyzovať prevádzkové alebo bezpečnostné incidenty, ktoré pravdepodobne ovplyvnia finančnú inštitúciu, ktoré boli identifikované alebo sa vyskytli v rámci organizácie a/alebo mimo nej, a mala by zvážiť hlavné poznatky získané z týchto analýz a zodpovedajúcim spôsobom aktualizovať bezpečnostné opatrenia;

d) účinné plány internej komunikácie vrátane postupov oznamovania a incidentov a postupovania nadriadeným — vzťahujúce sa aj na sťažnosti klienta týkajúce sa bezpečnosti — s cieľom zabezpečiť:
    i) aby incidenty s potenciálne veľkým nepriaznivým vplyvom na kritické IKT systémy a IKT služby boli nahlasované príslušnému vrcholovému manažmentu a vrcholovému manažmentu IKT;
    ii) aby riadiaci orgán bol informovaný na báze ad hoc v prípade významných incidentov a aby bol informovaný minimálne o vplyve, reakcii a dodatočných kontrolách, ktoré sa vymedzia v dôsledku incidentov;
e) postupy reakcie na incidenty s cieľom zmierniť vplyvy spojené s incidentmi a zabezpečiť, aby sa služba včas stala prevádzkyschopnou a bezpečnou;
f) osobitné plány externej komunikácie pre kritické obchodné funkcie a procesy s cieľom:
    i) spolupracovať s príslušnými zainteresovanými stranami v záujme účinnej reakcie a obnovy po incidente;
    ii) poskytnúť včas informácie externým stranám (napr. klientom, iným účastníkom trhu, orgánu dohľadu) tak, ako je to vhodné, a v súlade s platnou reguláciou.

1.6. Riadenie IKT projektov a zmien

1.6.1. Riadenie IKT projektov

61. Finančná inštitúcia by mala zaviesť program a/alebo proces projektového riadenia, v ktorom sú vymedzené úlohy, povinnosti a zodpovednosti s cieľom účinne podporiť vykonávanie stratégie v oblasti IKT.

62. Finančná inštitúcia by mala náležite monitorovať a zmierňovať riziká odvodené z jej portfólia IKT projektov (programové riadenie) so zreteľom aj na riziká, ktoré môžu vyplývať zo vzájomných závislostí medzi rôznymi projektami a zo závislostí viacerých projektov od rovnakých zdrojov a/alebo odborných znalostí.

63. Finančná inštitúcia by mala zaviesť a realizovať politiku riadenia IKT projektov, ktorá zahŕňa minimálne:

    a) ciele projektu;

    b) úlohy a zodpovednosti;

    c) posúdenie rizík projektu;

    d) projektový plán, harmonogram a kroky;

    e) hlavné míľniky;

    f) požiadavky na riadenie zmien.

64. Politikou riadenia IKT projektov by sa malo zabezpečiť, aby požiadavky na informačnú bezpečnosť boli analyzované a schválené funkciou, ktorá je nezávislá od vývojovej funkcie.

65. Finančná inštitúcia by mala zabezpečiť, aby boli všetky oblasti, na ktoré má IKT projekt vplyv, zastúpené v projektovom tíme, a aby projektový tím mal znalosti potrebné na zabezpečenie bezpečnej a úspešnej realizácie projektu.

66. O vytvorení a pokroku IKT projektov a ich súvisiacich rizikách by sa mala podávať správa riadiacemu orgánu jednotlivo alebo súhrnne v závislosti od dôležitosti a veľkosti IKT projektov, pravidelne a na báze ad hoc podľa primeranosti. Finančné inštitúcie by mali zaradiť projektové riziko do svojho rámca pre riadenie rizík.

1.6.2. Nadobudnutie a vývoj IKT systémov

67. Finančné inštitúcie by mali vyvíjať a realizovať proces, ktorým sa riadi nadobúdanie, vývoj a údržba IKT systémov. Tento proces by mal byť navrhnutý pomocou prístupu založeného na rizikách.

68. Finančná inštitúcia by mala zabezpečiť, aby boli pred akýmkoľvek nadobudnutím alebo vývojom IKT systémov jasne vymedzené a schválené príslušným obchodným vedením funkčné a iné ako funkčné požiadavky (vrátane požiadaviek na informačnú bezpečnosť).

69. Finančná inštitúcia by mala zabezpečiť, aby boli zavedené opatrenia na zmiernenia rizika nezámerného pozmenenia alebo zámernej manipulácie IKT systémov počas vývoja a implementácie v produkčnom prostredí.

70. Finančné inštitúcie by mali mať zavedenú metodiku na testovanie a schvaľovanie IKT systémov pred ich prvým použitím. V tejto metodike by mala byť zohľadnená kritická povaha obchodných procesov a aktív. Testovaním by sa malo zabezpečiť, aby nové IKT systémy fungovali podľa plánu. Mali by takisto používať testovacie prostredia, ktoré náležite zohľadňujú produkčné prostredie.

71. Finančné inštitúcie by mali testovať IKT systémy, IKT služby a opatrenia informačnej bezpečnosti s cieľom identifikovať potenciálne bezpečnostné slabé stránky, narušenia a incidenty.

72. Finančná inštitúcia by mala zaviesť samostatné IKT prostredia na zabezpečenie náležitého oddelenia povinností a s cieľom zmierniť vplyv neoverených zmien v produkčných systémoch. Konkrétne by finančná inštitúcia mala zabezpečiť oddelenie produkčných prostredí od vývojových, testovacích a iných neprodukčných prostredí. Finančná inštitúcia by mala zabezpečiť integritu a dôvernosť produkčných údajov v neprodukčných prostrediach. Prístup k produkčným údajom je obmedzený na oprávnených používateľov.

73. Finančné inštitúcie by mali zaviesť opatrenia na ochranu integrity zdrojových kódov IKT systémov, ktoré sú vyvinuté interne. Mali by takisto komplexne zaznamenávať vývoj, realizáciu, prevádzku a/alebo konfiguráciu IKT systémov, aby sa znížila akákoľvek nie nevyhnutná závislosť na odborníkoch v danej oblasti. Dokumentácia o IKT systéme by mala obsahovať, ak sa uplatňuje, aspoň používateľskú dokumentáciu, dokumentáciu technického systému a prevádzkové postupy.

74. Procesy finančnej inštitúcie týkajúce sa nadobudnutia a vývoja IKT systémov by sa mali vzťahovať aj na IKT systémy vyvinuté alebo riadené koncovými používateľmi obchodnej funkcie mimo IKT organizácie (napr. počítačové aplikácie koncových používateľov) pomocou prístupu

na základe rizík. Finančná inštitúcia by mala viesť register týchto aplikácií, ktoré podporujú kritické obchodné funkcie alebo procesy.

1.6.3. Riadenie IKT zmien

75. Finančné inštitúcie by mali stanoviť a vykonávať proces riadenia IKT zmien s cieľom zabezpečiť, aby boli všetky zmeny IKT systémov zaznamenané, testované, posúdené, schválené, vykonané a overené kontrolovaným spôsobom. Finančné inštitúcie by mali spracovať zmeny počas núdzových situácií (t. j. zmeny, ktoré musia byť zavedené čo najskôr) podľa postupov, ktoré poskytujú primerané ochranné opatrenia.

76. Finančné inštitúcie by mali určovať, či zmeny v existujúcom prevádzkovom prostredí ovplyvňujú existujúce bezpečnostné opatrenia alebo si vyžadujú prijatie dodatočných opatrení na zmiernenie príslušných rizík. Tieto zmeny by mali byť v súlade s formálnym procesom riadenia zmien finančných inštitúcií.

1.7. Riadenie kontinuity činnosti

77. Finančné inštitúcie by mali zaviesť proces riadenia kontinuity činností (business continuity management, BCM) s cieľom maximalizovať svoje schopnosti poskytovať služby na priebežnom základe a obmedziť straty v prípade závažného narušenia činnosti v súlade s článkom 85 ods. 2 smernice 2013/36/EÚ a hlavy VI Usmernení EBA o vnútornom riadení (EBA/GL/2017/11).

1.7.1. Analýza vplyvu na činnosť

78. V rámci správneho riadenia kontinuity činnosti by finančné inštitúcie mali vykonávať analýzu vplyvu na činnosť analyzovaním svojej expozície voči závažným narušeniam činnosti a posudzovaním ich potenciálnych vplyvov (a to aj na dôvernosť, integritu a dostupnosť) kvantitatívne a kvalitatívne s pomocou interných a/alebo externých údajov (napr. údaje poskytovateľa, ktorý je treťou stranou, relevantné pre proces činnosti alebo verejne dostupné údaje, ktoré môžu byť relevantné pre analýzu vplyvu na činnosť) a analýzou scenárov. V analýze vplyvu na činnosť by sa mala zvážiť aj kritická povaha identifikovaných a klasifikovaných funkcií činnosti, podporných procesov, tretích strán a informačných aktív a ich vzájomné závislosti v súlade s oddielom 1.3.3.

79. Finančné inštitúcie by mali zabezpečiť, aby ich IKT systémy a IKT služby boli navrhnuté a zosúladené s ich analýzou vplyvu na činnosť, napríklad s redundanciou určitých kritických zložiek, aby sa zabránilo narušeniam spôsobeným udalosťami, ktoré ovplyvňujú uvedené zložky.

1.7.2. Plánovanie zabezpečenia kontinuity činnosti

80. Na základe svojich analýz vplyvu na činnosť by finančné inštitúcie mali vytvoriť plány na zabezpečenie kontinuity činností (plány na zabezpečenie kontinuity činnosti), ktoré by mali byť zaznamenané a schválené ich riadiacimi orgánmi. V plánoch by mali byť osobitne zvážené riziká, ktoré by mohli mať nepriaznivý vplyv na IKT systémy a IKT služby. Plány by mali podporovať ciele, ktoré majú chrániť, a v prípade potreby obnoviť, dôvernosť, integritu a dostupnosť ich

obchodných funkcií, podporných procesov a informačných aktív. Finančné inštitúcie by mali počas vytvárania týchto plánov vykonávať koordináciu s príslušnými internými a externými zainteresovanými stranami, ako je to vhodné.

81. Finančné inštitúcie by mali zaviesť plány na zabezpečenie kontinuity činnosti na zabezpečenie toho, aby reagovali správne na možné scenáre zlyhania a aby boli schopné obnoviť operácie svojich kritických obchodných činností po narušeniach v rámci cieľového času obnovenia (maximálny čas, v rámci ktorého musí byť systém alebo proces obnovený po incidente) a cieľového bodu obnovenia (maximálne obdobie, počas ktorého je prijateľné, aby sa údaje v prípade incidentu stratili). V prípadoch závažného narušenia činnosti, na základe ktorých sa aktivujú osobitné plány na zabezpečenie kontinuity činnosti, by finančné inštitúcie mali určiť priority opatreniam kontinuity činností pomocou prístupu na základe rizík, ktorý môže byť založený na posúdeniach rizík vykonaných podľa oddielu 1.3.3. V prípade poskytovateľov platobných služieb to môže zahŕňať napríklad zjednodušenie ďalšieho spracovania kritických transakcií počas vynakladania úsilia o nápravu.

82. Finančná inštitúcia by mala vo svojom pláne na zabezpečenie kontinuity činností zvážiť celý rad rôznych scenárov vrátane extrémnych, ale vierohodných scenárov, ktorým by mohla byť vystavená, vrátane scenára kybernetického útoku, a posúdiť ich prípadný vplyv. Na základe týchto scenárov by finančná inštitúcia mala opísať, ako je zabezpečená kontinuita IKT systémov a služieb, ako aj informačná bezpečnosť finančnej inštitúcie.

1.7.3. Plány reakcie a obnovy

83. Na základe analýz vplyvu na činnosť (odsek 78) a vierohodných scenárov (odsek 82) by finančné inštitúcie mali vyvinúť plány reakcie a obnovy. V týchto plánoch by sa malo stanovovať, aké podmienky môžu vyvolať aktivovanie týchto plánov a aké kroky by sa mali prijať na zabezpečenie dostupnosti, kontinuity a obnovy aspoň kritických IKT systémov a IKT služieb finančných inštitúcií. Plány reakcie a obnovy by mali mať za cieľ splniť ciele obnovy operácií finančných inštitúcií.

84. Plány reakcie a obnovy by mali zohľadňovať krátkodobé, ako aj dlhodobé možnosti obnovy. Plány by:

    a) sa mali zameriavať na obnovu operácií kritických obchodných funkcií, podporných procesov, informačných aktív a ich vzájomných závislostí, aby sa zabránilo nepriaznivým vplyvom na fungovanie finančných inštitúcií a finančného systému vrátane platobných systémov a používateľov platobných služieb, a aby sa zabezpečilo vykonanie nevybavených platobných transakcií;
    b) mali byť zdokumentované a prístupné obchodným a podporným jednotkám a byť ľahko dostupné v prípade núdze;
    c) mali byť aktualizované v súlade so skúsenosťami získanými z incidentov, testov, identifikovanými novými rizikami a hrozbami, ako aj so zmenenými cieľmi a s prioritami obnovy.

85. V plánoch by takisto mali byť zohľadnené alternatívne možnosti, ak nie je možné zrealizovať obnovu v krátkodobom horizonte z dôvodu nákladov, rizík, logistiky či nepredvídaných okolností.

86. Okrem toho, v rámci plánov reakcie a obnovy by finančná inštitúcia mala zvážiť a zaviesť opatrenia týkajúce sa kontinuity, aby sa zmiernili zlyhania poskytovateľov, ktorí sú tretími stranami, ktoré majú zásadný význam pre kontinuitu IKT služieb finančnej inštitúcie [v súlade s ustanoveniami Usmernení EBA o outsourcingu (EBA/GL/2019/02), pokiaľ ide o plány na zabezpečenie kontinuity činnosti].

1.7.4. Testovanie plánov

87. Finančné inštitúcie by mali pravidelne testovať svoje plány na zabezpečenie kontinuity činnosti. Najmä by mali zabezpečiť, aby plány na zabezpečenie kontinuity činností týkajúce sa ich dôležitých obchodných funkcií, podporných procesov, informačných aktív a ich vzájomné súvislosti (vrátané tých, ktoré poskytujú tretie strany, ak sa uplatňuje) boli testované najmenej ročne, v súlade s odsekom 89.

88. Plány na zabezpečenie kontinuity činností by sa mali aktualizovať najmenej ročne, na základe výsledkov skúšania, súčasných spravodajských informácií o hrozbách a poznatkov získaných z predchádzajúcich udalostí. Všetky zmeny v cieľoch obnovy (vrátane cieľového času obnovenia a cieľového bodu obnovenia) a/alebo zmeny v obchodných funkciách, podporných procesoch a informačných aktívach by takisto mali byť zvážené, ak je to relevantné, ako základ pre aktualizáciu plánov na zabezpečenie kontinuity činností.

89. Testovanie plánov na zabezpečenie kontinuity činností finančnými inštitúciami by malo preukazovať, že sú schopné udržať životaschopnosť svojich činností do času obnovenia kritických operácií. Najmä by malo:

    a) zahŕňať testovanie primeraného súboru závažných, ale vierohodných scenárov vrátane tých, s ktorými sa uvažuje pre vývoj plánov na zabezpečenie kontinuity činností (ako aj testovanie služieb poskytované tretími stranami, ak sa uplatňuje); toto by malo zahŕňať prepnutie kritických obchodných funkcií, podporných procesov a informačných aktív do prostredia obnovy po havárii a preukázať, že môžu byť prevádzkované týmto spôsobom počas dostatočne reprezentatívneho obdobia a že následne je možné obnoviť normálne fungovanie;
    b) byť navrhnuté tak, aby spochybňovalo predpoklady, na ktorých stoja plány na zabezpečenie kontinuity činností vrátane dohôd o riadení a plánov krízovej komunikácie a
    c) zahŕňať postupy na overenie schopnosti ich zamestnancov a dodávateľov, IKT systémov a IKT služieb, či správne reagujú na scenáre v odseku 89 písm. a).

90. Výsledky testov by mali byť zaznamenané a všetky identifikované nedostatky vyplývajúce z testov by mali byť analyzované, riešené a nahlásené riadiacemu orgánu.

1.7.5. Komunikácia v prípade krízy

91. V prípade prerušenia prevádzky alebo núdzového stavu a počas vykonávania plánov na zabezpečenie kontinuity činností by finančné inštitúcie mali zabezpečiť, aby boli zavedené účinné opatrenia pre komunikáciu v prípade krízy, aby boli všetky príslušné interné a externé zainteresované strany vrátane príslušných orgánov, ak si to vyžadujú vnútroštátne predpisy, a takisto príslušných poskytovateľov služieb (poskytovatelia externého zabezpečovania činností,

subjekty v skupine alebo poskytovatelia, ktorí sú tretími stranami) včas a primerane informované.

1.8. Riadenie vzťahov s používateľmi platobných služieb

92. Poskytovatelia platobných služieb by mali stanoviť a implementovať procesy na zvýšenie povedomia používateľov platobných služieb o bezpečnostných rizikách spojených s platobnými službami tak, že poskytnú asistenčné služby a usmernenia pre používateľov platobných služieb.

93. Pomoc a usmernenia ponúkané používateľom platobných služieb by sa mali aktualizovať vzhľadom na nové hrozby a zraniteľné miesta, pričom používatelia platobných služieb by mali byť o zmenách informovaní.

94. Ak to umožňuje funkčnosť produktu, poskytovatelia platobných služieb by mali umožniť používateľom platobných služieb zakázať konkrétne platobné funkcie súvisiace s platobnými službami, ktoré poskytovateľ platobných služieb ponúka používateľovi platobných služieb.

95. Ak sa poskytovateľ platobných služieb v súlade s článkom 68 ods. 1 smernice (EÚ) 2015/2366 s platiteľom dohodne na výdavkových limitoch na platobné transakcie vykonávané prostredníctvom osobitných platobných nástrojov, poskytovateľ platobných služieb by mal poskytnúť platiteľovi možnosť upraviť tieto limity až do maximálneho dohodnutého limitu.

96. Poskytovatelia platobných služieb by mali používateľom platobných služieb poskytnúť možnosť prijímať upozornenia o iniciovaných a/alebo neúspešných pokusoch o iniciovanie platobných transakcií, čo im umožní odhaliť podvodné alebo škodlivé používanie ich účtov.

97. Poskytovatelia platobných služieb by mali informovať používateľov platobných služieb o aktualizáciách bezpečnostných postupov, ktoré majú vplyv na používateľov platobných služieb v súvislosti s poskytovaním platobných služieb.

98. Poskytovatelia platobných služieb by mali poskytnúť používateľom platobných služieb pomoc pri všetkých otázkach, žiadostiach o podporu a upozorneniach na anomálie alebo problémy týkajúce sa bezpečnostných záležitostí súvisiacich s platobnými službami. Používatelia platobných služieb by mali byť primerane informovaní o tom, ako možno takúto pomoc získať.