EBA/GL/2017/05

11/09/2017

Usmernenia

Usmernenia pre posudzovanie rizika súvisiaceho s informačnými a komunikačnými technológiami v rámci postupu preskúmania a hodnotenia orgánmi dohľadu (SREP)

1. Povinnosti týkajúce sa dodržiavania súladu (compliance) s predpismi a ohlasovacia povinnosť

Štatút týchto usmernení

1. Tento dokument obsahuje usmernenia vydané podľa článku 16 nariadenia (EÚ) č. 1093/20101. Podľa článku 16 ods. 3 nariadenia č. 1093/2010 príslušné orgány a finančné inštitúcie vynaložia všetko úsilie na dodržanie týchto usmernení a odporúčaní.

2. Tieto usmernenia zahŕňajú názor EBA na príslušné postupy dohľadu v rámci Európskeho systému finančného dohľadu alebo na spôsob uplatňovania právnych predpisov Únie v konkrétnej oblasti. Príslušné orgány, ako sú vymedzené v článku 4 ods. 2 nariadenia (EÚ) č. 1093/2010, na ktoré sa tieto usmernenia vzťahujú, ich majú 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 tieto usmernenia zamerané prevažne na banky.

Požiadavky na vykazovanie

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 musia uviesť dôvody ich nedodržania do 13.11.2017. 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 adrese compliance@eba.europa.eu spolu s označením „EBA/GL/2017/05“. Tieto oznámenia majú príslušnému orgánu predkladať osoby, ktoré sú oprávnené podávať správy o dodržaní v mene svojich príslušných orgánov. Akúkoľvek zmenu stavu dodržiavania ustanovení treba takisto oznámiť EBA.

4. Oznámenia budú uverejnené na webovej stránke 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).

2. Predmet úpravy, rozsah pôsobnosti a vymedzenia pojmov

Predmet úpravy a rozsah pôsobnosti

5. Účelom týchto usmernení vypracovaných podľa článku 107 ods. 3 smernice 2013/36/EÚ[2] je zabezpečiť zblíženie postupov dohľadu pri posudzovaní rizika súvisiaceho s informačnými a komunikačnými technológiami (ďalej len „IKT“) v rámci postupu preskúmania a hodnotenia orgánmi dohľadu (ďalej len „SREP“) uvedeného v článku 97 smernice 2013/36/EÚ a podrobnejšie špecifikovaného v Usmerneniach EBA o spoločných postupoch a metodikách postupu preskúmania a hodnotenia orgánmi dohľadu (SREP)[3]. V týchto usmerneniach sa konkrétne stanovujú kritériá posudzovania, ktoré by príslušné orgány mali uplatňovať pri posudzovaní orgánmi dohľadu v súvislosti so správou a riadením inštitúcií a ich stratégiou v oblasti IKT a pri posudzovaní orgánmi dohľadu v súvislosti s expozíciami inštitúcií voči rizikám súvisiacim s IKT a ich kontrolami týchto rizík. Tieto usmernenia tvoria neoddeliteľnú súčasť usmernení EBA o postupe SREP.

6. Príslušné orgány by tieto usmernenia mali uplatňovať v súlade s úrovňou uplatňovania postupu SREP stanovenou v usmerneniach EBA o postupe SREP a v súlade s modelom minimálnej účasti a požiadavkami na proporcionalitu stanovenými v uvedených usmerneniach.

Adresáti

7. Tieto usmernenia sú určené príslušným orgánom vymedzeným v článku 4 ods. 2 bode i) nariadenia (EÚ) č. 1093/2010.

Vymedzenia pojmov

8. Pokiaľ sa neuvádza inak, pojmy použité a vymedzené v smernici 2013/36/EÚ, nariadení (EÚ) č. 575/2013 a vymedzenia pojmov z usmernenia EBA o postupe SREP majú v týchto usmerneniach rovnaký význam. Na účely týchto usmernení sa okrem toho uplatňujú tieto vymedzenia pojmov:

[2] Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (1) – Ú. v. EÚ L 176, 27.6.2013, s. 338.

[3] EBA/GL/2014/13.

IKT systémy	IKT štruktúra ako súčasť mechanizmu alebo prepájacia sieť, ktorá slúži na podporu operácií inštitúcie.
IKT služby	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.
Riziko súvisiace s dostupnosťou a kontinuitou IKT	Riziko, že výkonnosť a dostupnosť IKT systémov a údajov budú nepriaznivo postihnuté vrátane neschopnosti včas obnoviť služby inštitúcie, a to z dôvodu zlyhania zložiek hardvéru a softvéru IKT; z dôvodu nedostatkov pri správe IKT systému; alebo z dôvodu inej udalosti, ako sa podrobnejšie uvádza v prílohe.
Riziko súvisiace s bezpečnosťou IKT	Riziko neoprávneného prístupu do IKT systémov a k údajom zo zariadení v rámci inštitúcie alebo mimo nej (napr. kybernetické útoky), ako sa podrobnejšie uvádza v prílohe.
Riziko súvisiace so zmenou IKT	Riziko vyplývajúce z neschopnosti inštitúcie zvládnuť zmeny IKT systému včas a kontrolovaným spôsobom, najmä v prípade programov rozsiahlych a zložitých zmien, ako sa podrobnejšie uvádza v prílohe.
Riziko súvisiace s integritou IKT údajov	Riziko, že by údaje uložené a spracované IKT systémami boli v rôznych IKT systémoch neúplné, chybné alebo nepresné, napríklad z dôvodu slabých kontrol IKT alebo ich neexistencie počas rôznych fáz životného cyklu IKT údajov (t. j. z dôvodu návrhu dátovej architektúry, konštrukcie dátového modelu a/alebo dátových slovníkov, overovania vstupných údajov, kontroly extrakcie, prenosu a spracovania údajov vrátane poskytnutých výstupných údajov), čo oslabuje schopnosť inštitúcie poskytovať služby a správne a včas vytvárať informácie o riadení (rizík) a finančné informácie, ako sa podrobnejšie uvádza v prílohe.
Riziko súvisiace s externým zabezpečovaním IKT služieb	Riziko, že zapojenie tretej strany alebo iného subjektu skupiny (zverenie výkonu činností externým subjektom v rámci skupiny) do poskytovania IKT systémov alebo súvisiacich služieb nepriaznivo ovplyvní fungovanie a riadenie rizík inštitúcie, ako sa podrobnejšie uvádza v prílohe.

3. Vykonávanie

Dátum uplatňovania

9. Tieto usmernenia sa uplatňujú od 1. januára 2018.

4. Požiadavky na posudzovanie rizika súvisiaceho s informačnými a komunikačnými technológiami

Hlava 1 – Všeobecné ustanovenia

10. Príslušné orgány by mali vykonávať posudzovanie rizika súvisiaceho s IKT a mechanizmov riadenia a stratégie IKT v rámci postupu preskúmania a hodnotenia orgánmi dohľadu (ďalej len „SREP“) na základe modelu minimálnej účasti a kritérií proporcionality stanovených v hlave 2 usmernení EBA o postupe SREP. To konkrétne znamená, že:

    a. frekvencia posudzovanie rizika súvisiaceho s IKT bude závisieť od modelu minimálnej účasti, ktorý sa riadi podľa kategórie postupu SREP, ku ktorej bola inštitúcia priradená, a podľa konkrétneho programu previerok v oblasti dohľadu; a

    b. dôkladnosť, podrobnosť a mohutnosť posudzovania IKT majú byť primerané veľkosti, štruktúre a operačnému prostrediu inštitúcie, ako aj povahe, rozsahu a zložitosti jej činností.

11. Zásada proporcionality sa v celých týchto usmerneniach uplatňuje na rozsah, frekvenciu a mieru účasti orgánov dohľadu, ich dialóg s inštitúciou a očakávania v oblasti dohľadu týkajúce sa štandardov, ktoré by inštitúcia mala spĺňať.

12. Príslušné orgány sa môžu opierať o prácu, ktorú už inštitúcia alebo príslušný orgán vykonali v súvislosti s posudzovaním ďalších rizík alebo s prvkami postupu preskúmania a hodnotenia orgánmi dohľadu, alebo túto prácu môžu zohľadniť s cieľom získať aktualizované posúdenie. Konkrétne pri posudzovaniach stanovených v týchto usmerneniach si príslušné orgány majú vybrať najvhodnejší prístup a metodiku posúdenia orgánmi dohľadu, ktoré najviac zodpovedajú a ktoré sú primerané inštitúcii, a príslušné orgány majú na získanie informácií pre svoje posúdenie použiť existujúcu a dostupnú dokumentáciu [napr. príslušné správy a iné dokumenty, stretnutia s manažmentom (rizík), zistenia z kontrol na mieste].

13. Príslušné orgány majú zhrnúť zistenia svojho hodnotenia podľa kritérií uvedených v týchto usmerneniach a použiť ich na dosiahnutie záverov v rámci hodnotenia SREP, ako sa stanovuje v usmerneniach EBA o postupe SREP.

14. Posudzovanie riadenia a stratégie IKT vykonané v súlade s hlavou 2 týchto usmernení by konkrétne malo poskytnúť zhrnutie zistení v elemente- kontroly v rámci postupu SREP týkajúceho sa posúdenia vnútorného riadenia a kontrol rizík celej inštitúcie, ako sa uvádza v hlave 5 usmernení EBA o postupe SREP, a malo by sa odzrkadliť v príslušnom skóringovom hodnotení daného elementu v rámci SREP. Príslušné orgány by navyše mali vziať do úvahy, že z každého významného nepriaznivého vplyvu

posúdenia stratégie IKT na obchodnú stratégiu inštitúcie alebo z akýchkoľvek obáv, že by inštitúcia nemusela mať dostatočné zdroje a spôsobilosti v oblasti IKT na vykonávanie a podporu dôležitých plánovaných strategických zmien, by sa mali poskytnúť informácie pre analýzu obchodného modelu podľa hlavy 4 usmernení EBA o postupe SREP.

15. Výsledky posudzovania rizika súvisiaceho s IKT, ako sa uvádza v hlave 3 týchto usmernení, by mali poskytnúť informácie pre zistenia z posúdenia operačného rizika a mali by sa považovať za základ pre príslušné skóringové hodnotenie, ako sa uvádza v oddiele 6.4 usmernení EBA o postupe SREP.

16. Treba pripomenúť, že hoci vo všeobecnosti by príslušné orgány podkategórie rizík mali posudzovať ako súčasť hlavných kategórií (t. j. riziko súvisiace s IKT sa bude posudzovať ako súčasť operačného rizika), v prípade, ak príslušné orgány považujú určité podkategórie za významné, môžu tieto podkategórie posudzovať samostatne. Na tento účel sa v týchto usmerneniach, ak by príslušný orgán označil riziko súvisiace s IKT ako významné riziko, uvádza aj tabuľka skóringového hodnotenia (Tabuľka 1), ktorá by sa mala použiť na skóringové hodnotenie samostatnej podkategórie rizika súvisiaceho s IKT na základe celkového prístupu k skóringovému hodnoteniu rizík pre kapitál v usmerneniach EBA o postupe SREP.

17. Na dosiahnutie stanoviska, či by sa riziko súvisiace s IKT malo považovať za významné, a teda či by mala byť možnosť toto riziko posudzovať a hodnotiť ako samostatnú podkategóriu operačného rizika, príslušné orgány môžu použiť kritériá stanovené v oddiele 6.1 usmernení EBA o postupe SREP.

18. Pri uplatňovaní týchto usmernení by príslušné orgány mali v náležitých prípadoch zohľadniť neúplný zoznam podkategórií a scenárov rizika súvisiaceho s IKT, ako sa uvádzajú v prílohe, pričom treba pripomenúť, že príloha je zameraná na riziká súvisiace s IKT, ktoré môžu viesť k veľmi vážnym stratám. Príslušné orgány môžu niektoré riziká súvisiace s IKT uvedených v taxonómii vylúčiť, ak nesúvisia s ich posudzovaním. Inštitúcie by mali udržiavať vlastné taxonómie rizík namiesto používania taxonómie rizík súvisiacich s IKT stanovenými v prílohe.

19. Ak sa tieto usmernenia uplatňujú v súvislosti s cezhraničnými bankovými skupinami a ich subjektmi a ak bolo zriadené kolégium orgánov dohľadu, zapojené príslušné orgány majú v kontexte svojej spolupráce na posúdení SREP v súlade s oddielom 11.1 usmernení EBA o postupe SREP v maximálnej možnej miere koordinovať presný a podrobný rozsah jednotlivých informácií jednotne pre všetky subjekty v skupine.

Hlava 2 – Posúdenie riadenia a stratégie inštitúcií v súvislosti s IKT

2.1 Všeobecné zásady

20. Príslušné orgány by mali posúdiť, či všeobecný rámec riadenia a vnútornej kontroly presne pokrýva IKT systémy a súvisiace riziká a či riadiaci orgán primerane rieši a spravuje tieto aspekty, keďže IKT sú neoddeliteľné od riadneho fungovania inštitúcie.

21. Pri vykonávaní hodnotenia by sa príslušné orgány mali riadiť požiadavkami a štandardmi správneho vnútorného riadenia a opatreniami na kontrolu rizík, ako sa uvádza v usmerneniach EBA o vnútornom riadení (GL 44)[4] a medzinárodnými usmerneniami v tejto oblasti, a to v takej miere, v akej sa tieto usmernenia môžu uplatňovať vzhľadom na osobitosť systémov a rizík súvisiacich s IKT.

22. Hodnotenie v tejto hlave sa nevzťahuje na konkrétne prvky IKT systému riadenia , riadenia rizík a kontrol IKT systému, ktoré sú zamerané na správu konkrétnych rizík súvisiacich s IKT, ktorou sa zaoberá hlava 3 týchto usmerneniach. Toto hodnotenie sa namiesto toho zameriava na tieto oblasti:

    a. stratégia IKT – či má inštitúcia stratégiu IKT, ktorá sa riadi primeraným spôsobom a ktorá je v súlade s obchodnou stratégiou inštitúcie;

    b. celkové vnútorné riadenie – či je celkový mechanizmus vnútorného riadenia inštitúcie primeraný vzhľadom na IKT systémy inštitúcie; a

    c. riziko súvisiace s IKT v rámci riadenia rizík inštitúcie – či rámec inštitúcie pre riadenie rizík a vnútornú kontrolu primerane ochraňuje IKT systémy inštitúcie.

23. Hoci výsledky hodnotenia v bode 22 písmene a) poskytujú informácie o prvkoch riadenia inštitúcie, mali by predstavovať predovšetkým vstupné údaje pre posúdenie obchodného modelu, ktorým sa zaoberá hlava 4 usmernení EBA o postupe SREP. Písmená b) a c) ďalej dopĺňajú hodnotenie tém, na ktoré sa vzťahuje hlava 5 usmernení EBA o postupe SREP, a hodnotenie opísané v týchto usmerneniach by malo poskytnúť vstupy pre príslušné hodnotenie podľa hlavy 5 usmernení EBA o postupe SREP.

24. Výsledok tohto hodnotenia by mal v náležitých prípadoch poskytnúť informácie pre posudzovanie riadenia rizík a kontrol v hlave 3 týchto usmernení.

2.2 Stratégia IKT

25. Podľa tohto oddielu by príslušné orgány mali hodnotiť, či inštitúcia disponuje stratégiou pre IKT: ktorá podlieha primeranému dohľadu riadiaceho orgánu inštitúcie; ktorá je v súlade s obchodnou stratégiou,

[4] Usmernenia EBA o vnútornom riadení, GL 44, 27. septembra 2011.

najmä stratégia pre udržiavanie aktuálnosti jej IKT a pre plánovanie alebo vykonávanie dôležitých a zložitých zmien IKT; a ktorá podporuje obchodný model inštitúcie.

2.2.1 Vývoj a primeranosť stratégie IKT

26. Príslušné orgány by mali posúdiť, či inštitúcia zaviedla rámec na prípravu a vývoj IKT stratégie primeraný povahe, rozsahu a zložitosti jej činností súvisiacich s IKT. Pri vykonávaní tohto hodnotenia by príslušné orgány mali zohľadniť:

    a. či sa vrcholový manažment [5] obchodnej línie (obchodných línií) primerane zapája do vymedzenia strategických priorít inštitúcie v oblasti IKT a či vrcholový manažment funkcie IKT má vedomosť o vývoji, plánovaní a zavedení hlavných obchodných stratégií a iniciatív na zabezpečenie nepretržitej podpory medzi IKT systémami, IKT službami a funkciou IKT (t. j. prvkami zodpovednými za riadenie a zavedenie týchto systémov a služieb) a obchodnou stratégiou inštitúcie, a či sa IKT účinne aktualizujú;

    b. či je stratégia IKT zdokumentovaná a podporená konkrétnymi implementačnými plánmi, najmä pokiaľ ide o dôležité medzníky a plánovanie zdrojov (vrátane finančných a ľudských zdrojov), aby boli tieto plány realistické a umožňovali plnenie stratégie IKT;

    c. či inštitúcia pravidelne aktualizuje svoju stratégiu IKT, najmä pri zmene obchodnej stratégie, aby sa zabezpečil nepretržitý súlad medzi IKT a strednodobými až dlhodobými obchodnými cieľmi, plánmi a činnosťami; a

    d. či riadiaci orgán inštitúcie schvaľuje stratégiu IKT, implementačné plány a či monitoruje jej plnenie.

2.2.2 Plnenie stratégie IKT

27. Ak je pre stratégiu IKT inštitúcie potrebné vykonať dôležité a komplexné zmeny IKT alebo zmeny s významnými dôsledkami pre obchodný model inštitúcie, príslušné orgány by mali posúdiť, či inštitúcia má kontrolný rámec primeraný jej veľkosti, jej činnostiam súvisiacich s IKT, ako aj úrovni činností súvisiacich so zmenami, ktorý slúži na podporu účinného plnenia stratégie IKT inštitúcie. Pri tomto posudzovaní by príslušné orgány mali zohľadniť, či v kontrolnom rámci:

    a. sú zahrnuté postupy riadenia (napr. monitorovanie pokroku a rozpočtu a podávanie správ o ňom) a príslušné subjekty (napr. oddelenie riadenia projektov, riadiaca skupina pre IKT alebo rovnocenná skupina) na účinnú podporu plnenia strategických programov IKT;

    b. boli vymedzené a pridelené úlohy a povinnosti týkajúce sa plnenia strategických programov IKT, pričom sa osobitná pozornosť venuje skúsenostiam kľúčových zainteresovaných strán pri organizovaní, riadení a monitorovaní významných a komplexných zmien IKT a riadeniu širších organizačných vplyvov a vplyvov na ľudí (napr. prekonávanie odporu proti zmene, odborná príprava, komunikácia);

[5] Vrcholový manažment a riadiaci orgán, ako sa vymedzujú v smernici 2013/36/EÚ z 26. júna 2013, „riadiaci orgán“ v článku 3 ods. 7 a „vrcholový manažment“ v článku 3 ods. 9.

c. sa zapája nezávislá funkcia kontroly a funkcia vnútorného auditu aby sa zabezpečilo, , že riziká spojené s plnením stratégie IKT sa identifikovali, posúdili a účinne zmiernili, a že rámec riadenia, určený vykonanie stratégie IKT, je účinný; a

d. je obsiahnuté plánovanie a postup preskúmania plánovania, ktorý umožňuje pružne reagovať na významné identifikované problémy (napr. problémy spojené s plnením alebo meškaním,) alebo externý vývoj (napr. významné zmeny podnikateľského prostredia, technologické problémy alebo inovácie) s cieľom zabezpečiť včasnú úpravu strategického implementačného plánu .

2.3 Celkové vnútorné riadenie

28. V súlade s hlavou 5 usmernení EBA o postupe SREP by príslušné orgány mali posúdiť, či inštitúcia má primeranú a transparentnú podnikovú štruktúru, ktorá je vhodná na daný účel, a či inštitúcia vykonala náležité opatrenia týkajúce sa riadenia. S osobitným zreteľom na IKT systémy a v súlade s usmerneniami EBA o vnútornom riadení by toto posúdenie malo obsahovať hodnotenie, či sa inštitúcia vyznačuje aspoň:

a. spoľahlivou a transparentnou organizačnou štruktúrou s jasne vymedzenými povinnosťami vo vzťahu k IKT vrátane riadiaceho orgánu a jeho výborov a tým, že kľúčové osoby zodpovedné za IKT (napr. vedúci pracovník v oblasti IT, výkonný riaditeľ alebo rovnocenná úloha) majú primeraný nepriamy alebo priamy prístup k riadiacemu orgánu s cieľom zabezpečiť, aby sa dôležité informácie alebo otázky týkajúce sa IKT primerane vykázali, prediskutovali a aby sa o nich rozhodlo na úrovni riadiaceho orgánu; a

b. tým, že riadiaci orgán pozná riziká spojené s IKT a zaoberá sa nimi.

29. Popri oddiele 5.2 usmernení EBA o postupe SREP by príslušné orgány mali posúdiť, či sa v politike a stratégii inštitúcie v oblasti outsourcingu IKT služieb v prípade potreby zohľadňuje vplyv outsourcingu IKT služieb na podnikanie inštitúcie a na jej obchodný model.

2.4 Riziko súvisiace s IKT v rámci riadenia rizík inštitúcie

30. Pri posudzovaní riadenia rizík a vnútornej kontroly celej inštitúcie, ako sa stanovuje v hlave 5 usmernení EBA o postupe SREP, by príslušné orgány mali posúdiť, či rámec riadenia rizík a vnútornej kontroly inštitúcie primerane ochraňuje IKT systémy inštitúcie spôsobom, ktorý je úmerný veľkosti a činnostiam inštitúcie a jej profilu z hľadiska rizika súvisiaceho s IKT, ako sa vymedzuje v hlave 3. Konkrétne by príslušné orgány mali určiť:

a. či sa ochota podstupovať riziká a postup hodnotenia primeranosti interného kapitálu vzťahujú na riziká súvisiace s IKT v rámci širšej kategórie operačného rizika v prípade vymedzenia celkovej stratégie riadenia rizík a určenia interného kapitálu; a

b. či riziká súvisiace s IKT patria do rozsahu pôsobnosti rámca pre riadenie rizík a vnútornú kontrolu celej inštitúcie.

31. Príslušné orgány by mali vykonať posúdenie podľa písmena a) so zreteľom na očakávané a nepriaznivé scenáre, napr. na scenáre zahrnuté v stresovom testovaní špecifickom pre inštitúciu alebo v stresovom testovaní orgánmi dohľadu.

32. S osobitným ohľadom na písmeno b) by príslušné orgány mali posúdiť, či je nezávislá funkcia kontroly a funkcia vnútorného auditu, ako sa podrobne uvádza v bode 104 písm. a) a d) a v bode 105 písm. a) a c) usmernení EBA o postupe SREP, vhodná na zabezpečenie dostatočnej úrovne nezávislosti medzi IKT a funkciami kontroly a auditu vzhľadom na veľkosť a profil inštitúcie z hľadiska rizika súvisiaceho s IKT.

2.5 Zhrnutie zistení

33. Tieto výsledky by sa mali odzrkadliť v zhrnutí zistení v hlave 5 usmernení EBA o postupe SREP a mali by tvoriť súčasť príslušného skóringového hodnotenia v súlade s kritériami v Tabuľke 3 usmernení EBA o postupe SREP.

34. Na posúdenie stratégie IKT by sa v záveroch uvedeného posúdenia mali zohľadniť tieto skutočnosti:

a. ak príslušné orgány dospeli k záveru, že rámec riadenia inštitúcie nie je vhodný na vypracovanie a plnenie stratégie inštitúcie v oblasti IKT podľa oddielu 2.2, tento záver by sa mal zohľadniť v hodnotení vnútorného riadenia inštitúcie podľa bodu 87 písm. a) v hlave 5 usmernení EBA o postupe SREP;

b. ak príslušné orgány na základe posudzovania podľa oddielu 2.2 dospeli k záveru, že medzi stratégiou IKT a obchodnou stratégiou je značný nesúlad, ktorý môže mať významný nepriaznivý vplyv na dlhodobé obchodné a/alebo finančné ciele inštitúcie, udržateľnosť a/alebo obchodný model inštitúcie alebo na obchodné oblasti/obchodné línie inštitúcie, ktoré boli podľa bodu 62 písm. a) usmernení EBA o postupe SREP určené ako najvýznamnejšie, tento záver by sa mal zohľadniť v hodnotení obchodného modelu podľa bodu 70 písm. b) a c) v hlave 4 usmernení o postupe SREP; a

c. ak príslušné orgány na základe posudzovania podľa oddielu 2.2 dospeli k záveru, že inštitúcia nemôže mať dostatočné zdroje a realizačné kapacity v oblasti IKT na vykonanie a podporu významných plánovaných strategických zmien, tento záver by sa mal zohľadniť v hodnotení obchodného modelu podľa bodu 70 písm. b) v hlave 4 usmernení EBA o postupe SREP.

Hlava 3 – Posúdenie expozícií inštitúcií voči rizikám súvisiacim s IKT a kontrol týchto rizík

3.1 Všeobecné aspekty

35. Príslušné orgány by mali posúdiť, či inštitúcia riadne identifikovala, posúdila a zmiernila svoje riziká súvisiace s IKT. Tento postup by mal byť súčasťou rámca riadenia operačného rizika a mal by byť zhodný s prístupom uplatňovaným na operačné riziko.

36. Príslušné orgány by najprv mali určiť významné inherentné riziká súvisiace s IKT, ktorým je alebo ktorým by mohla byť inštitúcia vystavená, na základe čoho by sa potom uskutočnilo posúdenie účinnosti riadenia rizík inštitúcie súvisiacich s IKT, postupov a kontrol na zmiernenie týchto rizík. Výsledok posúdenia by sa mal odzrkadliť v zhrnutí zistení, ktoré sa použije ako vstupné údaje pre skóringové hodnotenie operačného rizika podľa usmernení EBA o postupe SREP. Ak sa riziko súvisiace s IKT považuje za významné a príslušné orgány by chceli priradiť samostatné skóringové hodnotenie, potom by sa na priradenie skóringové hodnotenia ako podrizika operačného rizika mala použiť Tabuľka 1.

37. Pri vykonávaní posúdenia podľa tejto hlavy by príslušné orgány ako základ na určenie svojich priorít pri posudzovaní orgánmi dohľadu mali použiť všetky dostupné zdroje informácií, ako sa uvádza v bode 127 hlavy 6 usmernení EBA o postupe SREP, napr. činnosti, správy a výsledky v rámci riadenia rizík inštitúcie. Príslušné orgány by na vykonanie tohto posúdenia mali použiť aj iné zdroje informácií vrátane týchto zdrojov informácií (ak sú relevantné):

    a. posúdenie vlastného rizika a kontrol súvisiacich s IKT (ak bolo uvedené medzi informáciami z postupu ICAAP);
    b. informácie o riadení spojené s rizikom súvisiacim s IKT predložené riadiacemu orgánu inštitúcie, napr. pravidelné a na udalostiach založené podávanie správ o rizikách súvisiacich s IKT (vrátane podávania správ do databázy operačných strát), údaje o expozícii rizikám súvisiacim s IKT z funkcie riadenia rizík inštitúcie;
    c. zistenia vnútorného a externého auditu súvisiacich s IKT, ktoré boli oznámené výboru inštitúcie pre audit.

3.2 Identifikácia významných rizík súvisiacich s IKT

38. Príslušné orgány by mali určiť významné riziká súvisiace s IKT, ktorým je alebo ktorým by mohla byť vystavená inštitúcia, podľa krokov uvedených ďalej.

3.2.1 Preskúmanie profilu inštitúcie z hľadiska rizika súvisiaceho s IKT

39. Pri preskúmavaní profilu inštitúcie z hľadiska rizika súvisiaceho s IKT by príslušné orgány mali zohľadniť všetky relevantné informácie o expozíciách inštitúcie rizikám súvisiacim s IKT vrátane informácií v bode 37 a zistené významné nedostatky alebo slabiny organizácie IKT a kontrol celej inštitúcie podľa hlavy 2

týchto usmernení a v prípade potreby tieto informácie primeraným spôsobom preskúmať. V rámci tohto preskúmania by príslušné orgány mali zohľadniť:

a. potenciálny vplyv závažného narušenia IKT systémov inštitúcie na finančný systém buď na domácej, alebo na medzinárodnej úrovni;
b. či inštitúcia môže podliehať rizikám súvisiacim s bezpečnosťou IKT alebo rizikám súvisiacim s dostupnosťou a kontinuitou IKT z dôvodu závislosti od internetu, vysokej miery prijímania inovačných IKT riešení alebo iných obchodných distribučných reťazcov, ktoré môžu zvýšiť pravdepodobnosť, že inštitúcia sa stane cieľom pre kybernetické útoky;
c. či inštitúcia môže byť viac vystavená rizikám súvisiacim s bezpečnosťou IKT, rizikám súvisiacim s dostupnosťou a kontinuitou IKT, rizikám súvisiacim s integritou IKT údajov alebo rizikám súvisiacim so zmenou IKT z dôvodu zložitosti (napr. v dôsledku zlúčení alebo nadobudnutí) alebo zastaranej povahy jej IKT systémov;
d. či inštitúcia významne mení svoje IKT systémy a/alebo funkcie IKT (napr. v dôsledku zlúčení, nadobudnutí, odčlenení alebo výmeny jej kľúčových IKT systémov), čo môže nepriaznivo postihnúť stabilitu alebo riadne fungovanie IKT systémov a spôsobiť významné riziká súvisiace s dostupnosťou a kontinuitou IKT, riziká súvisiace s bezpečnosťou IKT, riziká súvisiace so zmenou IKT alebo riziká súvisiace s integritou IKT údajov;
e. či inštitúcia outsourcovala IKT služby alebo IKT systémy externým poskytovateľom v rámci vlastnej finančnej skupiny alebo mimo nej, čím by sa mohla vystaviť významným rizikám súvisiacim s externým zabezpečovaním IKT služieb;
f. či inštitúcia vykonáva agresívne úsporné opatrenia týkajúce sa IKT, čo môže viesť k zníženiu potrebných investícií, zdrojov a odbornosti v oblasti IKT a k zvýšeniu expozície všetkým druhom rizík súvisiacich s IKT v rámci taxonómie;
g. či poloha dôležitých prevádzok IKT/dátových stredísk (napr. regióny, krajiny) môže vystaviť inštitúciu prírodným katastrofám (napr. povodne, zemetrasenia), politickej nestabilite alebo pracovnoprávnym konfliktom a občianskym nepokojom, ktoré by mohli viesť k významnému zvýšeniu rizík súvisiacich s dostupnosťou a kontinuitou IKT a rizík súvisiacich s bezpečnosťou IKT.

3.2.2 Preskúmanie kritických IKT systémov a služieb

40. V rámci procesu identifikácie rizík súvisiacich s IKT s potenciálne závažným prudenciálnym vplyvom na inštitúciu by príslušné orgány mali preskúmať dokumentáciu inštitúcie a vypracovať stanovisko o tom, ktoré IKT systémy a služby sú kritické pre primerané fungovanie, dostupnosť, kontinuitu a bezpečnosť základných činností inštitúcie.

41. Na tento účel by príslušné orgány mali preskúmať metodiku a postupy uplatňované inštitúciou na identifikáciu IKT systémov a služieb, ktoré sú kritické, pričom by mali vziať ohľad na to, že inštitúcia môže niektoré IKT systémy a služby považovať za kritické z hľadiska kontinuity činností a dostupnosti, z hľadiska bezpečnosti (napr. predchádzanie podvodom) a/alebo z hľadiska dôvernosti (napr. dôverné údaje). Príslušné orgány by mali vykonať s ohľadom na to, že kritické IKT systémy a služby by mali spĺňať aspoň jednu z týchto podmienok:

a. podporujú hlavné obchodné operácie a distribučné reťazce (napr. bankomaty, elektronické a mobilné bankovníctvo) inštitúcie;

b. podporujú základné postupy riadenia a podnikové funkcie vrátane riadenia rizík (napr. systémy riadenia rizík a správy pokladnice);

c. vzťahujú sa na ne osobitné právne alebo regulatórne požiadavky (pokiaľ existujú), ktorými sa ukladajú silnejšie požiadavky na dostupnosť, odolnosť, dôvernosť alebo bezpečnosť [napr. právne predpisy v oblasti ochrany osobných údajov alebo možné časové ciele obnovy (RTO, maximálny čas, v rámci ktorého musí po udalosti nastať obnova systému alebo postupu) a ciele bodov obnovy (RPO, maximálne časové obdobie, počas ktorého môže v prípade udalosti dôjsť k strate údajov)] pre niektoré systémovo dôležité služby (v náležitých prípadoch);

d. slúžia na spracovanie alebo uchovanie dôverných alebo citlivých údajov, pri ktorých by neoprávnený prístup mohol vážne poškodiť dobrú povesť inštitúcie, finančné výsledky alebo zdravie a kontinuitu jej činnosti (napr. databázy s citlivými údajmi o klientoch); a/alebo

e. poskytujú základné funkcie, ktoré sú nevyhnutné pre primerané fungovanie inštitúcie (napr. telekomunikačné služby a služby prepojiteľnosti, služby bezpečnosti IKT a kybernetickej bezpečnosti).

3.2.3 Identifikácia významných rizík súvisiacich s IKT pre kritické IKT systémy a služby

42. Vzhľadom na vykonané preskúmania profilu inštitúcie z hľadiska rizika súvisiaceho s IKT a kritických IKT systémov a služieb uvedené vyššie by príslušné orgány mali vypracovať stanovisko o významných rizikách súvisiacich s IKT, ktoré podľa ich úsudku pri výkone dohľadu, môžu mať významný prudenciálny vplyv na kritické IKT systémy a služby inštitúcie.

43. Pri posudzovaní možného vplyvu rizík súvisiacich s IKT na kritické IKT systémy a služby inštitúcie by príslušné orgány mali zohľadniť:

a. finančný vplyv vrátane (okrem iného) straty finančných prostriedkov alebo aktív, možnej kompenzácie zákazníkovi, právnych nákladov a nákladov na nápravu, zodpovednosti za zmluvné škody, straty príjmov;

b. možnosť narušenia obchodnej činnosti vzhľadom na (okrem iného) kritickosť dotknutých finančných služieb; počet zákazníkov a/alebo pobočiek a zamestnancov, ktorých sa riziká potenciálne dotýkajú;

c. možný vplyv na dobrú povesť inštitúcie na základe kritickosti dotknutých bankových služieb alebo prevádzkovej činnosti (napr. krádež údajov zákazníkov); externý profil/viditeľnosť dotknutých IKT systémov a služieb (napr. systémy mobilného alebo elektronického bankovníctva, platobné terminály v mieste predaja, bankomaty alebo platobné systémy);

d. regulačný vplyv vrátane možnosti verejnej kritiky regulačným orgánom, pokút, či dokonca zmeny povolení;

e. strategický vplyv na inštitúciu, napríklad v prípade, keď dôjde k vyzradeniu alebo krádeži strategického produktu alebo obchodných plánov.

44. Príslušné orgány by potom mali premietnuť zistené riziká súvisiace s IKT, ktoré sa považujú za významné, do týchto kategórií rizík súvisiacich s IKT, pre ktoré sa v prílohe uvádzajú doplňujúce opisy rizika a príklady. Príslušné orgány by v rámci posudzovania podľa hlavy 3 mali zohľadniť riziká súvisiace s IKT uvedené v prílohe:

    a. riziko súvisiace s dostupnosťou a kontinuitou IKT;
    b. riziko súvisiace s bezpečnosťou IKT;
    c. riziko súvisiace so zmenou IKT;
    d. riziko súvisiace s integritou IKT údajov;
    e. riziko súvisiace s oustourcingom IKT služieb.

    Priradenie rizík do kategórií má príslušným orgánom pomôcť pri určovaní, ktoré riziká sú významné (pokiaľ také existujú), a preto by malo podliehať užšiemu a/alebo dôkladnejšiemu preskúmaniu v týchto krokoch posudzovania.

3.3 Posudzovanie kontrol na zmiernenie významných rizík súvisiacich s IKT

45. Na posúdenie expozície inštitúcie reziduálnemu riziku súvisiacemu s IKT by príslušné orgány mali preskúmať spôsob, akým inštitúcia identifikuje, monitoruje, posudzuje a zmierňuje významné riziká zistené príslušnými orgánmi pri spomínanom posudzovaní.

46. Príslušné orgány by na tento účel v prípade zistených významných rizík súvisiacich s IKT mali preskúmať platné:

    a. politiky a procesy riadenia rizík súvisiacich s IKT a prahové hodnoty tolerancie rizika;
    b. rámec organizačného riadenia a dohľadu;
    c. rozsah a zistenia vnútorného auditu; a
    d. kontroly rizík súvisiacich s IKT, ktoré sú vlastné pre zistené významné riziko súvisiace s IKT.

47. V posúdení by sa mal zohľadniť výsledok analýzy celkového rámca riadenia rizík a vnútornej kontroly, ako sa uvádza v hlave 5 usmernení EBA o postupe SREP, ako aj riadenie a stratégia inštitúcie, ktorými sa zaoberá hlava 2 týchto usmernení, keďže závažné nedostatky zistené v týchto oblastiach môžu ovplyvniť schopnosť inštitúcie zvládnuť a zmierniť jej expozície rizikám súvisiacim s IKT. V náležitých prípadoch by príslušné orgány mali využiť aj zdroje informácií uvedené v bode 37 týchto usmernení.

48. Príslušné orgány by tieto kroky posudzovania mali vykonať spôsobom, ktorý bude primeraný povahe, rozsahu a zložitosti činností inštitúcie, a uplatnením preskúmania orgánmi dohľadu, ktoré je vhodné pre profil inštitúcie z hľadiska rizika súvisiaceho s IKT.

3.3.1 Politika a procesy riadenia rizík súvisiacich s IKT a prahové hodnoty tolerancie rizika

49. Príslušné orgány by mali preskúmať, či inštitúcia má vhodné politiky a procesy riadenia rizík a prahové hodnoty tolerancie rizika pre zistené významné riziká súvisiace s IKT. Môžu byť súčasťou rámca riadenia

operačného rizika alebo môže ísť o samostatný dokument. Príslušné orgány by na účely tohto posúdenia mali zohľadniť:

a. či politika riadenia rizík bola potvrdená a schválená riadiacim orgánom a či obsahuje dostatočné usmernenia rizikový apetít inštitúcie súvisiaci IKT a pre hlavné sledované ciele riadenia rizík súvisiacich s IKT a/alebo použité prahové hodnoty tolerancie rizika súvisiaceho s IKT. Príslušná politika riadenia rizík súvisiacich s IKT by sa takisto mala oznámiť všetkým dotknutým zainteresovaným stranám;

b. či sa platná politika pokrýva všetky významné prvky riadenia rizík v rámci zistených významných rizík súvisiacich s IKT;

c. či inštitúcia implementovala proces a súvisiace postupy na identifikáciu (napr. vlastné hodnotenia rizík a kontrol, analýzu rizikového scenára) a monitorovanie príslušných významných rizík súvisiacich s IKT; a

d. či inštitúcia zaviedla postupy monitoringu a rizík súvisiacich s IKT, ktorý poskytuje včas informácie pre vrcholový manažment a riadiaci orgán a ktorý vrcholovému manažmentu a/alebo riadiacemu orgánu umožňuje posúdiť a monitorovať, či sú plány a opatrenia inštitúcie na zmiernenie rizika súvisiaceho s IKT v súlade so schváleným rizikovým apetítom a/alebo toleranciou rizika (v prípade potreby), a monitoruje zmeny významných rizík súvisiacich s IKT.

3.3.2 Rámec organizačného riadenia a dohľadu

50. Príslušné orgány by mali posúdiť, akým spôsobom sú uplatniteľné úlohy a zodpovednosti riadenia rizík zakotvené a začlenené do vnútornej organizácie na riadenie zistených významných rizík súvisiacich s IKT a dohľad nad nimi. V tejto súvislosti by príslušné orgány mali posúdiť, či inštitúcia vykazuje:

a. jasné úlohy a povinnosti týkajúce sa identifikácie, posudzovania, monitorovania, zmierňovania príslušných významných rizík súvisiacich s IKT, podávania správ o nich a dohľadu nad nimi;

b. že povinnosti a úlohy týkajúce sa rizika sú jasne oznamované, rozdeľované a začleňované vo všetkých príslušných častiach (napr. obchodné línie, IT) a procesoch organizácie vrátane úloh a povinností týkajúcich sa získavania a zhromažďovania informácií o riziku a podávania správ o týchto informáciách vrcholovému manažmentu a/alebo riadiacemu orgánu;

c. že činnosti spojené s riadením rizík súvisiacich s IKT sa vykonávajú s dostatočnými a kvalitatívne primeranými ľudskými a technickými zdrojmi. Príslušné orgány by na účely posúdenia dôveryhodnosti platných plánov na zmiernenie rizika mali posúdiť aj to, či inštitúcia pridelila dostatočný finančný rozpočet a/alebo iné požadované zdroje na ich realizáciu;

d. primeranú následnú kontrolu a reakciu riadiaceho orgánu v súvislosti s dôležitými zisteniami pochádzajúcimi z nezávislých kontrolných funkcií, pokiaľ ide o riziká súvisiace s IKT, pričom sa zohľadňuje možnosť delegovania určitých aspektov na výbor, ak tento výbor existuje; a

e. že výnimky z platných predpisov a politík týkajúcich sa IKT sa zaznamenajú a nezávislá kontrolná funkcia vypracuje zdokumentované stanovisko a podá o nich správu so zameraním na súvisiace riziká.

3.3.3 Rozsah a zistenia vnútorného auditu

51. Príslušné orgány by mali posúdiť, či je funkcia vnútorného auditu efektívna vzhľadom na vykonávanie auditu platného rámca kontroly rizík súvisiacich s IKT, a to tak, že preskúmajú:

    a. či sa audity rámca kontroly rizík súvisiacich s IKT vykonávajú v požadovanej kvalite, hĺbke a frekvencii a či sú úmerné veľkosti, činnostiam a profilu inštitúcie z hľadiska rizika súvisiaceho s IKT;

    b. či súčasťou plánu auditu sú audity zamerané na kritické riziká súvisiace s IKT identifikované inštitúciou;

    c. či sa dôležité zistenia auditu v oblasti IKT vrátane dohodnutých opatrení vykazujú riadiacemu orgánu; a

    d. či zistenia auditu v oblasti IKT vrátane dohodnutých nápravných opatrení kontrolujú po skončení auditu a či vrcholový manažment a/alebo výbor pre audit pravidelne preskúmavajú správy o nápravných opatreniach.

3.3.4 Kontroly rizík súvisiacich s IKT, ktoré sú vlastné pre identifikované významné riziká súvisiace s IKT

52. Príslušné orgány by v prípade identifikovaných významných rizík súvisiacich s IKT mali posúdiť, či inštitúcia zaviedla konkrétne kontroly na riešenie týchto rizík. V nasledujúcich oddieloch sa uvádza neúplný zoznam konkrétnych kontrol, ktoré sa majú zohľadniť pri posudzovaní významných rizík zistených v oddiele 3.2.2, ktoré boli priradené k týmto kategóriám rizík súvisiacich s IKT:

    a. riziká súvisiace s dostupnosťou a kontinuitou IKT;
    b. riziká súvisiace s bezpečnosťou IKT;
    c. riziká súvisiace so zmenou IKT;
    d. riziká súvisiace s integritou IKT údajov;
    e. riziká súvisiace s outsourcingom IKT služieb.

(a) Kontroly na riadenie významných rizík súvisiacich s dostupnosťou a kontinuitou IKT

53. Okrem požiadaviek v usmerneniach EBA o postupe SREP (body 279 – 281) by príslušné orgány mali posúdiť, či má inštitúcia vhodný rámec na identifikáciu, meranie a zmiernenie rizík súvisiacich s dostupnosťou a kontinuitou IKT a na porozumenie týmto rizikám.

54. Príslušné orgány by na účely tohto posúdenia mali konkrétne zohľadniť, či tento rámec:

    a. identifikuje kritické procesy týkajúce sa IKT a príslušné podporné IKT systémy, ktoré by mali byť súčasťou plánov na zabezpečenie odolnosti a kontinuity činností pomocou:

        i. komplexnej analýzy závislostí medzi kritickými podnikateľskými postupmi a podpornými systémami;

        ii. určenia cieľov obnovy pre podporné IKT systémy (napr. za normálnych okolností určených podnikom a/alebo na základe právnych predpisov z hľadiska časových cieľov obnovy a cieľov bodov obnovy);

iii. vhodného pohotovostného plánovania s cieľom umožniť dostupnosť, kontinuitu a obnovenie kritických IKT systémov a služieb na minimalizáciu narušenia operácií inštitúcie v rámci prijateľných obmedzení;

b. má politiky a štandardy týkajúce sa kontrolného prostredia pre odolnosť a kontinuitu činností a operatívne kontroly, ktoré zahŕňajú:

i. opatrenia, ktorých účelom je zabrániť tomu, aby jeden scenár, udalosť alebo katastrofa mohli ovplyvniť systémy produkcie a obnovenia IKT;

ii. postupy zálohovania a obnovenia IKT systému týkajúce sa kritického softvéru a dát, prostredníctvom ktorých sa zabezpečí, aby sa tieto zálohy archivovali na bezpečnom a dostatočne vzdialenom mieste, aby v prípade nehody alebo katastrofy nedošlo k zničeniu alebo poškodeniu týchto kritických dát;

iii. riešenia v oblasti monitorovania na včasné odhalenie udalostí súvisiacich s dostupnosťou a kontinuitou IKT;

iv. zdokumentovaný postup riadenia a eskalácie udalosti, ktorý obsahuje aj usmernenie o rôznych úlohách a povinnostiach súvisiacich s riadením a eskaláciou udalosti, o členoch krízových výborov a hierarchii velenia v prípade núdze;

v. fyzikálne opatrenia na ochranu kritickej IKT infraštruktúry inštitúcie (napr. dátové strediská) pred environmentálnymi rizikami (napr. povodne a iné prírodné katastrofy), ako aj na zabezpečenie vhodného prevádzkového prostredia pre IKT systémy (napr. klimatizácia);

vi. postupy, úlohy a povinnosti na zabezpečenie, aby sa aj na IKT systémy a služby outsourcované externým poskytovateľom vzťahovali primerané riešenia a plány na zabezpečenie odolnosti a kontinuity;

vii. riešenia v oblasti plánovania výkonnosti a kapacity IKT a v oblasti monitorovania pre kritické IKT systémy a služby so stanovenými požiadavkami na dostupnosť, aby bolo možné včas odhaliť závažné obmedzenia týkajúce sa výkonnosti a kapacity;

viii. v prípade nevyhnutnosti a potreby riešenia na ochranu kritických internetových činností alebo služieb (napr. služby elektronického bankovníctva) proti odmietnutiu služby a ďalším kybernetickým útokom z internetu, ktoré sú zamerané na zabránenie alebo narušenie prístupu k týmto činnostiam a službám;

c. testuje riešenia týkajúce sa dostupnosti a kontinuity IKT v porovnaní s množstvom realistických scenárov vrátane kybernetických útokov, testov prechodu a záloh kritického softvéru a dát:

i. ktoré sú plánované, potvrdené a zdokumentované, a výsledky testov sa používajú na posilnenie účinnosti riešení súvisiacich s dostupnosťou a kontinuitou IKT;

ii. ktoré zahŕňajú zainteresované strany a funkcie v rámci organizácii, ako je manažment obchodnej línie vrátane skupín pre kontinuitu činností, udalosti a reakciu na krízu, ako aj príslušné externé zainteresované strany v ekosystéme;

iii. v rámci ktorých riadiaci orgán a vrcholový manažment sú primerane zapojené (napr. ako súčasť skupín na krízové riadenie) a v rámci ktorých dostávajú informácie o výsledkoch testov.

(b) Kontroly na riadenie významných rizík súvisiacich s bezpečnosťou IKT

55. Príslušné orgány by mali posúdiť, či inštitúcia má účinný rámec na identifikáciu, meranie a zmiernenie rizík súvisiacich s bezpečnosťou IKT a na porozumenie týmto rizikám. Príslušné orgány by na účely tohto hodnotenia mali konkrétne posúdiť, či sa v tomto rámci zohľadňujú:

a. jasne vymedzené úlohy a povinnosti týkajúce sa:
   i. osôb a/alebo výborov, ktoré nesú zodpovednosť za každodenné riadenie bezpečnosti IKT a za vypracovanie spoločných politík bezpečnosti IKT, pričom je pozornosť zameraná na ich potrebnú nezávislosť;
   ii. návrhu, vykonávania, riadenia a monitorovania kontrol bezpečnosti IKT;
   iii. ochrany kritických IKT systémov a služieb napríklad prostredníctvom postupov posúdenia zraniteľnosti, správy softvérových opráv, ochrany koncového používateľa (napr. malvérový vírus), nástrojov na odhaľovanie neoprávnených vniknutí a ich zabraňovanie;
   iv. monitorovania, klasifikácie a spracovania vonkajších alebo vnútorných udalostí súvisiacich s bezpečnosťou IKT; vrátane reakcie na udalosť a kontinuity a obnovy IKT systémov a služieb;
   v. pravidelného a proaktívneho posudzovania hrozieb na zachovanie primeraných kontrol bezpečnosti;

b. politika bezpečnosti IKT, v ktorej sa zohľadňujú a v prípade potreby dodržiavajú medzinárodne uznávané normy bezpečnosti IKT a zásady bezpečnosti (napr. tzv. zásada najnižších práv, t. j. obmedzenie prístupu na minimálnu úroveň, ktorá umožní normálne fungovanie správy prístupových práv, a zásada tzv. ochrany do hĺbky, t. j. vrstvené bezpečnostné mechanizmy na zvýšenie bezpečnosti systému ako celku pre vytvorenie bezpečnostnej architektúry);

c. postupy na identifikáciu IKT systémov, služieb a primeraných bezpečnostných požiadaviek, v ktorých sa odzrkadľuje možné riziko podvodu a/alebo prípadné nesprávne použitie a/alebo zneužitie dôverných údajov popri zdokumentovaných bezpečnostných očakávaniach, ktoré sa majú v prípade týchto zistených IKT systémov, služieb a údajov dodržiavať, zosúladiť s toleranciou rizika inštitúcie a monitorovať v súvislosti s ich správnym vykonávaním;

d. zdokumentovaný postup riadenia a eskalácie bezpečnostnej udalosti, ktorý obsahuje aj usmernenie o rôznych úlohách a povinnostiach súvisiacich s riadením a eskaláciou udalosti, o členoch krízových výborov a hierarchii velenia v prípade bezpečnostnej pohotovosti;

e. zaznamenávanie činnosti používateľom a administrátorom s cieľom umožniť efektívne monitorovanie a včasné odhalenie neoprávnenej činnosti a reakciu na túto činnosť; s cieľom pomôcť pri vykonávaní forenzného vyšetrovania bezpečnostných udalostí. Inštitúcia by mala mať politiky zaznamenávania, v ktorých sa vymedzujú vhodné druhy denníkov, ktoré sa majú viesť, a obdobie ich uchovávania;

f. osvetové a informačné kampane alebo iniciatívy na informovanie všetkých úrovní v inštitúcii o bezpečnom používaní a ochrane IKT systémov inštitúcie a hlavné riziká súvisiace s bezpečnosťou IKT (a iné riziká), o ktorých by mali byť informované, najmä pokiaľ ide o existujúce a vyvíjajúce sa počítačové hrozby (napr. počítačové vírusy, možné vnútorné alebo vonkajšie zneužitia alebo útoky, kybernetické útoky), a ich úlohu pri zmierňovaní narušenia bezpečnosti;

g. primerané fyzické bezpečnostné opatrenia (napr. kamerový systém, poplašný systém proti vlámaniu, bezpečnostné dvere) na zabránenie neoprávnenému fyzickému prístupu ku kritickým a citlivým IKT systémom (napr. k dátovým strediskám);

h. opatrenia na ochranu IKT systémov pred útokmi z internetu (t. j. pred kybernetickými útokmi) alebo z iných vonkajších sietí (napr. tradičné telekomunikačné prepojenia alebo prepojenia s dôveryhodnými partnermi). Príslušné orgány by mali preskúmať, či rámec inštitúcie zohľadňuje:

   i. proces a riešenia na zachovanie úplného a aktuálneho zoznamu a prehľadu všetkých miest pripojenia k sieti smerujúcich z organizácie (napr. webové sídla, internetové aplikácie, WIFI, vzdialený prístup), prostredníctvom ktorých by tretie strany mohli preniknúť do interných IKT systémov;

   ii. úzko riadené a monitorované bezpečnostné opatrenia (napr. firewally, proxy servery, prenosy poštových správ, antivírusové programy a prehliadače obsahu) na zabezpečenie prichádzajúcej a odchádzajúcej sieťovej prevádzky (napr. elektronická pošta) a sieťových pripojení smerujúcich von, prostredníctvom ktorých by tretie strany mohli preniknúť do interných IKT systémov;

   iii. postupy a riešenia na zabezpečenie webových sídel a aplikácií, na ktoré môže byť podniknutý priamy útok z internetu a/alebo zvonku a ktoré môžu poslúžiť ako miesto vstupu do interných IKT systémov. Vo všeobecnosti medzi tieto postupy a riešenia patrí kombinácia uznávaných bezpečných vývojových postupov, spevnenia IKT systému a postupov na pozorné vyhľadávanie zraniteľností a/alebo vykonávanie doplňujúcich bezpečnostných riešení, ako napríklad použitie firewallov a/alebo systémov na odhaľovanie neoprávnených prienikov a/alebo na zabránenie týmto prienikom;

   iv. pravidelné bezpečnostné penetračné testy na posúdenie účinnosti realizovaných počítačových a interných opatrení a postupov v oblasti bezpečnosti IKT. Tieto testy by mali vykonávať zamestnanci a/alebo externí experti s potrebnými odbornými znalosťami a zdokumentované výsledky a závery testov by sa mali oznámiť vrcholovému manažmentu a/alebo riadiacemu orgánu. V prípade potreby by sa inštitúcia mala z týchto testov poučiť, kde by mohla ešte zlepšiť bezpečnostné kontroly a postupy a/alebo získať lepšiu istota o ich účinnosti.

(c) Kontroly na riadenie významných rizík súvisiacich so zmenou IKT

56. Príslušné orgány by mali posúdiť, či inštitúcia má účinný rámec na identifikáciu, meranie a zmiernenie rizík súvisiacich so zmenou IKT a na porozumenie týmto rizikám, ktoré sú úmerné povahe, rozsahu a zložitosti činností inštitúcie a jej profilu z hľadiska rizika súvisiaceho s IKT. Rámec inštitúcie by sa mal vzťahovať na riziká spojené s vývojom, testovaním a schvaľovaním zmien IKT systémov vrátane vývoja alebo zmeny softvéru predtým, než sa prenesie do produkčného prostredia, a mal by zabezpečovať

primerané riadenie životného cyklu IKT. Príslušné orgány by na účely tohto posúdenia mali konkrétne posúdiť, či sa v tomto rámci zohľadňujú:

a. zdokumentované procesy na riadenie a kontrolu zmien IKT systémov (napr. konfigurácia a správa opráv) a dát (napr. oprava chýb alebo opravy dát), pričom sa zabezpečuje primerané zapojenie riadenia rizík súvisiacich s IKT do dôležitých zmien IKT, ktoré môžu významne postihnúť rizikový profil alebo expozíciu inštitúcie;

b. špecifikácie týkajúce sa požadovaného oddelenia funkcií počas rôznych fáz vykonávaných postupov zmien IKT (napr. návrh a vývoj riešenia, testovanie a schválenie nového softvéru a/alebo zmeny, presun a vykonávanie v rámci produkčného prostredia a oprava chýb) so zameraním na vykonávané riešenia a oddelenie funkcií riadenia a kontroly zmien výroby IKT systémov a dát zamestnancami IKT (napr. programátori, správcovia IKT systému, správcovia databáz) alebo inou stranou (napr. obchodní používatelia, poskytovatelia služieb);

c. testovacie prostredia, ktoré primerane odzrkadľujú produkčné prostredia;

d. zoznam aktív existujúcich aplikácií a IKT systémov vo produkčnom prostredí, ako aj v skúšobnom a vývojovom prostredí, aby sa požadované zmeny (napr. aktualizácie alebo modernizácie verzií, opravy systémov, zmeny konfigurácie) mohli v prípade dotknutých IKT systémov riadne spravovať, realizovať a monitorovať;

e. proces na monitorovanie a riadenie životného cyklu použitých IKT systémov, na zabezpečenie, aby naďalej spĺňali a podporovali aktuálne hospodárske požiadavky a požiadavky riadenia rizík, a na zabezpečenie, že použité IKT riešenia a systémy ich predajcovia stále podporujú; a že tento proces dopĺňajú primerané postupy životného cyklu vývoja softvéru;

f. kontrolný systém zdrojového kódu softvéru a vhodné postupy na zabránenie neoprávneným zmenám v zdrojovom kóde softvéru, ktorý sa vyvíja interne;

g. proces na vykonanie bezpečnostného vyšetrovania a overenia zraniteľnosti nových alebo významne upravených IKT systémov a softvéru pred ich uvedením do výroby a pred ich vystavením možným kybernetickým útokom;

h. proces a riešenia na zabránenie neoprávneného alebo neúmyselného zverejnenia dôverných údajov pri výmene, archivácii, vyraďovaní alebo likvidácii IKT systémov;

i. postupy nezávislého preskúmania a potvrdenia na zníženie rizík ľudských chýb pri vykonávaní zmien IKT systémov, ktoré môžu mať závažný nežiaduci účinok na dostupnosť, kontinuitu alebo bezpečnosť inštitúcie (napr. významné zmeny v konfigurácii firewallu) alebo na bezpečnosť inštitúcie (napr. zmeny firewallu).

(d) Kontroly na riadenie významných rizík súvisiacich s integritou IKT údajov

57. Príslušné orgány by mali posúdiť, či inštitúcia má účinný rámec na identifikáciu, meranie a zmiernenie rizík súvisiacich s integritou IKT údajov a na porozumenie týmto rizikám, ktoré sú úmerné povahe, rozsahu a zložitosti činností inštitúcie a jej profilu z hľadiska rizika súvisiaceho s IKT. Rámec inštitúcie by mal zohľadňovať riziká spojené so zachovaním integrity údajov uložených a spracúvaných IKT systémami. Príslušné orgány by na účely tohto posúdenia mali konkrétne posúdiť, či sa v tomto rámci zohľadňujú:

    a. politika, ktorou sa vymedzujú úlohy a povinnosti na riadenie integrity údajov v IKT systémoch (napr. dátový architekt, dátoví referenti[6], opatrovníci dát[7], vlastníci/správcovia dát[8]) a ktorá poskytuje usmernenia o tom, ktoré údaje sú kľúčové z hľadiska integrity údajov a mali by podliehať osobitným kontrolám IKT (napr. automatizované kontroly vstupných parametrov, kontroly prenosu údajov, zosúlaďovanie atď.) alebo preskúmaniam (napr. kontrola kompatibility s dátovou architektúrou) v rôznych fázach životného cyklu údajov IKT;

    b. zdokumentovaná dátová architektúra, dátový model a/alebo slovník, ktoré potvrdzujú príslušné obchodné zainteresované strany a zainteresované strany v oblasti IT na účely podpory potrebnej súdržnosti údajov vo všetkých IKT systémoch a na uistenie sa, že dátová architektúra, dátový model a/alebo slovník ostanú v súlade s potrebami v oblasti obchodovania a riadenia rizík;

    c. politika týkajúca sa povoleného použitia spracovania údajov koncového používateľa, najmä pokiaľ ide o identifikáciu, registráciu a zdokumentovanie významných riešení spracovania údajov koncového používateľa (napr. pri spracovaní dôležitých údajov), a predpokladaných úrovní bezpečnosti na zabránenie neoprávneným úpravám samotného nástroja, ako aj údajov v ňom uložených;

    d. zdokumentované postupy spracovania výnimiek na riešenie zistených problémov týkajúcich sa integrity IKT údajov v súlade s ich kritickosťou a citlivosťou.

58. V prípade inštitúcií podliehajúcich dohľadu, ktoré patria do rozsahu pôsobnosti zásad BCBS 239 pre účinné zhromažďovanie údajov o rizikách a podávanie správ o riziku[9], by príslušné orgány mali preskúmať analýzu rizík inštitúcie týkajúcu sa jej podávania správ o rizikách a schopností zhromažďovať údaje v porovnaní s týmito zásadami a s vypracovanou dokumentáciou na túto tému, pričom zohľadnia implementačný harmonogram a prechodné opatrenia v týchto zásadách.

[6] Dátový referent zodpovedá za spracovanie a použitie údajov.

[7] Opatrovník dát zodpovedá za bezpečnú úschovu, prepravu a uloženie údajov.

[8] Správca dát zodpovedá za riadenie a vhodnosť dátových prvkov – obsahu, ako aj metaúdajov.

[9] Bazilejský výbor pre bankový dohľad, Zásady pre účinné zhromažďovanie údajov o rizikách a podávanie správ o rizikách, január 2013, k dispozícii on-line: http://www.bis.org/publ/bcbs239.pdf.

(e) Kontroly na riadenie významných rizík súvisiacich s outsourcingom /externým zabezpečovaním IKT služieb

59. Príslušné orgány by mali posúdiť, či stratégia inštitúcie v oblasti outsourcingu v súlade s požiadavkami usmernení Výboru európskych orgánov bankového dohľadu o outsourcingu (2006), ako aj s požiadavkami v bode 85 písm. d) usmernení EBA o postupe SREP, bola primerane uplatnená v prípade outsourcingu IKT služieb vrátane outsourcingu IKT služieb v rámci finančnej skupiny. Pri posudzovaní rizík súvisiacich s outsourcingom IKT služieb by príslušné orgány mali zohľadniť skutočnosť, že tieto riziká sa môžu posudzovať aj v rámci hodnotenia vlastných operačných rizík podľa bodu 240 písm. j) usmernení EBA o postupe SREP, aby sa zabránilo duplicite práce alebo dvojitému započítaniu.

60. Príslušné orgány by konkrétne mali posúdiť, či inštitúcia má účinný rámec na identifikáciu a meranie rizík súvisiacich s outsourcingom IKT služieb a na porozumenie týmto rizikám, a konkrétne či má kontroly a kontrolné prostredie na zmierňovanie rizík spojených s významnými IKT službami zabezpečovanými externe, ktoré sú úmerné povahe, rozsahu a zložitosti činností inštitúcie a jej profilu z hľadiska rizika súvisiaceho s IKT a ktoré zahŕňajú:

    a. posúdenie vplyvu outsourovaných IKT služieb na riadenie rizík inštitúcie spojeného s využívaním poskytovateľov služieb (napr. poskytovateľov cloudových služieb) a ich služieb počas obstarávania, ktoré sa zdokumentuje a ktoré vrcholový manažment alebo riadiaci orgán zohľadní v rozhodnutí, či sa služby zadajú externe. Inštitúcia by mala preskúmať politiky riadenia rizík súvisiacich s IKT a kontroly IKT a kontrolné prostredie poskytovateľa služieb s cieľom zabezpečiť, aby napĺňali interné ciele inštitúcie v oblasti riadenia rizík a jej ochotu podstupovať riziká. Toto preskúmanie by sa malo pravidelne aktualizovať v priebehu zmluvného využívania outsourcovaných služieb, pričom sa zohľadnia charakteristické vlastnosti outsourcovaných služieb;

    b. monitorovanie rizík outsourcovaných služieb súvisiacich s IKT v priebehu zmluvného využívania outsourcovanýchslužieb v rámci riadenia rizík inštitúcie, ktoré poslúži ako vstup pre reporting o riadení rizík súvisiacich s IKT (napr. reporting o kontinuite činností, reporting o bezpečnosti);

    c. monitorovanie a porovnanie úrovní prijatých služieb so zmluvne dohodnutými úrovňami služieb, ktoré by mali tvoriť súčasť zmluvy o outsourcingu alebo dohody o úrovni poskytovaných služieb (SLA); a

    d. vhodných zamestnancov, zdroje a schopnosti na monitorovanie a riadenie rizík súvisiacich s IKT vyplývajúcich zo služieb zabezpečovaných externe.

3.4 Zhrnutie zistení a skóring

61. Na základe uvedeného posúdenia by príslušné orgány mali vypracovať stanovisko o riziku inštitúcie súvisiacom s IKT. Toto stanovisko by sa malo odzrkadliť v zhrnutí zistení, ktoré by príslušné orgány mali zohľadniť pri prideľovaní bodového hodnotenia operačného rizika v Tabuľke 6 usmernení EBA o postupe SREP. Príslušné orgány by mali svoje stanovisko založiť na významných rizikách súvisiacich s IKT a zohľadniť pritom tieto aspekty, ktorú poslúžia ako vstupné údaje pre posúdenie operačného rizika:

    a. Aspekty rizika

        i. profil inštitúcie z hľadiska rizika súvisiaceho s IKT a súvisiace expozície;

ii. zistené kritické IKT systémy a služby; a
iii. významnosť rizika súvisiaceho s IKT, pokiaľ ide o kritické IKT systémy.

b. Aspekty riadenia a kontroly

i. či medzi politikou a stratégiou riadenia rizika súvisiaceho s IKT inštitúcie a jej celkovou stratégiou a rizikovým apetítom existuje súlad;
ii. či je organizačný rámec riadenia rizík súvisiacich s IKT spoľahlivý s jasne vymedzenými povinnosťami a zreteľným oddelením úloh medzi vlastníkmi rizika a funkciami riadenia a kontroly rizík;
iii. či sú systémy merania, monitorovania a reportingu rizika súvisiaceho s IKT primerané; a
iv. či sú kontrolné mechanizmy významných rizík súvisiacich s IKT spoľahlivé.

62. Ak príslušné orgány považujú riziko súvisiace s IKT za významné a príslušný orgán sa rozhodne posúdiť a ohodnotiť toto riziko ako podkategóriu operačného rizika, v tabuľke uvedenej ďalej (Tabuľka 1) sa uvádzajú odôvodnenia bodového hodnotenia rizika súvisiaceho s IKT.

Tabuľka 1: Kritériá orgánov dohľadu, ktoré uplatňujú pri bodovaní rizika súvisiaceho s IKT

Skóre rizika	Stanovisko orgánov dohľadu	Kritériá týkajúce sa inherentného rizika	Kritéria týkajúce sa náležitého riadenia a kontrol
1	Vzhľadom na úroveň inherentného rizika a riadenie a kontroly neexistuje žiadne viditeľné riziko významného prudenciálneho vplyvu na inštitúciu.	• Zo zdrojov informácií, ktoré sa mali zohľadniť podľa bodu 37, nevyplynuli nijaké významné expozície rizikám súvisiacim s IKT. • Z povahy profilu inštitúcie z hľadiska rizika súvisiaceho s IKT v spojení preskúmaním kritických IKT systémov a významných rizík súvisiacich s IKT pre IKT systémy a služby nevyplynuli nijaké významné riziká súvisiace s IKT.	• Politika a stratégia inštitúcie týkajúce sa rizika súvisiaceho s IKT je úmerná s jej celkovou stratégiou a ochotou podstupovať riziká. • Organizačný rámec rizika súvisiaceho s IKT je spoľahlivý s jasne vymedzenými
2	Vzhľadom na úroveň inherentného rizika a riadenie a kontroly existuje nízke riziko významného prudenciálneho vplyvu na inštitúciu.	• Zo zdrojov informácií, ktoré sa mali zohľadniť podľa bodu 37, nevyplynuli nijaké významné expozície rizikám súvisiacim s IKT. • Z povahy profilu inštitúcie z hľadiska rizika súvisiaceho s IKT v spojení s preskúmaním kritických IKT systémov a významných rizík súvisiacich s IKT pre IKT systémy a služby vyplynula obmedzená expozícia rizikám súvisiacim s IKT (napr. najviac 2 z 5 vopred	

		stanovených kategórií rizík súvisiacich s IKT).	povinnosťami a zreteľným oddelením úloh medzi vlastníkmi rizika a funkciami riadenia a kontroly rizík. • Systémy merania, monitorovania a oznamovania rizika súvisiaceho s IKT sú primerané. • Rámec kontroly rizika súvisiaceho s IKT je spoľahlivý.
3	Vzhľadom na úroveň inherentného rizika a riadenie a kontroly existuje stredne vysoké riziko významného prudenciálneho vplyvu na inštitúciu.	• Zo zdrojov informácií, ktoré sa mali zohľadniť podľa bodu 37, vyplynuli náznaky možných významných expozícií rizikám súvisiacim s IKT. • Z povahy profilu inštitúcie z hľadiska rizika súvisiaceho s IKT v spojení preskúmaním kritických IKT systémov a významných rizík súvisiacich s IKT pre IKT systémy a služby vyplynula zvýšená expozícia rizikám súvisiacim s IKT (napr. 3 alebo viac z 5 vopred stanovených kategórií rizík súvisiacich s IKT).	
4	Vzhľadom na úroveň inherentného rizika a riadenie a kontroly existuje vysoké riziko významného prudenciálneho vplyvu na inštitúciu.	• Zo zdrojov informácií, ktoré sa mali zohľadniť podľa bodu 37, vyplynulo viacero náznakov významných expozícií rizikám súvisiacim s IKT. • Z povahy profilu inštitúcie z hľadiska rizika súvisiaceho s IKT v spojení preskúmaním kritických IKT systémov a významných rizík súvisiacich s IKT pre IKT systémy a služby vyplynula vysoká expozícia rizikám súvisiacim s IKT (napr. 4 alebo 5 z 5 vopred stanovených kategórií rizík súvisiacich s IKT).	

Príloha – Taxonómia rizík súvisiacich s IKT

Päť kategórií rizík súvisiacich s IKT s neúplným zoznamom rizík súvisiacich s IKT s možnou vysokou závažnosťou a/alebo vplyvom na operácie, dobrú povesť alebo financie

Kategórie rizík súvisiacich s IKT	Riziká súvisiace s IKT (neúplné[10])	Opis rizika	Príklady
Riziká súvisiace s dostupnosťou a kontinuitou IKT	Neprimerané riadenie kapacít	Nedostatok zdrojov (napr. hardvér, softvér, zamestnanci, poskytovatelia služieb) môže viesť k neschopnosti zmeniť mieru služby na účely splnenia potrieb podnikov, k prerušovaniu systému, degradácii služby a/alebo prevádzkovým chybám.	• Deficit kapacít môže ovplyvniť mieru prenosu a dostupnosť siete (internetu) pre služby ako je elektronické bankovníctvo. • Nedostatok zamestnancov (interných alebo od tretích strán) môže viesť k prerušovaniu systému a/alebo prevádzkovým chybám.
	Zlyhania IKT systému	Strata dostupnosti spôsobená zlyhaním hardvéru.	• Zlyhanie úložiska (pevné disky), servera alebo ďalšieho vybavenia IKT zapríčinené napr. nedostatočnou údržbou.
		Strata dostupnosti spôsobená zlyhaním softvéru a chybami.	• Nekonečná slučka v aplikačnom softvéri bráni výkonu transakcie. • Výpadky z dôvodu pokračovania v používaní zastaraných IKT systémov a riešení, ktoré už nespĺňajú súčasné požiadavky na dostupnosť a odolnosť a/alebo ich už ich predajcovia nepodporujú.
	Neprimerané plánovanie kontinuity IKT a obnovy po havárii	Zlyhanie plánovaných riešení týkajúcich sa dostupnosti a/alebo kontinuity a/alebo obnovy po havárii (napr. dátové stredisko pre obnovu návratom k predchádzajúcej verzii) pri aktivácii v reakcii na udalosť.	• Rozdiely v konfigurácii medzi primárnym a sekundárnym dátovým strediskom môžu viesť k neschopnosti dátových stredísk pre návrat k predchádzajúcim verziám zabezpečiť plánovanú kontinuitu služby.
	Narúšajúce a deštruktívne	Útoky s rôznymi účelmi (napr. aktivizmus, vydieračstvo), ktoré vedú k preťaženiu systémov a siete	• Útoky typu distribuovaného odmietnutia služby sa vykonávajú prostredníctvom veľkého počtu

[10] Riziká súvisiace s IKT sa uvádzajú v kategórii rizík, v ktorej majú najväčší vplyv, môžu však ovplyvňovať iné kategórie rizika.

Kategórie rizík súvisiacich s IKT	Riziká súvisiace s IKT (neúplné[10])	Opis rizika	Príklady
	kybernetické útoky	a bránia oprávneným používateľom v prístupe k on-line počítačovým službám.	počítačových systémov na internete ovládaných hekerom, ktorý odosiela veľké množstvo zdanlivo oprávnených požiadaviek na internetové služby (napr. elektronické bankovníctvo).
Riziká súvisiace s bezpečnosťou IKT	Kybernetické útoky a iné externé útoky založené na IKT	Útoky z internetu alebo z vonkajších sietí, ktoré majú rôzne účely (napr. podvod, špionáž, aktivizmus/sabotáž, kybernetický terorizmus) a ktoré využívajú rozmanité techniky (napr. sociálne inžinierstvo, pokusy o prienik využitím zraniteľností, využitie malvéru), čo vedie k prevzatiu kontroly nad internými IKT systémami.	Rôzne typy útokov: • APT (Advanced Persistent Threat – vyspelá vytrvalá hrozba) na prevzatie kontroly nad internými systémami alebo na krádež informácií (napr. informácií súvisiacich s krádežou totožnosti, informácií o kreditných kartách). • Malvér (napr. ransomware), ktorý zašifruje údaje s cieľom vydierať. • Nakazenie interného IKT systému tzv. trójskymi koňmi s cieľom spáchať zákerné činnosti v systéme skrytým spôsobom. • Využitie zraniteľností IKT systému a/alebo (webovej) aplikácie (napr. vloženie SQL …) na získanie prístupu do interného IKT systému.
		Vykonanie podvodných platobných transakcií hekermi prostredníctvom narušenia alebo obchádzania bezpečnostných prvkov elektronického bankovníctva a platobných služieb a/alebo útokom na bezpečnostné slabiny a využitím týchto slabín v interných platobných systémoch inštitúcie.	• Útoky proti elektronickému bankovníctvu alebo platobným službám s cieľom uskutočniť neoprávnené transakcie. • Vytvorenie a odoslanie podvodných platobných transakcií z interných platobných systémov inštitúcie (napr. podvodné správy týkajúce sa SWIFT kódu).
		Vykonanie podvodných transakcií s cennými papiermi hekermi prostredníctvom narušenia alebo obídenia bezpečnostných prvkov služieb elektronického bankovníctva, ktoré poskytujú aj prístup k účtom cenných papierov klientov.	• Útoky typu „pump and dump“ (vyčerpať a odhodiť), pri ktorých útočníci získajú prístup k účtu cenných papierov klientov elektronického bankovníctva a zadajú podvodné pokyny na nákup alebo predaj s cieľom ovplyvniť trhovú cenu a/alebo zarobiť na základe vopred určených pozícií cenných papierov.
		Útoky na komunikačné prepojenia a konverzácie	• Odpočúvanie alebo zachytenie nechráneného

Kategórie rizík súvisiacich s IKT	Riziká súvisiace s IKT (neúplné[10])	Opis rizika	Príklady
		všetkého druhu alebo na IKT systémy s cieľom zhromaždiť informácie a/alebo sa dopustiť podvodu.	prenosu overovacích údajov v čistom textovom formáte.
	Neprimeraná interná bezpečnosť IKT	Získanie neoprávneného prístupu do kritických IKT systémov zvnútra inštitúcie, a to na rôzne účely (napr. podvod, vykonanie a zakrytie nebezpečných obchodných činností, krádež údajov, aktivizmus/sabotáž) prostredníctvom rôznych techník (napr. prostredníctvom zneužitia a/alebo eskalovania prednostných práv, krádeže totožnosti, sociálneho inžinierstva, využitia zraniteľných miest v IKT systéme, nasadenia malvéru).	• Inštalovanie softvéru na zaznamenávanie stlačených klávesov (tzv. key logger) s cieľom ukradnúť používateľskú identifikáciu a heslá na účely získania neoprávneného prístupu k dôverným údajom a/alebo spáchania podvodu. • Prelomenie alebo uhádnutie slabých hesiel na získanie neoprávnených alebo vyšších prístupových práv. • Správca systému používa operačné systémy alebo databázové nástroje (na priamu úpravu databázy) s cieľom spáchať podvod.
		Neoprávnená manipulácia s IKT z dôvodu nevhodných postupov a praxe riadenia prístupu IKT.	• Nevyradenie alebo nevymazanie zbytočných účtov, ako sú účty zamestnancov, ktorí zmenili pracovné zaradenie a/alebo odišli z inštitúcie vrátane hostí alebo dodávateľov, ktorí už nepotrebujú prístup, čím sa poskytuje neoprávnený prístup do IKT systémov. • Udelenie nadmerných prístupových práv a oprávnení, ktoré umožňujú neoprávnený prístup a/alebo umožňujú zakryť škodlivé činnosti.
		Bezpečnostné hrozby spôsobené nedostatočnou informovanosťou o bezpečnosti, v dôsledku čoho zamestnanci nerozumejú, zanedbávajú alebo nedodržiavajú politiky a postupy bezpečnosti IKT.	• Zamestnanci, ktorí boli navedení k napomáhaniu pri útok (t. j. sociálne inžinierstvo). • Nesprávne postupy týkajúce sa poverení: používanie spoločných hesiel, používanie hesiel, ktoré sú jednoduché na uhádnutie, používanie rovnakého hesla na veľa rôznych účelov atď. • Uloženie nezašifrovaných dôverných údajov na laptopoch a prenosných úložiskách (napr. na USB kľúčoch), ktoré sa môžu stratiť alebo môžu byť odcudzené.

Kategórie rizík súvisiacich s IKT	Riziká súvisiace s IKT (neúplné[10])	Opis rizika	Príklady
		Neoprávnené uloženie alebo prenos dôverných informácií mimo inštitúcie.	• Osoby, ktoré kradnú alebo úmyselne vynášajú či pašujú dôverné informácie pre neoprávnené osoby alebo pre verejnosť.
	Nevhodná fyzická bezpečnosť IKT	Nesprávne použitie alebo krádež majetku IKT prostredníctvom fyzického prístupu, čím sa spôsobí škoda, strata majetku alebo údajov alebo sa tým umožnia ďalšie hrozby.	• Fyzické vlámanie do kancelárskych budov a/alebo dátových stredísk s cieľom ukradnúť vybavenia IKT (napr. počítače, laptopy, úložiská) a/alebo vytvoriť kópie údajov prostredníctvom fyzického prístupu k IKT systémom.
		Úmyselné alebo náhodné poškodenie fyzického majetku IKT spôsobené pri teroristickom útoku, nehode alebo nešťastnom/nesprávnom zaobchádzaní zo strany zamestnancov inštitúcie a/alebo tretích strán (dodávatelia, opravár).	• Fyzický teroristický útok (t. j. teroristický bombový útok) alebo sabotáž proti majetku IKT. • Zničenie dátového strediska spôsobené ohňom, únikom vody alebo inými činiteľmi.
		Nedostatočná fyzická ochrana proti prírodným katastrofám, ktorá má za následok čiastočné alebo úplné zničenie IKT systémov / dátových stredísk prírodnými katastrofami.	• Zemetrasenia, extrémne horúčavy, veterné víchrice, husté sneženie, povodne, požiare, blesky.
Riziká súvisiace so zmenou IKT	Nevhodné kontroly nad zmenami IKT systémov a ich vývojom	Udalosti spôsobené napríklad softvéru, IKT systémom a údajom prostredníctvom neodhalených chýb alebo zraniteľností v dôsledku zmeny (napr. nepredvídané následky zmeny, slabo riadená zmena spôsobená nedostatočným testovaním alebo nevhodné postupy riadenia zmeny).	• Uvedenie do výroby softvéru, ktorý nebol dostatočne testovaný alebo zmien konfigurácie s neočakávanými nežiaducimi účinkami na údaje (napr. poškodenie, vymazanie) a/alebo na výkonnosť IKT systému (napr. pád systému, zníženie výkonnosti). • Nekontrolované zmeny IKT systémov alebo údajov vo výrobnom prostredí. • Uvedenie do výroby zle zabezpečených IKT systémov a internetových aplikácií, ktoré vytvárajú príležitosti pre hekerské útoky na poskytované internetové služby a/alebo preniknutie do interných IKT systémov. • Neskontrolované zmeny v zdrojovom kóde interne vyvíjaného softvéru.

Kategórie rizík súvisiacich s IKT	Riziká súvisiace s IKT (neúplné[10])	Opis rizika	Príklady
			• Nedostatočné testovanie z dôvodu neprítomnosti vhodného testovacieho prostredia.
	Nevhodná architektúra IKT	Slabé riadenie architektúry IKT pri navrhovaní, budovaní a udržiavaní IKT systémov (napr. softvéru, hardvéru, údajov) môže časom viesť k nepružným IKT systémom, ktoré sú zložité, náročné a nákladné na riadenie a ktoré už nie sú v súlade s obchodnými potrebami a neuspokojujú skutočné požiadavky na riadenie rizík.	• Nevhodne riadené zmeny IKT systémov, softvéru a/alebo údajov v dlhšom časovom období, ktoré vedú k IKT systémom a architektúram, ktoré sú zložité, nerovnorodé a náročné na riadenie, čo spôsobuje veľa nežiaducich účinkov na činnosť a riadenie rizík (napr. chýbajúca flexibilita a svižnosť, udalosti a zlyhania IKT, vysoké prevádzkové náklady, oslabená bezpečnosť a odolnosť IKT, nižšia kvalita údajov a znížená kapacita podávania správ). • Nadmerné prispôsobovanie a rozširovanie obchodných softvérových balíkov pomocou interne vyvíjaného softvéru, čo vedie k neschopnosti zaviesť budúce vydania a modernizácie obchodného softvéru a k riziku, že tento softvér už predajca nebude podporovať.
	Nevhodné riadenie životného cyklu a opráv	Neudržiavanie primeraného zoznamu všetkého majetku IKT na podporu spoľahlivých postupov životného cyklu a riadenia opráv a v kombinácii s nimi. To vedie k tomu, že IKT systém nie sú dostatočne opravené (a teda sú zraniteľnejšie) a sú zastarané a nemusia podporovať obchodné potreby a potreby riadenia rizík.	• Neopravené a zastarané IKT systémy, ktoré môžu mať nežiaduce účinky na činnosť a riadenie rizík (napr. chýbajúca flexibilita a svižnosť, výpadky IKT, oslabená bezpečnosť a odolnosť IKT).
Riziká súvisiace s integritou IKT údajov	Nefunkčné spracovanie údajov a zaobchádzanie s nimi v rámci IKT	Z dôvodu systémových, komunikačných a/alebo aplikačných chýb alebo zlyhaní, alebo z dôvodu chybne vykonaného procesu extrakcie, prenosu a nahratia údajov môže dôjsť k poškodeniu alebo strate údajov.	• Výpočtová systémová chyba pri hromadnom spracovaní, ktorá zapríčiní nesprávnu bilanciu na bankových účtoch klienta. • Nesprávne vykonané dopyty. • Strata údajov z dôvodu chyby pri replikácii (zálohovaní).
	Zle navrhnuté kontroly na	Chyby týkajúce sa chýbajúcich alebo neúčinných automatizovaných kontrol dátových vstupov a prijatia	• Nedostatočné alebo neplatné formátovanie/potvrdenie vkladaných údajov

Kategórie rizík súvisiacich s IKT	Riziká súvisiace s IKT (neúplné[10])	Opis rizika	Príklady
	potvrdzovanie údajov v IKT systémoch	(napr. pre použité údaje tretej strany), kontrol pre prenos, spracovanie a výstup údajov v IKT systémoch (napr. kontroly platnosti vkladaných údajov, zosúladenie údajov).	v aplikáciách a/alebo používateľských rozhraniach. • Neexistencia kontrol na zosúladenie údajov vo vytvorených výstupných údajoch. • Neexistencia kontrol vykonávaných procesov extrakcie údajov (napr. databázové dopyty), čo vedie k chybným údajom. • Použitie chybných externých údajov.
	Zle kontrolované zmeny údajov v prevádzkových IKT systémoch.	Chyby údajov spôsobené nedostatočnými kontrolami správnosti a odôvodnenej povahy manipulácie s údajmi vykonanými v prevádzkových IKT systémoch.	• Vývojári alebo správcovia databáz, ktorí priamo pristupujú k údajom v prevádzkových IKT systémoch a menia ich nekontrolovaným spôsobom, napríklad v prípade udalosti týkajúcej sa IKT.
	Zle navrhnutá a/alebo riadená dátová architektúra, dátové toky, dátové modely a dátové slovníky	Zle riadené dátové architektúry, dátové modely, dátové toky alebo dátové slovníky môžu vyústiť do viacerých verzií rovnakých údajov v IKT systémoch, ktoré už viac nebudú zhodné z dôvodu odlišne používaných dátových modelov alebo dátových definícií a/alebo rozdielov v súvisiacom procese tvorby údajov a ich zmeny.	• Existencia rôznych zákazníckych databáz na produkt alebo obchodný útvar s odlišnými dátovými definíciami a poľami, čo vedie k nezosúladeným zákazníckym údajom, ktoré je na úrovni celej finančnej inštitúcie alebo skupiny ťažké porovnať a integrovať.
Riziká súvisiace s externým zabezpečovaním IKT služieb	Nedostatočná odolnosť služieb tretej strany alebo iného subjektu skupiny	Nedostupnosť kritických IKT služieb, telekomunikačných služieb a zariadení zadaných externe. Strata alebo poškodenie kritických alebo citlivých údajov zverených poskytovateľovi služieb	• Nedostupnosť hlavných služieb v dôsledku zlyhania na strane IKT systémov alebo aplikácií (externe zadaných) dodávateľov. • Prerušenie telekomunikačných prepojení. • Výpadok elektrickej energie.
	Nedostatočné riadenie outsourcingu	Veľké zhoršenie služieb alebo zlyhania spôsobené nedostatočnou pripravenosťou alebo postupmi kontroly externého poskytovateľa služieb. Nedostatočné riadenie outsourcingu môže viesť k nedostatku vhodných zručností a kapacít na plnú identifikáciu, posúdenie, zmiernenie a monitorovanie rizík súvisiacich s IKT a môže obmedziť prevádzkové schopnosti inštitúcií.	• Nedostatočné postupy zvládania udalostí, zmluvné kontrolné mechanizmy a záruky zakotvené v dohode s poskytovateľom služieb, ktoré zvyšujú závislosť kľúčového subjektu od tretích strán a predajcov. • Nevhodná zmena kontrol nad riadením týkajúcich sa poskytovateľa služieb prostredia IKT môže spôsobiť významné zhoršenie služieb alebo ich zlyhanie.

Kategórie rizík súvisiacich s IKT	Riziká súvisiace s IKT (neúplné[10])	Opis rizika	Príklady
	Nedostatočná bezpečnosť tretej strany alebo iného subjektu skupiny	Hekerský útok proti IKT systémom poskytovateľa služieb tretej strany s priamym vplyvom na externe zadávané služby alebo na kritické/dôverné údaje uložené v systéme poskytovateľa služieb. Zamestnanci poskytovateľa služieb, ktorí získali neoprávnený prístup ku kritickým alebo citlivým údajom uloženým v systéme poskytovateľa služieb.	• Hekerský útok proti poskytovateľom služieb zločincami alebo teroristami, ktorý predstavuje miesto vstupu do IKT systému inštitúcie, alebo takýto útok na získanie prístupu ku kritickým alebo citlivým údajom uloženým v systéme poskytovateľa služieb alebo na zničenie týchto údajov. • Interní pracovníci na strane poskytovateľa služieb so zlými úmyslami, ktorí sa snažia ukradnúť a predať citlivé údaje.