EBA/GL/2017/05

11/09/2017

Obecné pokyny

Obecné pokyny k posuzování rizik IKT v rámci procesu přezkoumání a vyhodnocení

1. Dodržování předpisů a oznamovací povinnost

Status těchto obecných pokynů

1. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010[1]. V souladu s čl. 16 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 příslušné orgány a finanční instituce vynaloží veškeré úsilí, aby se těmito obecnými pokyny řídily.

2. Obecné pokyny formulují názor orgánu EBA na náležité postupy dohledu v rámci Evropského systému dohledu nad finančním trhem nebo na to, jak by unijní právní předpisy měly být uplatňovány v konkrétní oblasti. Příslušné orgány ve smyslu čl. 4 odst. 2 nařízení (EU) č. 1093/2010, na které se tyto obecné pokyny vztahují, by s nimi měly být v souladu a začlenit je do svých postupů (např. pozměněním právního rámce nebo dohledových postupů), včetně případů, kdy jsou obecné pokyny zaměřeny v prvé řadě na instituce.

Oznamovací povinnost

3. V souladu s čl. 16 odst. 3 nařízení (EU) č. 1093/2010 musí příslušné orgány do 13.11.2017 orgánu EBA oznámit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést do tohoto data důvody, proč se jimi neřídí či nehodlají řídit. Neposkytnou-li příslušné orgány oznámení v této lhůtě, bude mít orgán EBA za to, že se těmito obecnými pokyny neřídí nebo nehodlají řídit. Oznámení by měla být zasílána na formuláři, který je k dispozici na internetových stránkách orgánu EBA, na adresu compliance@eba.europa.eu s označením „EBA/GL/2017/05“. Oznámení by měly předkládat osoby s příslušným oprávněním oznamovat, zda se jejich příslušné orgány těmito obecnými pokyny řídí nebo hodlají řídit. Jakoukoli změnu stavu dodržování pokynů je rovněž nutno oznámit orgánu EBA.

4. Oznámení budou zveřejněna na internetových stránkách orgánu EBA v souladu s čl. 16 odst. 3.

[1] Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12).

2. Předmět, oblast působnosti a definice

Předmět a oblast působnosti

5. Tyto obecné pokyny byly vypracovány podle čl. 107 odst. 3 směrnice 2013/36/EU[2] a jejich cílem je zajistit sbližování postupů dohledu při posuzování rizik spojených s informačními a komunikačními technologiemi (IKT) v rámci procesu dohledu a hodnocení, který je zmiňován v článku 97 směrnice 2013/36/EU a podrobněji popsán v Obecných pokynech orgánu EBA ke společným postupům a metodikám procesu přezkoumání a vyhodnocení[3]. Tyto obecné pokyny popisují zejména hodnotící kritéria, která by příslušné orgány dohledu měly používat při hodnocení kontrolního a řídicího systému a strategie institucí v oblasti IKT a při posuzování expozic institucí rizikům IKT a souvisejících kontrolních mechanismů. Tyto obecné pokyny tvoří nedílnou součást Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení.

6. Příslušné orgány by tyto obecné pokyny měly uplatňovat v souladu s úrovní použití procesu přezkoumání a vyhodnocení popsanou v Obecných pokynech orgánu EBA k procesu přezkoumání a vyhodnocení a v souladu s modelem minimálního zapojení a zásadou proporcionality uváděnými tamtéž.

Určení

7. Tyto obecné pokyny jsou určeny příslušným orgánům ve smyslu čl. 4 odst. 2 bodu i) nařízení (EU) č. 1093/2010.

Definice

8. Není-li uvedeno jinak, mají pojmy použité a vymezené ve směrnici 2013/36/ES, nařízení (EU) č. 575/2013 a v Obecných pokynech orgánu EBA k procesu přezkoumání a vyhodnocení stejný význam i v těchto obecných pokynech. Kromě toho platí pro účely těchto obecných pokynů tyto definice:

[2] Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (1) – Úř. věst. L 176, 27.6.2013.

[3] EBA/GL/2014/13

Systémy IKT	Dílčí funkční celky zajišťující podporu procesů instituce pomocí informačních a komunikačních technologií.
Služby IKT	Služby poskytované systémy IKT jednomu nebo několika interním či externím uživatelům. Příkladem může být zadávání, ukládání a zpracování dat, vytváření sestav, ale také monitorování, podnikové služby a služby na podporu rozhodování.
Riziko spojené s dostupností a zachováním kontinuity IKT	Riziko nežádoucího zásahu do výkonnosti a dostupnosti systémů a dat IKT, včetně neschopnosti včas obnovit služby instituce, v důsledku selhání hardwarových nebo softwarových součástí IKT; slabin v řízení systému IKT; nebo jakékoli další události, jak je podrobně rozvedeno v příloze.
Riziko spojené se zabezpečením IKT	Riziko neoprávněného přístupu do systémů a dat IKT z vnitřního prostředí instituce nebo zvnějšku (např. kybernetické útoky), jak je podrobně rozvedeno v příloze.
Riziko spojené se změnou IKT	Riziko spočívající v neschopnosti instituce včas a kontrolovaně řídit změny v systémech IKT, a to zejména u velkých a složitých změnových programů, jak je podrobně rozvedeno v příloze.
Riziko ohrožení integrity dat IKT	Riziko, že data uložená a zpracovávaná v systémech IKT nebudou napříč různými systémy IKT kompletní, přesná nebo konzistentní, například vlivem slabých nebo chybějících kontrol IKT v různých etapách životního cyklu dat IKT (tzn. navrhování datové architektury, vytváření datových modelů a/nebo datových slovníků, ověřování zadaných dat, kontrola nad extrakcí, transferem a zpracováním dat, včetně vytvořených datových výstupů), které by instituci znemožnilo správně a včas poskytovat služby a vydávat informace týkající se řízení (rizik) a financí, jak je podrobně rozvedeno v příloze.
Riziko spojené s externím zajištěním IKT	Riziko, že pověření třetí strany nebo jiného subjektu skupiny (zajištění v rámci skupiny) poskytováním systémů IKT či souvisejících služeb nežádoucím způsobem ovlivní výkonnost a řízení rizik instituce, jak je podrobně rozvedeno v příloze.

3. Provádění

Datum použití

9. Tyto obecné pokyny se použijí od 1. ledna 2018.

4. Požadavky na posuzování rizik IKT

Hlava 1 – Obecná ustanovení

10. Příslušné orgány by měly rizika IKT i řídicí a kontrolní mechanismy a strategii v oblasti IKT posuzovat v rámci procesu přezkoumání a vyhodnocení za použití modelu minimálního zapojení a zásady proporcionality, které popisuje hlava 2 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení. To zejména znamená, že:

    a. četnost posuzování rizik IKT by se měla odvíjet od modelu minimálního zapojení podle kategorie, do níž instituce v rámci procesu dohledu a hodnocení spadá, a také s ohledem na konkrétní program dohledových šetření; a

    b. hloubka, podrobnost a náročnost posuzování IKT by měly být úměrné velikosti, struktuře a provoznímu prostředí instituce a rovněž povaze, měřítku a složitosti jejích činností.

11. Princip proporcionality se v rámci těchto obecných pokynů uplatňuje na rozsah, četnost a náročnost zapojení orgánu dohledu, dialog s institucí a také na standardy, která by instituce měla podle očekávání orgánu dohledu splnit.

12. Příslušné orgány se mohou spoléhat na práci, kterou již instituce nebo příslušný orgán odvedly v souvislosti s ostatními riziky nebo prvky procesu přezkoumání a vyhodnocení s cílem získat aktualizované hodnocení, a měly by k ní přihlížet. Jestliže příslušné orgány provádí posuzování vymezené těmito obecnými pokyny, měly by jmenovitě zvolit pro posouzení orgánem dohledu takovou koncepci a metodiku, která je z hlediska instituce nejvhodnější a nejpřiměřenější, a zdrojem informací by jim pro tento účel měla být dostupná stávající dokumentace (např. relevantní zprávy a jiné dokumenty, porady s vedením (pro řízení rizik), zjištění inspekcí na místě).

13. Příslušné orgány by měly zjištění ze svých posudků podle kritérií stanovených těmito obecnými pokyny shrnout a použít je jako podklad pro závěry týkající se posuzování prvků procesu přezkoumání a vyhodnocení dle Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení.

14. Posouzení řízení, kontroly a strategie v oblasti IKT podle hlavy 2 těchto obecných pokynů by mělo zejména přinést zjištění, která budou zahrnuta do souhrnu zjištění hodnocení vnitřního řídicího a kontrolního systému a kontrolních mechanismů v celé instituci, jež je prvkem procesu přezkoumání a vyhodnocení popsaného v hlavě 5 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení, a mělo by se odrazit i ve skóre daného prvku. Příslušné orgány by dále měly zvážit, zda do analýzy obchodního modelu podle hlavy 4 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení nezahrnou také případný nežádoucí vliv hodnocení strategie v oblasti IKT na obchodní strategii instituce nebo obavy, zda instituce disponuje v oblasti IKT dostatečnými prostředky a kapacitami, aby mohla provádět důležité plánované strategické změny.

15. Výsledek posouzení rizik IKT dle hlavy 3 těchto obecných pokynů by se měl promítnout do zjištění z posouzení operačního rizika a měl by být považován za dílčí složku příslušného skóre, jak je uvedeno v oddílu 6.4 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení.

16. Je známo, že příslušné orgány by obecně měly posuzovat dílčí kategorie rizika jako součásti hlavních kategorií (tzn. riziko IKT bude posuzováno jako součást operačního rizika), považují-li však některé dílčí kategorie za podstatné, mohou je posuzovat individuálně. Pro případ, že by příslušný orgán považoval riziko IKT za podstatné, obsahují tyto obecné pokyny také tabulku s bodovým hodnocením (tabulka č. 1), která by měla sloužit k samostatnému bodování dílčí kategorie rizika IKT podle celkové koncepce bodového hodnocení rizik pro kapitál obsažené v Obecných pokynech orgánu EBA k procesu přezkoumání a vyhodnocení.

17. Při rozhodování, zda riziko IKT považovat za podstatné a jako takové ho posuzovat a hodnotit jako samostatnou dílčí kategorii operačního rizika, mohou příslušné orgány použít kritéria uvedená v oddílu 6.1 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení.

18. V rámci uplatňování těchto obecných pokynů by měly příslušné orgány v relevantních případech zohlednit demonstrativní výčet dílčích kategorií rizika IKT a rizikových scénářů, jenž je uveden v příloze. Je však třeba mít na paměti, že příloha zmiňuje rizika IKT, která mohou vést k vysoce závažným škodám. Pokud některá rizika IKT zahrnutá do této klasifikace s daným posudkem nesouvisí, mohou je příslušné orgány vynechat. Předpokládá se, že instituce nejspíše namísto klasifikace rizik IKT v příloze používají vlastní zatřídění.

19. Jsou-li tyto obecné pokyny uplatňovány ve vztahu k přeshraničním bankovním skupinám a jejich subjektům a bylo-li vytvořeno kolegium orgánů dohledu, měly by dotčené příslušné orgány v rámci spolupráce pro účely hodnocení přezkoumání a vyhodnocení podle oddílu 11.1 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení v maximálním možném rozsahu koordinovat zajištění jednotlivých informací ve stejném rozsahu a konzistentně u všech subjektů skupiny.

Hlava 2 – Posuzování řídicího a kontrolního systému a strategie institucí v oblasti IKT

2.1 Všeobecné principy

20. Příslušné orgány by měly posoudit, zda obecný rámec řídicího a kontrolního systému a mechanismů vnitřní kontroly instituce náležitě zohledňuje systémy IKT i související rizika a zda vedoucí orgán tyto aspekty odpovídajícím způsobem řeší a řídí, neboť IKT jsou neodmyslitelně spjaty s řádným fungováním instituce.

21. Při tomto posuzování by se příslušné orgány měly opírat o požadavky a standardy v oblasti řídicího a kontrolního systému a mechanismy kontroly rizik popsané v Obecných pokynech orgánu EBA k internal governance (GL 44)[4] a mezinárodních pokynech pro danou oblast, a to v míře použitelné s ohledem na specifika systémů a rizik IKT.

22. Posuzování popisované v této hlavě se nevztahuje na specifické prvky řízení a kontroly, řízení rizik a kontrolních mechanismů systémů IKT zaměřené na řízení konkrétních rizik IKT, o nichž pojednává hlava 3 těchto obecných pokynů, ale zaměřuje se na tyto oblasti:

    a. strategie v oblasti IKT – zda má instituce v oblasti IKT strategii, která je patřičně řízena a kontrolována a která odpovídá obchodní strategii instituce;

    b. celkový rámec vnitřního řídicího a kontrolního systému – zda jsou mechanismy celkového rámce vnitřního řízení a kontroly v souvislosti se systémy IKT instituce přiměřené; a

    c. riziko IKT v rámci řízení rizik instituce – zda rámec řízení rizik a vnitřních kontrolních mechanismů instituce patřičně chrání její systémy IKT.

23. Ačkoli odst. 22 písm. a) poskytuje informace o prvcích řídicího a kontrolního systému instituce, měly by tyto informace sloužit především jako zdroj při hodnocení obchodního modelu dle hlavy 4 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení. Písmena b) a c) dále doplňují hodnocení oblastí popsaných v hlavě 5 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení a posuzování popsané těmito obecnými pokyny by se mělo promítnout do příslušného hodnocení podle hlavy 5 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení.

24. Výsledky tohoto hodnocení by se měly v relevantních případech zohlednit při posuzování řízení rizik a kontrolních mechanismů podle hlavy 3 těchto pokynů.

[4] Obecné pokyny Evropského orgánu pro bankovnictví k internal governance (řídicí a kontrolní systém), GL 44, 27. září 2011.

2.2 Strategie v oblasti IKT

25. Tato část pojednává o tom, že by příslušné orgány měly posoudit, zda instituce disponuje v oblasti IKT strategií, která: podléhá odpovídajícímu dohledu ze strany vedoucího orgánu instituce; je v souladu s obchodní strategií, zejména s ohledem na aktuálnost IKT nebo implementaci důležitých a složitých změn IKT; a podporuje obchodní model instituce.

2.2.1 Rozvoj a přiměřenost strategie v oblasti IKT

26. Příslušné orgány by měly posoudit, zda instituce svoji strategii v oblasti IKT připravuje a rozvíjí podle rámce, který je přiměřený povaze, rozsahu a složitosti její činnosti v oblasti IKT. Při tom by příslušné orgány měly zohlednit, zda:

    a. je do určování strategických priorit v oblasti IKT patřičně zapojeno vrcholné vedení[5] příslušných linií podnikání, zda je vrcholné vedení pro oblast IKT seznámeno s přípravou, navrhováním a zaváděním hlavních obchodních strategií a iniciativ, aby byl i nadále zajištěn soulad mezi systémy IKT, službami IKT a funkcemi IKT (tzn. osobami odpovědnými za řízení a nasazování těchto systémů a služeb) a obchodní strategií instituce, a zda jsou IKT efektivně aktualizovány;

    b. se strategie v oblasti IKT dokumentuje a je podložena konkrétními plány na realizaci, zejména v souvislosti s významnými milníky a plánováním zdrojů (včetně finančních prostředků a lidských zdrojů) a je tak zjištěna její proveditelnost a praktické uplatňování;

    c. instituce svoji strategii v oblasti IKT pravidelně aktualizuje, zejména při změnách obchodní strategie, a střednědobé až dlouhodobé cíle, plány a činnosti v oblasti IKT tudíž soustavně odpovídají obchodním cílům, plánům a činnostem; a

    d. vedoucí orgán instituce schvaluje strategii v oblasti IKT i plány na její realizaci a monitoruje provádění strategie.

2.2.2 Provádění strategie v oblasti IKT

27. Pokud strategie instituce v oblasti IKT vyžaduje provedení důležitých a složitých změn IKT, nebo změn se závažným dopadem na obchodní model instituce, měly by příslušné orgány posoudit, zda instituce disponuje kontrolním rámcem, který odpovídá její velikosti, činnostem v oblasti IKT i úrovni prováděných změn a podporuje tak efektivní provádění strategie instituce v oblasti IKT. Při tom by příslušné orgány měly zohlednit, zda kontrolní rámec:

    a. zahrnuje procesy řízení a kontroly (např. monitorování a vykazování postupu a rozpočtu) a příslušné subjekty (např. oddělení řízení projektů, řídící komisi pro ICT apod.), které účinně podporují strategické plány v oblasti IKT;

[5] Pojmy „vrcholné vedení“ a „vedoucí orgán“ jsou vymezeny ve směrnici 2013/36/EU ze dne 26. června 2013, v čl. 3 odst. 7 (vedoucí orgán), resp. v čl. 3 odst. 9 (vrcholné vedení).

b. obsahuje úlohy a odpovědnosti určené a přidělené pro účely provádění strategických plánů v oblasti IKT, zejména s důrazem na zkušenosti klíčových účastníků, pokud jde o organizování, řízení a monitorování důležitých a složitých změn IKT a o řízení širších účinků těchto změn na organizaci a lidské zdroje (např. zvládání řešení připomínek a stížností ke změně, školení, komunikace);

c. využívá nezávislé útvary pro kontrolu a interní audity s cílem zajistit identifikaci, posouzení a účinné snižování rizik spojených s prováděním strategie v oblasti IKT a prokázat existenci efektivního rámce řízení a kontroly provádění strategie v oblasti IKT; a

d. zahrnuje proces plánování a revize plánování, který zajistí pružnou reakci na zjištěné důležité problémy (např. problémy nebo prodlevy, k nimž při prováděné dojde) nebo na vnější vývoj (např. důležité změny podnikatelského prostředí, technologické záležitosti nebo inovace), který umožňuje plán provádění strategie včas upravit.

2.3 Celkový rámec vnitřního řídicího a kontrolního systému

28. Podle hlavy 5 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení by příslušné orgány měly posoudit, zda má instituce patřičně transparentní podnikovou strukturu, která je vhodná pro daný účel, a zda zavedla odpovídající mechanismy vnitřního řízení a kontroly. Toto hodnocení by mělo s výslovným přihlédnutím k systémům IKT a v souladu s Obecnými pokyny orgánu EBA k internal governance zahrnovat hodnocení toho, zda instituce prokazuje:

a. pevně zavedenou a transparentní organizační strukturu s jasně vymezenými odpovědnostmi v oblasti IKT, včetně vedoucího orgánu a jeho výborů, a zda má hlavní osoba odpovědná za IKT (např. ředitel informačních technologií „CIO“, provozní ředitel „COO“ nebo obdobná funkce) odpovídající nepřímý nebo přímý přístup k vedoucímu orgánu, aby byla schopna náležitým způsobem zajistit oznamování, projednávání a rozhodování v souvislosti s důležitými informacemi a otázkami v oblasti IKT na úrovni vedoucího orgánu; a

b. zda vedoucí orgán zná a chápe rizika spojená s IKT.

29. V návaznosti na oddíl 5.2 Obecných pokynů orgánu EBA k postupu přezkoumání a vyhodnocení by příslušné orgány měly posoudit, zda směrnice a strategie instituce pro externí zajištění IKT v relevantních případech zohledňují dopad externího zajištění IKT na podnikání a obchodní model instituce.

2.4 Riziko IKT v rámci řízení rizik instituce

30. Při hodnocení řízení rizik a mechanismů vnitřní kontroly v celé instituci dle hlavy 5 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení by příslušné orgány měly zvážit, zda rámec řízení rizik a vnitřních kontrolních mechanismů instituce patřičně chrání její systémy IKT způsobem, který odpovídá rozsahu a činnostem instituce a rizikovému profilu jejích IKT, jak popisuje hlava 3. Příslušné orgány by měly zejména určit, zda:

a. ochota podstupovat rizika a interní postupy pro hodnocení kapitálové přiměřenosti (ICAAP) zahrnují pro účely vymezení celkové strategie v oblasti rizik a stanovení vnitřního kapitálu do širší kategorie operačních rizik také rizika spojená s IKT; a

b. zda rizika IKT spadají do působnosti rámců řízení rizik a vnitřní kontroly v celé instituci.

31. Příslušné orgány by měly provést hodnocení podle písmene a) uvedeného výše s přihlédnutím k očekávanému vývoji i nepříznivým scénářům, například ke scénářům, které jsou součásti zátěžového testu prováděného danou institucí nebo v rámci dohledu.

32. S přihlédnutím k písmenu b) by měly příslušné orgány posoudit, zda jsou útvary nezávislé kontroly a interního auditu, podrobně popsané v odst. 104 písm. a) a d) a odst. 105 písm. a) a c) Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení, natolik přiměřené, aby dokázali zajistit dostatečnou míru nezávislosti IKT a funkcí kontroly a auditu s ohledem na velikost a rizikový profil IKT instituce.

2.5 Souhrn zjištění

33. Tyto výsledky by se měly promítnout do souhrnu zjištění podle hlavy 5 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení a měly by být zahrnuty do příslušného bodového hodnocení v souladu s faktory uvedenými v tabulce č. 3 zmíněných obecných pokynů.

34. Při posuzování strategie v oblasti IKT by příslušné orgány měly pro účely výše uvedeného hodnocení vzít v úvahu tyto body:

a. pokud příslušné orgány dojdou podle oddílu 2.2 k závěru, že rámec řídicího a kontrolního systému instituce nedostačuje k rozvoji a provádění její strategie v oblasti IKT, měly by tento závěr promítnout do hodnocení vnitřního řídicího a kontrolního systému instituce uvedeného v odst. 87 písm. a) hlavy 5 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení;

b. pokud příslušné orgány dojdou na základě hodnocení uvedených výše v oddílu 2.2 k závěru, že by se strategie v oblasti IKT významně odlišovala od obchodní strategie, což by mohlo podstatným způsobem nepříznivě ovlivnit dlouhodobé obchodní a/nebo finanční cíle instituce, udržitelnost instituce a/nebo její obchodní model nebo oblasti/linie jejího podnikání, které jsou v odst. 62 písm. a) Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení určeny za nejpodstatnější, pak by se tento závěr měl odrazit na hodnocení obchodního modelu podle odst. 70 písm. b) a c) hlavy 4 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení; a

c. pokud příslušné orgány dojdou na základě hodnocení uvedených v oddílu 2.2 výše k závěru, že instituce nemusí mít v oblasti IKT dostatečné prostředky a dostatečné realizační kapacity, aby mohla provádět a podporovat důležité plánované strategické změny, měly by tento závěr zohlednit v hodnocení obchodního modelu podle odst. 70 písm. b) hlavy 4 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení.

Hlava 3 – Posuzování expozice instituce rizikům IKT a jejích kontrolních mechanismů

3.1 Obecné úvahy

35. Příslušné orgány by měly posoudit, zda instituce řádně identifikuje, hodnotí a snižuje rizika IKT, která jí hrozí. Tento proces by měl být začleněn do rámce řízení operačního rizika a měl by se shodovat s přístupem uplatňovaným v případě operačního rizika.

36. Příslušné orgány by měly nejprve určit podstatná rizika spjatá s IKT, jimž instituce čelí nebo může čelit, a následně posoudit účinnost rámce, postupů a kontrolních mechanismů instituce pro řízení rizik v oblasti IKT, které mají tato rizika snížit. Výsledek hodnocení by se měl promítnout do souhrnu zjištění, z něhož vychází skóre operačního rizika podle Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení. Je-li riziko IKT považováno za podstatné a příslušné orgány mu chtějí udělit samostatné skóre, měly by jej bodově ohodnotit podle tabulky č. 1 jako dílčí kategorii operačního rizika.

37. Při posuzování podle této hlavy by příslušné orgány měly využít veškeré dostupné zdroje informací uvedené v odstavci 127 hlavy 6 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení, například činnosti, zprávy a výsledky z oblasti řízení rizik a vytvořit tak základ pro identifikaci svých priorit při hodnocení v rámci dohledu. Příslušné orgány by měly k posouzení využít i další zdroje informací, jsou-li relevantní, také následující:

    a. vlastní hodnocení rizik a kontrolních mechanismů v oblasti IKT (je-li součástí interních postupů pro hodnocení kapitálové přiměřenosti);
    b. informace vedení o rizicích IKT předkládané vedoucímu orgánu instituce, například hlášení o rizicích IKT poskytovaná pravidelně i při konkrétní události (včetně databáze provozních ztrát), údaje o expozici rizikům IKT od člena vedení pro řízení rizik instituce;
    c. nálezy interních i externích auditů oznámené výboru pro audit dané instituce v souvislosti s IKT.

3.2 Identifikace podstatných rizik IKT

38. Příslušné orgány by měly identifikovat podstatná rizika IKT, kterým instituce čelí nebo může čelit, podle postupu uvedeného níže.

3.2.1 Přezkoumání rizikového profilu IKT instituce

39. Při přezkoumání rizikového profilu IKT instituce by příslušné orgány měly zvážit veškeré relevantní informace o expozici instituce rizikům IKT, včetně informací uvedených v odstavci 37 a zjištěných podstatných nedostatků a slabin v organizaci IKT i kontrolních mechanismech celé instituce podle hlavy 2 těchto obecných pokynů, a ve vhodných případech by tyto informace měly přiměřeně přezkoumat. V rámci přezkoumání by příslušné orgány měly vzít v úvahu:

a. možný dopad významného narušení systémů IKT instituce na celý finanční systém na tuzemské i mezinárodní úrovni;
b. zda může být instituce kvůli závislosti na internetu, rozsáhlému přijímání inovativních řešení v oblasti IKT nebo jiným firemním distribučním kanálům, díky nimž se pravděpodobněji stane cílem kybernetických útoků, vystavena rizikům souvisejícím se zabezpečením nebo dostupností a kontinuitou IKT;
c. zda nemůže být instituce více vystavena rizikům souvisejícím se zabezpečením IKT, dostupností a kontinuitou IKT, integritou dat IKT nebo se změnou IKT kvůli složitosti (např. při fúzích a akvizicích) nebo zastaralosti svých systémů IKT;
d. zda instituce provádí podstatné změny svých systémů IKT a/nebo funkcí IKT (např. při fúzích, akvizicích, divesticích nebo výměně klíčových systémů IKT), které by mohly nepříznivě ovlivnit stabilitu nebo řádné fungování systémů IKT a mohly by vyvolat podstatné riziko, pokud jde o dostupnost, kontinuitu, zabezpečení nebo změnu IKT nebo integritu dat IKT;
e. zda instituce zajišťuje služby nebo systémy IKT externě, v rámci skupiny nebo mimo ni, což může instituci vystavit podstatným rizikům spojeným s externím zajištěním IKT;
f. zda instituce provádí opatření, která agresivně snižují náklady na IKT, což může vést k omezení potřebných investic do IKT, prostředků a informačních kompetencí a zvýšit expozici všem druhům rizik IKT v klasifikaci;
g. zda umístění důležitých provozních / datových center IKT (např. regiony, země) může instituci vystavit přírodním katastrofám (např. záplavám, zemětřesením), politické nestabilitě nebo pracovním konfliktům a občanským nepokojům, což může vést k podstatnému zvýšení rizik týkajících se dostupnosti, kontinuity a zabezpečení IKT.

3.2.2 Přezkoumání kritických systémů a služeb IKT

40. Příslušné orgány by v rámci procesu identifikace rizik IKT s možným významným obezřetnostním dopadem na instituci měly přezkoumat dokumentaci instituce a rozhodnout o tom, které systémy a služby IKT jsou kritické pro řádné fungování, dostupnost, kontinuitu a zabezpečení základních činností instituce.

41. Za tímto účelem by příslušné orgány měly přezkoumat metodiku a procesy, které instituce používá k identifikaci kritických systémů a služeb IKT, s přihlédnutím k tomu, že některé systémy a služby IKT může instituce považovat za kritické z hlediska zachování provozu instituce a dostupnosti, zabezpečení (např. prevence podvodů) a/nebo utajení (např. důvěrných dat). Při provádění přezkoumání by měly příslušné orgány vzít v úvahu, že by kritické systémy a služby IKT měly splňovat alespoň jednu z následujících podmínek:

a. podporují klíčové obchodní operace a distribuční kanály (např. bankomaty, internetové a mobilní bankovnictví) instituce;
b. podporují základní procesy systému řízení a kontroly a podnikové funkce, včetně řízení rizik (např. systémy pro řízení rizik a správu pokladny);
c. vztahují se na ně zvláštní zákonné nebo regulatorní požadavky (pokud jsou), které v souvislosti s některými systémově důležitými službami (připadají-li v úvahu) kladou zvýšené nároky na dostupnost, odolnost, důvěrnost nebo zabezpečení (např. zákony o ochraně osobních údajů

nebo případné cílové doby obnovy (RTO, tedy maximální doba nutná pro obnovení systému nebo procesu po mimořádné události) a cílové body obnovy (RPO, tedy maximální doba, za kterou mohou být v případě mimořádné události data ztracena);

d. zpracovávají nebo ukládají důvěrná nebo citlivá data, která by v případě neoprávněného přístupu mohla významně ovlivnit reputaci, finanční výsledky nebo spolehlivost a kontinuitu podnikání instituce (např. databáze s citlivými údaji o zákaznících); a/nebo

e. poskytují základní liniové funkce, které jsou životně důležité pro řádné fungování instituce (např. služby zajišťující telekomunikaci a konektivitu, služby IKT a služby kybernetického zabezpečení).

3.2.3 Identifikace podstatných rizik IKT u kritických systémů a služeb IKT

42. Příslušné orgány by si s přihlédnutím k provedeným přezkoumáním rizikového profilu IKT a kritických systémů a služeb IKT instituce, zmiňovaným výše, měly utvořit názor na podstatná rizika IKT, která mohou mít v rámci posouzení ze strany orgánu dohledu významný obezřetnostní dopad na kritické systémy a služby IKT instituce.

43. Při posuzování potenciálního dopadu rizik IKT na kritické systémy a služby IKT instituce by příslušné orgány měly vzít v úvahu:

a. finanční dopad, včetně (mimo jiné) ztráty finančních prostředků nebo aktiv, případných kompenzací pro zákazníky, právních nákladů a nákladů na nápravné prostředky, smluvní náhrady škody, ušlého zisku;

b. možné přerušení obchodní činnosti, s ohledem (mimo jiné) na kritickou povahu dotčených finančních služeb; počet zákazníků a/nebo poboček a zaměstnanců, kteří mohou být dotčeni;

c. potenciální dopad na reputaci instituce na základě kritické povahy dotčené bankovní služby nebo provozní činnosti (např. odcizení údajů o zákaznících); externí profil/viditelnost dotčených systémů a služeb IKT (např. mobilních nebo on-line bankovních systémů, prodejních míst, bankomatů nebo platebních systémů);

d. regulatorní dopad, včetně případného veřejného napomenutí ze strany regulátora, pokuty nebo dokonce změny povolení;

e. strategický dopad na instituci, například při zneužití nebo zcizení strategického produktu nebo obchodních plánů.

44. Příslušné orgány by následně měly identifikovaná rizika IKT považovaná za podstatná zařadit do následujících kategorií rizik IKT. Rizika jsou blíže popsána spolu s příklady v příloze. Příslušné orgány by měly v rámci hodnocení podle hlavy 3 reagovat na rizika IKT uvedená v příloze:

a. riziko spojené s dostupností a zachováním kontinuity IKT
b. riziko spojené se zabezpečením IKT
c. riziko spojené se změnou IKT
d. riziko ohrožení integrity dat IKT

e. riziko spojené s externím zajištěním IKT

Přiřazení rizik do jednotlivých kategorií má příslušným orgánům pomoci určit, která rizika jsou podstatná (pokud vůbec) a měla by být proto podrobena širšímu a/nebo hlubšímu přezkoumání v dalších etapách hodnocení.

3.3 Posouzení kontrolních mechanismů ke snižování podstatných rizik IKT

45. Aby mohly příslušné orgány posoudit zbytkovou expozici instituce rizikům IKT, měly by přezkoumat, jak instituce identifikuje, monitoruje, vyhodnocuje a snižuje podstatná rizika, která příslušné orgány určily při výše uvedeném hodnocení.

46. Příslušné orgány by proto měly s ohledem na identifikovaná podstatná rizika IKT přezkoumat relevantní:

a. zásady a procesy řízení rizik IKT a prahové hodnoty tolerance rizik;

b. rámec organizačního řízení a dohledu;

c. rozsah a nálezy interních auditů; a

d. mechanismy pro kontrolu rizik IKT, které se vztahují ke konkrétnímu identifikovanému podstatnému riziku IKT.

47. Hodnocení by mělo zohlednit výsledek analýzy celkového rámce řízení rizik a vnitřní kontroly, o němž hovoří hlava 5 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení, jakož i řídicí a kontrolní systém a strategii instituce, o nichž pojednává hlava 2 těchto obecných pokynů, neboť významné nedostatky v těchto oblastech mohou ovlivnit schopnost instituce řídit a snižovat vlastní expozici rizikům IKT. Ve vhodných případech by příslušné orgány měly rovněž využít zdroje informací zmiňované v odstavci 37 těchto obecných pokynů.

48. Příslušné orgány by měly další etapy hodnocení provádět způsobem, který je úměrný povaze, rozsahu a složitosti činností instituce a měly by při nich uplatnit přezkoumání orgánem dohledu, který odpovídá rizikovému profilu IKT instituce.

3.3.1 Zásady a procesy řízení rizik IKT a prahové hodnoty tolerance

49. Příslušné orgány by měly přezkoumat, zda instituce u identifikovaných podstatných rizik IKT uplatňuje vhodné zásady a procesy řízení rizik IKT a prahové hodnoty tolerance. Ty mohou být součástí rámce řízení operačního rizika nebo mohou tvořit samostatný dokument. V tomto hodnocení by příslušné orgány měly zohlednit, zda:

a. zásady řízení rizik formálně schválil vedoucí orgán, a zda obsahují dostačující vodítka, pokud jde o ochotu instituce podstupovat rizika IKT, hlavní sledované cíle v oblasti řízení rizik IKT a/nebo používané prahové hodnoty tolerance rizik IKT; s příslušnými zásadami řízení rizik IKT by měly být rovněž seznámeny všechny relevantní zúčastněné osoby;

b. platné zásady zahrnují všechny prvky, které jsou pro řízení identifikovaných podstatných rizik IKT významné;

c. instituce provádí proces a podpůrné postupy identifikace (např. vlastní hodnocení rizik a kontroly – RCSA, analýza rizikových scénářů) a monitorování dotčených podstatných rizik IKT; a

d. instituce vypracovává výkazy řízení rizik IKT, které poskytují vrcholnému vedení a vedoucímu orgánu včasné informace a umožňují vrcholnému vedení a/nebo vedoucímu orgánu vyhodnocovat a monitorovat soulad plánů a opatření instituce na snižování rizik IKT se schválenou ochotou podstupovat riziko a/nebo prahovými hodnotami tolerance (v relevantních případech) a monitorovat změny podstatných rizik IKT.

3.3.2 Rámec organizačního řízení a dohledu

50. Příslušné orgány by měly posoudit, nakolik jsou příslušné role a odpovědnosti v oblasti řízení rizik zasazeny a začleněny do vnitřní organizace pro účely řízení identifikovaných podstatných rizik IKT a dohled nad nimi. Příslušné orgány by v tomto ohledu měly posoudit, zda instituce prokazuje:

a. jasně vymezené role a odpovědnosti k identifikaci, hodnocení, monitorování, snižování a vykazování dotčeného podstatného rizika IKT a k dohledu nad ním;

b. zda odpovědnosti a role spojené s riziky jsou jasně oznamovány, přidělovány a zakotveny ve všech příslušných součástech (např. linií podnikání, IT) a procesech organizace, včetně rolí a odpovědností k získávání a shromažďování informací o rizicích a jejich předávání vrcholnému vedení a/nebo vedoucímu orgánu;

c. zda činnosti v oblasti řízení rizik IKT provádí dostatečný počet patřičně kvalifikovaných pracovníků s dostatečnými a přiměřeně kvalitními technickými prostředky; aby mohly příslušné orgány vyhodnotit věrohodnost příslušných plánů na snižování rizik, měly by rovněž posoudit, zda instituce vyhradila na jejich provádění dostatečné finanční rozpočty a/nebo další potřebné prostředky;

d. odpovídající následnou kontrolu a reakci ze strany vedoucího orgánu, pokud jde o důležitá zjištění nezávislých kontrolních funkcí týkající se rizik(a) IKT, s přihlédnutím k možnému postoupení některých aspektů výboru, pokud je zřízen; a

e. zda se výjimky z nařízení a zásad platných pro IKT evidují a zda jsou předmětem zdokumentovaného přezkoumání a oznamování ze strany nezávislé kontrolní funkce s důrazem na související rizika.

3.3.3 Rozsah a nálezy interních auditů

51. Příslušné orgány by měly zvážit, zda je funkce interního auditu při provádění auditu platných rámců kontroly rizik IKT efektivní, a přezkoumat, zda:

a. je rámec kontrol rizik IKT podrobován auditu požadované kvality, hloubky a četnosti a zda odpovídá velikostí činnostem a rizikovému profilu IKT instituce;

b. plán auditu zahrnuje audity kritických rizik IKT identifikovaných institucí;

c. jsou důležité nálezy auditu IKT, včetně odsouhlasených opatření, předkládány vedoucímu orgánu; a

d. zda se vrcholné vedení a/nebo výbor pro audit nálezy auditu IKT, včetně odsouhlasených opatření, následně zabývá a zda pravidelně přezkoumává zprávy o pokroku.

3.3.4 Mechanismy pro kontrolu rizik IKT, které se vztahují ke konkrétním identifikovaným podstatným rizikům IKT

52. V případě identifikovaných podstatných rizik IKT by příslušné orgány měly posoudit, zda instituce využívá k řešení těchto rizik konkrétní kontrolní mechanismy. Oddíly níže uvádí demonstrativní výčet konkrétních kontrolních mechanismů, které je třeba brát v úvahu při hodnocení rizik, která byla podle oddílu 3.2.3 identifikována jako podstatná a přiřazená do následujících kategorií rizik IKT:

a. rizika spojená s dostupností a zachováním kontinuity IKT;
b. rizika spojená se zabezpečením IKT;
c. rizika spojené se změnou IKT;
d. rizika ohrožení integrity dat IKT;
e. rizika spojené s externím zajištěním IKT.

(a) Kontrolní mechanismy pro řízení podstatných rizik spojených s dostupností a zachováním kontinuity IKT

53. Kromě požadavků uvedených v Obecných pokynech orgánu EBA k procesu přezkoumání a vyhodnocení (odstavce 279–281) by příslušné orgány měly posoudit, zda instituce uplatňuje vhodný rámec pro identifikaci, pochopení, měření a snižování rizika spojená s dostupností a zachováním kontinuity IKT.

54. V tomto hodnocení by příslušné orgány měly zejména zohlednit, zda tento rámec:

a. označuje kritické procesy IKT a příslušné podpůrné systémy IKT, které by měly být součástí plánů zajištění odolnosti a zachování provozu instituce společně:

   i. s komplexní analýzou závislostí mezi kritickými podnikovými procesy a podpůrnými systémy;

   ii. s určením cílů obnovy podpůrných systémů IKT (např. instituce a/nebo předpisy obvykle stanoví RTO a RPO);

   iii. s vhodnými pohotovostními plány, které zajistí dostupnost, kontinuitu a obnovu kritických systémů a služeb IKT s cílem omezit přerušení operací instituce na přijatelnou mez;

b. obsahuje zásady a standardy pro zajištění odolnosti a kontrolu kontinuity a provozní kontrolní mechanismy, které zahrnují:

   i. opatření, která brání tomu, aby jednotlivé scénáře, mimořádné události nebo katastrofy zasáhly jak produkční tak záložní systémy IKT;

   ii. postupy pro zálohu a obnovu kritického softwaru a dat systémů IKT, které zajišťují, aby se tyto zálohy ukládaly na zabezpečené a dostatečně vzdálené místo a aby mimořádnou událostí ani katastrofou nemohla být tato kritická data zničena či poškozena;

   iii. monitorovací procesy pro včasné zjištění mimořádných událostí týkajících se dostupnosti a zachování kontinuity IKT;

iv. zdokumentovaný proces řízení a eskalace mimořádných událostí, který rovněž obsahuje pokyny pro různé úlohy a odpovědnosti v rámci řízení a eskalace mimořádných událostí, členy krizových výborů a hierarchii řízení v případě krizové situace;

v. fyzická opatření na ochranu kritické infrastruktury IKT instituce (např. datových center) před environmentálními riziky (např. záplavami a jinými přírodními katastrofami) a k zajištění vhodného provozního prostředí pro systémy IKT (např. klimatizace);

vi. procesy, úlohy a odpovědnosti, které zajistí, aby byly do příslušných řešení a plánů zajištění odolnosti a zachování provozu instituce zahrnuty i externě zajišťované systémy a služby IKT;

vii. řešení pro plánování a monitorování výkonnosti a kapacity kritických systémů a služeb IKT s vymezenými požadavky na dostupnost, aby bylo možné včas odhalit významná omezení výkonnosti a kapacity;

viii. řešení na ochranu kritických internetových činností nebo služeb (např. služby elektronického bankovnictví), v nezbytných a vhodných případech, proti útokům typu DoS (odepření služeb) nebo jiným kybernetickým útokům z internetu zaměřeným na odepření nebo narušení přístupu k těmto činnostem nebo službám;

c. testuje řešení pro zajištění dostupnosti a kontinuity IKT podle řady realistických scénářů včetně kybernetických útoků, testuje převzetí služeb při selhání a zálohy kritického softwaru a dat, přičemž tyto testy:

i. jsou plánovány, formálně schvalovány a dokumentovány a výsledky testů slouží k posílení účinnosti řešení pro zajištění dostupnosti a kontinuity IKT;

ii. zahrnují zúčastněné osoby a funkce v organizaci, jako je vedení jednotlivých linií podnikání včetně týmů zodpovědných za zachování provozu instituce a reakci na mimořádné a krizové události, jakož i příslušné zainteresované subjekty z vnějšího prostředí;

iii. vedoucí orgán a vrcholné vedení jsou patřičným způsobem zapojeny (např. jako součást týmů krizového řízení) a seznámeny s výsledky testů.

(b) Kontrolní mechanismy pro řízení podstatných rizik spojených se zabezpečením IKT

55. Příslušné orgány by měly posoudit, zda má instituce efektivní rámec pro identifikaci, chápání, měření a snižování rizik spojených se zabezpečením IKT. V tomto hodnocení by příslušné orgány měly zejména zohlednit, zda daný rámec bere v potaz:

a. jasně vymezené role a odpovědnosti, pokud jde o:

i. osoby a/nebo výbory, které odpovídají za každodenní správu zabezpečení IKT a přípravu zastřešujících zásad zabezpečení IKT, s důrazem na jejich potřebnou nezávislost;
ii. koncepci, provádění, řízení a monitorování kontrolních mechanismů pro zabezpečení IKT;

iii. ochranu kritických systémů a služeb IKT například přijetím procesu hodnocení zranitelnosti, správy softwarových aktualizací, ochrany koncových bodů (např. proti škodlivému softwaru), nástrojů na detekci a prevenci neoprávněného průniku;
iv. monitorování, klasifikaci a zpracování externích nebo interních mimořádných událostí v rámci zabezpečení IKT; včetně reakce na mimořádné události a opětovného zprovoznění a obnovy systémů a služeb IKT;
v. pravidelné a proaktivní hodnocení hrozeb s cílem udržet kontrolní mechanismy zabezpečení v řádném stavu;

b. zásady zabezpečení IKT, které zohledňují a ve vhodných případech také dodržují mezinárodně uznávané standardy a principy zabezpečení IKT (např. princip nejnižších možných oprávnění, to znamená omezení přístupu na minimální úroveň, která umožní běžné fungování správy přístupových práv, a princip „hloubkové ochrany“, tzn. že vrstvené bezpečnostní mechanismy posilují zabezpečení systému jako celku při navrhování architektury zabezpečení);

c. proces identifikace systémů a služeb IKT a úměrné bezpečnostní požadavky odrážející potenciální riziko podvodů a/nebo možného nesprávného užití a/nebo zneužití důvěrných údajů spolu se zdokumentovanými bezpečnostními předpoklady, které tyto identifikované systémy, služby a data IKT musí splňovat, v souladu s rizikovou tolerancí instituce, a které musí být monitorovány z hlediska jejich správného provádění;

d. zdokumentovaný proces řízení a eskalace mimořádných událostí v oblasti zabezpečení, který obsahuje pokyny pro různé úlohy a odpovědnosti v rámci řízení a eskalace mimořádných událostí, členy krizových výborů a hierarchií řízení v případě krizových situací;

e. protokolování činnosti uživatelů a administrátorů, které umožní efektivněji monitorovat a včas detekovat neoprávněnou aktivitu a reagovat na ni; pro účely asistence při forenzním šetření mimořádných událostí v oblasti bezpečnosti nebo pro účely provádění tohoto šetření. Instituce by měla mít zavedeny zásady protokolování, které vymezí patřičné druhy záznamů, jež mají být uchovávány, a také dobu, po kterou mají být uchovávány;

f. povědomí a informační kampaně nebo iniciativy, které všechny úrovně instituce seznámí s bezpečným používáním a ochranou systémů IKT instituce a s hlavními bezpečnostními (i jinými) riziky IKT, o nichž by tito pracovníci měli vědět, zejména v souvislosti se stávajícími i rozvíjejícími se kybernetickými hrozbami (např. počítačové viry, možné interní nebo externí zneužití či útoky, kybernetické útoky) a jejich vlastní úlohou při omezování porušení zabezpečení;

g. odpovídající fyzická bezpečnostní opatření (např. průmyslové kamery, poplašné zařízení, bezpečnostní dveře), která zabrání neoprávněnému fyzickému přístupu ke kritickým a citlivým systémům IKT (např. datovým centrům);

h. opatření chránící systémy IKT před útoky z internetu (tzn. kybernetickými útoky) nebo jiných externích sítí (např. tradiční telekomunikační připojení nebo propojení s důvěryhodnými partnery); příslušné orgány by měly přezkoumat, zda rámec instituce zohledňuje:

i. proces a řešení k udržování kompletního aktualizovaného inventáře a přehledu všech vnějších hraničních bodů síťového připojení (např. internetových stránek, internetových aplikací, Wi-Fi, vzdáleného přístupu), přes něž by mohly třetí strany prolomit interní systémy IKT;

ii. přísně řízená a monitorovaná bezpečnostní opatření (např. firewally, proxy servery, přenos pošty, antiviry a skenery obsahu) pro zabezpečení příchozího i odchozího síťového provozu (např. elektronické pošty) a vnějších hraničních síťových připojení, přes něž by mohly třetí strany prolomit interní systémy IKT;

iii. procesy a řešení pro zabezpečení internetových stránek a aplikací, které mohou být přímo napadeny z internetu a/nebo zvenčí a které by mohly sloužit jako vstupní bod do interních systémů IKT; obecně sem patří kombinace uznávaných postupů pro vývoj zabezpečení, postupů pro posílení systémů IKT a skenování slabin a realizace doplňkových bezpečnostních řešení, například používání firewallů a/nebo systémů pro odhalování neoprávněného průniku (IDS) a/nebo prevenci neoprávněného průniku (IPS);

iv. pravidelné bezpečnostní penetrační testy, které slouží k posouzení účinnosti prováděných opatření a procesů v rámci kybernetického a interního zabezpečení IKT; tyto testy by měli provádět pracovníci a/nebo externí specialisté, kteří mají potřebné odborné znalosti, přičemž by se výsledky a závěry testů měly dokumentovat a vykazovat vrcholnému vedení a/nebo vedoucímu orgánu; v případě potřeby a použitelnosti by instituce při těchto testech měla zjistit, zda je třeba dále zdokonalovat bezpečnostní kontroly a procesy a/nebo získat lepší ujištění o jejich efektivitě.

(c) Kontrolní mechanismy pro řízení podstatných rizik změn IKT

56. Příslušné orgány by měly posoudit, zda má instituce efektivní rámec pro identifikaci, chápání, měření a snižování rizika spojená se změnou IKT, který je úměrný povaze, rozsahu a složitosti činností instituce a jejímu rizikovému profilu IKT. Rámec instituce by měl zahrnovat rizika spojená s vývojem, testováním a schvalováním změn systémů IKT, včetně vývoje nebo změny softwaru, a to před jejich přenesením do produkčního prostředí, s cílem zajistit řádné řízení životního cyklu IKT. V tomto hodnocení by příslušné orgány měly zejména zohlednit, zda daný rámec bere v potaz:

a. zdokumentované procesy řízení a kontroly změn systémů IKT (např. správa konfigurace a aktualizací) a dat (např. opravy chyb nebo dat), které zajišťují odpovídající zahrnutí řízení rizik IKT do důležitých změn IKT, které by mohly mít významný dopad na rizikový profil nebo expozici instituce;

b. specifikace týkající se nezbytného oddělení povinností v různých etapách prováděných procesů změn IKT (např. koncepce a vývoj řešení, testování a schvalování nového softwaru a/nebo změn, přenos a realizace v produkčním prostředí a opravy chyb) s důrazem na prováděná řešení a oddělení povinností při řízení a kontrole změn produkčních systémů a dat IKT pracovníky IKT (např. vývojáři, administrátory systémů IKT, administrátory databází) nebo jinou stranou (např. podnikovými uživateli, poskytovateli služeb);

c. zkušební prostředí, které patřičně odráží prostředí produkční;

d. inventář aktiv stávajících aplikací a systémů IKT v produkčním a také ve zkušebním a vývojovém prostředí, aby bylo možné potřebné změny (např. aktualizace nebo povýšení na nové verze, systémové aktualizace, změny konfigurace) dotčených systémů IKT řádně řídit, provádět a monitorovat;

e. proces monitorování a řízení životního cyklu používaných systémů IKT, který zajistí, aby tyto systémy nadále splňovaly a podporovaly současné požadavky v oblasti řízení podnikání a rizik a prověří, zda prodejci používaných řešení a systémů IKT k nim stále ještě poskytují podporu; a zda tento proces doplňují odpovídajícími postupy životního cyklu vývoje softwaru (SDLC);

f. systém a vhodné postupy na kontrolu zdrojového kódu, jež brání neoprávněným změnám ve zdrojovém kódu interně vyvíjeného softwaru;

g. proces provádění detekce a kontroly zabezpečení a slabin nových nebo podstatně změněných systémů a softwaru, než jsou uvolněny do produkce a vystaveny možným kybernetickým útokům;

h. proces a řešení bránící neoprávněnému nebo neúmyslnému zveřejnění důvěrných dat během výměny, archivace, mazání nebo likvidace systémů IKT;

i. proces nezávislého přezkoumání a validace, který snižuje riziko lidského pochybení při provádění změn systémů IKT, jež by mohlo mít značný nepříznivý dopad na dostupnost, kontinuitu nebo zabezpečení instituce (např. důležité změny konfigurace firewallu) nebo na zabezpečení instituce (např. změny firewallů).

(d) Kontrolní mechanismy pro řízení podstatných rizik ohrožení integrity dat IKT

57. Příslušné orgány by měly posoudit, zda má instituce efektivní rámec pro identifikaci, chápání, měření a snižování rizika ohrožení integrity dat IKT, který je úměrný povaze, rozsahu a složitosti činností instituce a jejímu rizikovému profilu IKT. Rámec instituce by měl zohledňovat rizika spojená s ochranou integrity dat uložených a zpracovávaných v systémech IKT. V tomto hodnocení by příslušné orgány měly zejména zohlednit, zda daný rámec bere v potaz:

a. zásady, které vymezují role a odpovědnosti při řízení integrity dat v systémech IKT (např. architekti dat, uživatelé dat[6], správci dat[7], vlastníci dat[8]) a poskytují pokyny pro identifikaci dat kritických z hlediska integrity, na která by se měly uplatňovat speciální kontrolní mechanismy IKT (např. automatizované kontroly ověřování vstupů, kontroly datového přenosu, kontrolní srovnání atd.) nebo přezkoumání (např. kontrola kompatibility s datovou architekturou) ve třech různých etapách životního cyklu dat IKT;

b. zdokumentovanou datovou architekturu, datový model a/nebo slovník ověřený příslušnými podnikovými nebo IT účastníky za účelem podpory potřebné integrity dat ve všech systémech IKT a zajištění trvalého souladu datové architektury, datového modelu a/nebo slovníku s potřebami řízení obchodní činnosti a rizik;

c. zásady pro přípustné používání a závislost na informační technice koncových uživatelů, zejména pokud jde o identifikaci, registraci a dokumentaci důležitých koncových řešení (např. při zpracování důležitých dat) a předpokládané úrovně zabezpečení na ochranu proti neoprávněným úpravám, jak nástroje samotného, tak i dat v něm uložených;

[6] Uživatel dat zpracovává a využívá data.
[7] Správce dat odpovídá za bezpečnou úschovu, přenos a ukládání dat.
[8] Vlastník dat odpovídá za řízení a vhodnost datových prvků – obsahu i metadat.

d. zdokumentované procesy nakládání s výjimkami pro řešení zjištěných problémů s integritou dat IKT v souladu s jejich kritickou a citlivou povahou.

58. U institucí, které podléhají dohledu a které spadají do působnosti principů BCBS 239 pro účinné shromažďování údajů v oblasti rizik a podávání zpráv o rizicích[9], by příslušné orgány měly přezkoumat analýzu rizik souvisejících s kapacitami instituce pro podávání hlášení o rizicích a shromažďování údajů na pozadí uvedených principů a vypracované související dokumentace a rovněž přihlédnout k prováděcímu harmonogramu a přechodným ustanovením daných principů.

(e) Kontrolní mechanismy pro řízení podstatných rizik spojených s externím zajištěním IKT

59. Příslušné orgány by měly posoudit, zda strategie externího zajištění instituce odpovídá požadavkům Obecných pokynů výboru CEBS k externímu zajištění činností nebo služeb (2006) a dále požadavku odst. 85 písm. d) Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení, v rozsahu týkajícím se externího zajištění IKT, včetně externího zajištění služeb IKT v rámci skupiny. Při posuzování rizik spojených s externím zajištěním IKT by příslušné orgány měly mít na paměti, že rizika spojená s externím zajištěním IKT již mohou být zahrnuta do hodnocení inherentních operačních rizik podle odst. 240 písm. j) Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení, a je-li tomu tak, měly by se vyhnout duplicitní práci i hodnocení.

60. Příslušné orgány by zejména měly posoudit, zda má instituce efektivní rámec pro identifikaci, chápání a měření rizika spojeného s externím zajištěním IKT, a především kontrolní mechanismy a prostředí, jež snižují rizika spojená s podstatnými, externě zajišťovanými službami IKT a jež jsou úměrné velikosti, činnostem i rizikovému profilu IKT instituce. Jejich součástí by mělo být:

a. posouzení dopadu externího zajištění IKT na řízení rizik instituce v souvislosti s využíváním poskytovatelů služeb (např. poskytovatelů cloudových služeb) a jejich služeb v průběhu zadávacího řízení, jež je zdokumentováno a k němuž vrcholné vedení nebo vedoucí orgán při rozhodování o externím zajištění služeb přihlíží; instituce by měla přezkoumat zásady řízení rizik IKT i mechanismy a prostředí pro kontrolu IKT využívané poskytovatelem služeb, aby se ujistila, zda odpovídají cílům v oblasti řízení interních rizik instituce i její ochotě podstupovat riziko; toto přezkoumání by se mělo po dobu smluvního externího zajišťování služeb pravidelně aktualizovat s přihlédnutím k povaze externě zajišťovaných služeb;

b. po dobu smluvního externího zajišťování služeb monitorování souvisejících rizik IKT v rámci řízení rizik instituce, které slouží instituci jako zdroj informací pro účely podávání hlášení o řízení rizik IKT (např. podávání hlášení o kontinuitě podnikání, hlášení o zabezpečení);

c. monitorování a porovnávání dodaných úrovní služeb se sjednanými úrovněmi služeb, které by měly být součástí smlouvy o externím zajištění služeb nebo smlouvy o úrovni poskytovaných služeb; a

d. odpovídající personální obsazení, prostředky a kompetence pro účely monitorování a řízení rizik IKT spojených s externě zajišťovanými službami.

[9] Basilejský výbor pro bankovní dohled, Principy účinného shromažďování údajů v oblasti rizik a podávání hlášení o rizicích, leden 2013, k dispozici on-line na adrese: http://www.bis.org/publ/bcbs239.pdf.

3.4 Souhrn zjištění a bodové hodnocení

61. Příslušné orgány by si měly na základě výše uvedeného posouzení utvořit názor o rizicích IKT instituce. Tento názor by se měl promítnout do souhrnu zjištění, která by příslušné orgány měly zohlednit při přidělování skóre operačnímu riziku v tabulce č. 6 Obecných pokynů orgánu EBA k procesu přezkoumání a vyhodnocení. Příslušné orgány by měly své stanovisko založit na podstatných rizicích IKT s přihlédnutím k následujícím posuzovaným faktorům a ty zohlednit v hodnocení operačního rizika:

a. Posuzované rizikové faktory

i. rizikový profil IKT a expozice instituce;
ii. identifikované kritické systémy a služby IKT; a
iii. podstatnost rizika IKT z hlediska kritických systémů IKT.

b. Posuzované faktory v oblasti řízení a kontrolních mechanismů

i. zda jsou zásady a strategie řízení rizik IKT instituce v souladu s její celkovou strategií a ochotou podstupovat riziko;
ii. zda je organizační rámec řízení rizik IKT stabilní, zda vlastníkům rizik a řídicím a kontrolním funkcím jasně vymezuje odpovědnosti a zda zřetelně odděluje jejich úlohy;
iii. zda jsou systémy pro měření, monitorování a vykazování rizik IKT přiměřené; a
iv. zda jsou rámce kontroly podstatných rizik IKT důkladné.

62. Pokud příslušné orgány považují riziko IKT za podstatné a rozhodnou se jej posuzovat a hodnotit jako dílčí kategorii operačního rizika, poskytuje jim níže uvedená tabulka (tabulka č. 1) faktory, které by měly při bodovém hodnocení rizik IKT zvážit.

Tabulka č. 1: Faktory, které orgány dohledu zohlední při určování skóre rizik IKT

Skóre rizika	Názor orgánů dohledu	Posuzované faktory u inherentního rizika	Posuzované faktory u přiměřeného řízení a kontrolních mechanismů
1	Vzhledem k úrovni inherentního rizika a k řízení a kontrolním mechanismům neexistuje zjistitelné riziko významného obezřetnostního dopadu na instituci.	• Zdroje informací zohledněné v souladu s odstavcem 37 neodhalily žádné významné expozice rizikům IKT. • Povaha rizikového profilu IKT instituce ani přezkoumání kritických systémů IKT a podstatných rizik systémů a služeb IKT neodhalily žádné podstatné riziko IKT.	
2	Vzhledem k úrovni inherentního rizika a k řízení a kontrolním mechanismům existuje nízké	• Zdroje informací zohledněné v souladu s odstavcem 37 neodhalily žádné významné expozice rizikům IKT. • Povaha rizikového profilu IKT instituce, spolu s přezkoumáním	• Zásady a strategie instituce v oblasti rizik IKT je

	zjistitelné riziko významného obezřetnostního dopadu na instituci.	kritických systémů IKT a podstatných rizik systémů a služeb IKT, odhalily jen omezenou expozici rizikům IKT (např. pouze ve 2 z 5 předem stanovených kategorií rizik IKT).	v souladu s její celkovou strategií a ochotou podstupovat riziko. • Organizační rámec řízení rizik IKT je stabilní, vlastníkům rizik a řídicím a kontrolním funkcím jasně vymezuje odpovědnosti a zřetelně odděluje jejich úlohy. • Systémy pro měření, monitorování a vykazování rizik IKT jsou přiměřené. • Rámec kontroly rizik IKT je důkladný.
3	Vzhledem k úrovni inherentního rizika a k řízení a kontrolním mechanismům existuje středně vysoké riziko významného obezřetnostního dopadu na instituci.	• Zdroje informací zohledněné v souladu s odstavcem 37 odhalily náznaky možné významné expozice rizikům IKT. • Povaha rizikového profilu IKT instituce, spolu s přezkoumáním kritických systémů IKT a podstatných rizik systémů a služeb IKT, odhalily zvýšenou expozici rizikům IKT (např. nejméně ve 3 z 5 předem stanovených kategorií rizik IKT).	
4	Vzhledem k úrovni inherentního rizika a k řízení a kontrolním mechanismům existuje vysoké zjistitelné riziko významného obezřetnostního dopadu na instituci.	• Zdroje informací zohledněné v souladu s odstavcem 37 odhalily četné náznaky možné významné expozice rizikům IKT. • Povaha rizikového profilu IKT instituce, spolu s přezkoumáním kritických systémů IKT a podstatných rizik systémů a služeb IKT, odhalily vysokou expozici rizikům IKT (např. ve 4 až 5 z 5 předem stanovených kategorií rizik IKT).	

Příloha – Klasifikace rizik IKT

5 kategorií rizik IKT s demonstrativním výčtem rizik IKT, která mají potenciálně vysoce závažné dopady a/nebo dopady na operace, reputaci nebo finance instituce

Kategorie rizik IKT	Rizika IKT (demonstrativní výčet[10])	Popis rizik	Příklady
Rizika spojená s dostupností a zachováním kontinuity IKT	Nedostatečné řízení kapacit	Nedostatek prostředků (např. hardwaru, softwaru, personálu, poskytovatelů služeb) může vést k neschopnosti škálovat službu podle podnikových potřeb, k narušení systémů, snížení výkonnosti služby a/nebo k chybné obsluze.	• Nedostatečná kapacita může ovlivnit přenosovou rychlost a dostupnost sítě (internetu) pro služby jako je internetové bankovnictví. • Nedostatek pracovníků (interních nebo třetích stran) může vést k narušení systému a/nebo k chybné obsluze.
	Selhání systémů IKT	Ztráta dostupnosti kvůli selháním hardwaru.	• Selhání / špatné fungování úložišť (pevných disků), serverů nebo jiného vybavení IKT způsobené například nedostatečnou údržbou.
		Ztráta dostupnosti kvůli selháním a chybám softwaru.	• Zacyklení aplikačního softwaru brání provedení transakce. • Výpadky kvůli neustálému používání zastaralých systémů a řešení IKT, které už nesplňují aktuální požadavky na dostupnost a odolnost a/nebo již nejsou ze strany prodejců podporovány.
	Nevhodné plány na zajištění kontinuity a obnovy IKT po katastrofě	Selhání řešení v oblasti zajištění plánované dostupnosti a/nebo kontinuity IKT a/nebo jejich obnovy po katastrofě (např. nouzová obnova datového centra) při jejich aktivaci v rámci reakce na mimořádnou událost.	• Rozdíly v konfiguraci primárního a sekundárního datového centra mohou vést k tomu, že nouzové datové centrum nedokáže plánovanou kontinuitu služby zajistit.
	Rušivé a ničivé kybernetické	Útoky za různým účelem (např. aktivismus, vydírání), které mohou přetížit systémy i síť a znemožnit	• Distribuované útoky s cílem odepření služeb (DoS) probíhají na internetu za použití množství

[10] Rizika IKT jsou uvedena v kategorii rizik, na níž mají největší dopad, mohou však mít dopad i na jiné kategorie

Kategorie rizik IKT	Rizika IKT (demonstrativní výčet[10])	Popis rizik	Příklady
	útoky	legitimním uživatelům přístup k on-line počítačové službě.	počítačových systémů, které hacker ovládá a jejichž prostřednictvím odesílá velký počet podle všeho legitimních požadavků na internetové služby (např. elektronické bankovnictví).
Rizika spojená se zabezpečením IKT	Kybernetické útoky a další rizika externích IKT	Útoky z internetu nebo vnějších sítí za různým účelem (např. podvod, špionáž, aktivismus/sabotáž, kybernetický terorismus) prováděné pomocí rozmanitých technik (např. sociální inženýrství, pokusy o narušení zneužitím slabin, nasazením škodlivého softwaru), jejichž výsledkem je převzetí kontroly nad interními systémy IKT.	Různé druhy útoků: • Pokročilá trvalá hrozba (Advanced Persistent Threat – APT) převzetí kontroly nad interními systémy nebo odcizení informací (např. krádež informací o identitě, o kreditních kartách). • Škodlivý software (např. ransomware), který zašifruje data s cílem vydírat jejich majitele. • Infikování interních systémů IKT trojskými viry, které umožní v systému skrytě provádět vadné akce. • Zneužití slabin systémů IKT a/nebo (webových) aplikací (např. prolomení SQL) s cílem získat přístup do interního systému IKT.
		Realizace podvodných transakcí poté, co hacker prolomí nebo obejde zabezpečení elektronického bankovnictví a platebních služeb a/nebo napadne a zneužije slabá místa zabezpečení interních platebních systémů instituce.	• Útoky na elektronické bankovnictví nebo platební služby s cílem uskutečnit neoprávněnou transakci. • Vytváření a odesílání podvodných platebních transakcí z interních platebních systémů instituce (např. podvodné swiftové zprávy).
		Provádění podvodných transakcí s cennými papíry poté, co hacker prolomí nebo obejde zabezpečení elektronického bankovnictví a získá současně přístup také k účtům s cennými papíry zákazníka.	• Útoky typu „pump and dump“, kdy útočníci získají přístup k účtům cenných papírů v elektronickém bankovnictví zákazníka a zadávají podvodné příkazy k nákupu nebo prodeji, aby ovlivnili tržní cenu cenných papíru a/nebo vydělali na pozicích, kterých cenné papíry dříve dosáhly.
		Útoky na komunikační připojení a konverzace všeho druhu nebo systémů IKT s cílem získat informace a/nebo spáchat podvod.	• Sledování/zachycování nechráněných přenosů autentizačních dat v prostém textu.

Kategorie rizik IKT	Rizika IKT (demonstrativní výčet[10])	Popis rizik	Příklady
	Nevhodné zabezpečení interních IKT	Získání neoprávněného přístupu ke kritickým systémům IKT zevnitř instituce k různým účelům (např. podvod, provádění a zamaskování nedovoleného obchodování, odcizení dat, aktivismus/sabotáž) různými technikami (např. zneužití a/nebo eskalace privilegií, krádež identity, sociální inženýrství, zneužití slabin systémů IKT, nasazení škodlivého softwaru).	• Instalace softwaru, který zaznamenává stisknuté klávesy (tzv. key stroke logger nebo key logger), s cílem ukrást identifikační údaje a hesla uživatele a získat tak neoprávněný přístup k důvěrným datům a/nebo spáchat podvod. • Prolomení/rozluštění slabých hesel s cílem získat nelegitimní nebo vyšší přístupová práva. • Systémový administrátor použije operační systémy a databázové utility (k přímé modifikaci databází) ke spáchání podvodu.
		Neoprávněná manipulace s IKT díky nevhodným postupům a praktikám řízení přístupu k IKT.	• Opomenutí deaktivovat nebo smazat nepotřebné účty, například účty pracovníků, kteří změnili funkci a/nebo z instituce odešli, včetně hostů nebo dodavatelů, kteří přístup již nepotřebují, a s tím související umožnění neoprávněného přístupu do systémů IKT. • Udělení zbytečně rozsáhlých přístupových práv a privilegií a s tím související umožnění neoprávněného přístupu a/nebo zakrytí nedovolených činností.
		Bezpečnostní hrozby vlivem nízké informovanosti o zabezpečení, kdy zaměstnanci nechápou, opomíjí nebo nedodržují zásady a postupy zabezpečení IKT.	• Zaměstnanci, kteří v mylné představě napomáhají útoku (tzn. sociální inženýrství). • Špatné postupy v oblasti přihlašovacích údajů: sdílení hesel, používání snadno rozluštitelných hesel, používání stejného hesla k mnoha různým účelům apod. • Ukládání nezašifrovaných důvěrných dat do notebooků a na přenosná úložiště (např. USB flash disky), která mohou být ztracena nebo odcizena.

Kategorie rizik IKT	Rizika IKT (demonstrativní výčet[10])	Popis rizik	Příklady
		Neoprávněné ukládání nebo přenos důvěrných informací mimo instituci.	• Osoby, které odcizí nebo úmyslně vyzradí nebo vynesou důvěrné informace nepovolaným osobám nebo veřejnosti.
	Nevhodné fyzické zabezpečení IKT	Zneužití nebo odcizení aktiv IKT prostřednictvím fyzického přístupu a způsobení škody, ztráty aktiv nebo dat nebo umožnění dalších hrozeb.	• Fyzické vloupání do kancelářských budov a/nebo datových center s cílem odcizit vybavení IKT (např. počítače, notebooky, úložiště) a/nebo zkopírovat data při fyzickém přístupu do systémů IKT.
		Úmyslné nebo náhodné poškození fyzických aktiv IKT v důsledku terorismu, nehod nebo nešťastné/nesprávné manipulace ze strany pracovníků instituce a/nebo třetích stran (dodavatelů, opravářů).	• Fyzický terorismus (tzn. teroristické bombové útoky) nebo sabotáž aktiv IKT. • Zničení datového centra při požáru, úniku vody nebo jiných okolnostech.
		Nedostatečná fyzická ochrana proti přírodním katastrofám, která má za následek částečné nebo úplné zničení systémů IKT / datových center při živelné pohromě.	• Zemětřesení, extrémně vysoké teploty, vichřice, siné vánice, záplavy, požár, zásah bleskem.
Rizika spojená se změnou IKT	Nevhodné mechanismy kontroly změn systémů IKT a vývoje IKT	Mimořádné události vyvolané neodhalenými chybami nebo slabinami vzniklými při změně (např. nepředvídané vlivy změny nebo špatně řízená změna vlivem nedostatečného testování nebo nevhodných postupů řízení změn) například softwaru, systémů IKT nebo dat.	• Uvolnění nedostatečně otestovaných změn softwaru nebo konfigurace do produkčního prostředí s nečekaně nepříznivými dopady na data (např. poškození, výmaz) a/nebo výkonnost systémů IKT (např. pád systému, pokles výkonnosti). • Nekontrolované změny systémů IKT nebo dat v produkčním prostředí. • Uvolnění špatně zabezpečených systémů IKT a internetových aplikací do produkčního prostředí a vytvoření příležitostí pro útoky hackerů na poskytované internetové služby a/nebo k prolomení interních systémů IKT. • Nekontrolované změny zdrojového kódu interně vyvíjeného softwaru. • Nedostatečné testování bez vhodných testovacích prostředí.

Kategorie rizik IKT	Rizika IKT (demonstrativní výčet[10])	Popis rizik	Příklady
	Nevhodná architektura IKT	Špatná správa architektury IKT při navrhování, tvorbě a údržbě systémů IKT (např. softwaru, hardwaru, dat) může časem vést k vytvoření spletitých, složitých, z hlediska nákladů na správu náročných a nepružných systémů IKT, které nadále nevyhovují potřebám instituce a nedostačují skutečným požadavkům na řízení rizik.	• Nevhodně řízené změny systémů IKT, softwaru a/nebo dat po delší dobu, které vyústí ve složitou, nerovnoměrnou a obtížnou správu systémů a architektury IKT s mnoha negativními dopady na řízení obchodní činnosti i rizik (např. nedostatečná flexibilita a odezva, nehody a selhání IKT, vysoké provozní náklady, oslabené zabezpečení a odolnost IKT, zhoršená kvalita dat a snížená schopnost podávat zprávy). • Nadměrné úpravy a rozšíření komerčních softwarových sad interně vyvíjeným softwarem, které znemožní implementaci v budoucnu vydaných verzí a upgradů daného komerčního softwaru a ohrozí tak poskytování podpory ze strany prodejce.
	Nevhodné řízení životního cyklu a aktualizací	Neschopnost vést patřičnou evidenci všech aktiv IKT na podporu řádných postupů řízení životního cyklu a aktualizací a v kombinaci s nimi. Výsledkem jsou nedostatečně aktualizované (a tím pádem náchylnější) a zastaralé systémy IKT, které nemusí odpovídat potřebám řízení obchodní činnosti a rizik.	• Neaktualizované a zastaralé systémy IKT, které mohou nepříznivě ovlivňovat řízení obchodní činnosti i rizik (např. nedostatečná flexibilita a odezva, výpadky IKT, oslabené zabezpečení a odolnost IKT).
Rizika ohrožení integrity dat IKT	Nefunkční zpracování dat IKT nebo manipulace s nimi	Data mohou být vlivem chyb nebo selhání systémů, komunikace a/nebo aplikací, nebo nesprávně provedeného procesu jejich extrakce, transformace a naplnění (ETL) poškozena nebo ztracena.	• Chyba informačního systému při dávkovém zpracování, která vede k nesprávným zůstatkům na bankovních účtech klientů. • Špatně provedené dotazy. • Ztráta dat kvůli chybě při jejich replikaci (zálohování).
	Špatně navržené kontrolní mechanismy pro validaci dat	Chyby související s chybějícími nebo neúčinnými mechanismy kontroly automatizovaných datových vstupů a jejich akceptace (např. při využití dat třetí strany), přenosu dat, zpracování a výstupů v systémech	• Nedostatečné nebo neplatné formátování/ověřování datových vstupů v aplikacích a uživatelských rozhraních. • Absence kontrolních mechanismů pro srovnávání

Kategorie rizik IKT	Rizika IKT (demonstrativní výčet[10])	Popis rizik	Příklady
	v systémech IKT	IKT (např. kontrola validity vstupních dat, srovnávání dat).	dat ve vytvořených výstupech. • Absence kontrolních mechanismů v procesech extrakce dat (např. databázových dotazech) mající za následek nepřesná data. • Použití chybných externích dat.
	Špatně kontrolované změny dat v produkčních systémech IKT.	Zadání chybných dat kvůli nedostatku mechanismů pro kontrolu správnosti a oprávněnosti manipulace s daty v produkčních systémech IKT.	• Vývojáři nebo administrátoři databází, kteří mají nekontrolovaný přímý přístup k datům v produkčních systémech IKT a k jejich změnám, například při mimořádné události v oblasti IKT.
	Špatně navržená a/nebo spravovaná architektura dat, datové toky, datové modely nebo datové slovníky	Špatně spravovaná architektura dat, datové modely, datové toky nebo datové slovníky mohou zapříčinit vznik několika verzí stejných dat v systémech IKT, které již dále nejsou kvůli rozdílně aplikovaným datovým modelům nebo definicím konzistentní, a/nebo rozdílů v základních procesech tvorby a změn dat.	• Existence různých zákaznických databází u jednotlivých produktů nebo organizačních jednotek s různými datovými definicemi a poli, která má za následek neslučitelné a obtížně srovnatelné a začlenitelné údaje o zákaznících na úrovni celé finanční instituce nebo skupiny.
Rizika spojená s externím zajištěním IKT	Nedostatečná odolnost služeb třetí strany nebo jiného subjektu skupiny	Nedostupnost kritických externě zajišťovaných služeb IKT, telekomunikačních služeb a technické infrastruktury. Ztráta nebo poškození kritických/citlivých dat svěřených poskytovateli služeb.	• Nedostupnost klíčových služeb v důsledku selhání (externě zajišťovaných) systémů IKT nebo aplikací dodavatelů. • Přerušení telekomunikačního připojení. • Výpadek elektrické energie.
	Nevhodný systém řízení a kontroly externího zajištění	Závažné snížení výkonnosti nebo selhání služeb kvůli nedostatečné připravenosti nebo kontrolním procesům poskytovatele externě zajišťovaných služeb. Neúčinný systém řízení a kontroly externího zajištění může vést k nedostatku vhodných schopností a kapacit k úplné identifikaci, hodnocení, snižování a monitorování rizik IKT a může omezit operační schopnosti.	• Špatné postupy zvládání mimořádných událostí, smluvní kontrolní mechanismy a záruky zakotvené ve smlouvě s poskytovatelem služeb, které zvyšují závislost klíčových osob na třetích stranách a prodejcích. • Nevhodné kontrolní mechanismy řízení změn v oblasti prostředí IKT poskytovatele služby mohou vést k závažnému snížení výkonnosti nebo selhání

Kategorie rizik IKT	Rizika IKT (demonstrativní výčet[10])	Popis rizik	Příklady
			služby.
	Nedostatečné zabezpečení třetí strany nebo jiného subjektu skupiny	Nabourání systémů IKT třetí stranou, která je poskytovatelem služeb, s přímým dopadem na externě zajišťované služby nebo kritická/důvěrná data uložená u poskytovatele služeb. Pracovníci poskytovatele služeb, kteří získají neoprávněný přístup ke kritickým/citlivým datům uloženým u poskytovatele služeb.	• Nabourání poskytovatelů služeb zločinci nebo teroristy, kteří tak získají přístup k systémům IKT institucí nebo k jejich kritickým či citlivým datům uloženým u poskytovatelů služeb a mohou tak tato data zničit. • Zasvěcené osoby s nekalými úmysly, které působí u poskytovatele služeb, se pokusí citlivá data ukrást a prodat.