Obecné pokyny

EBA/GL/2019/04

28. listopadu 2019

Obecné pokyny Evropského orgánu pro bankovnictví pro řízení rizik v oblasti IKT a bezpečnosti

Dodržování předpisů a oznamovací povinnosti

Status těchto obecných pokynů

1. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení (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 právní předpisy Evropské unie 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 se jimi měly řídit a začlenit je do svých postupů (např. pozměněním svého právního rámce nebo dohledových postupů), včetně případů, kdy jsou obecné pokyny zaměřeny v prvé řadě na instituce.

Oznamovací povinnosti

3. Podle čl. 16 odst. 3 nařízení (EU) č. 1093/2010 musí příslušné orgány do ([dd.mm.rrrr]) orgánu EBA oznámit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě do tohoto data uvést 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/2019/04“. Oznámení by měly předložit osoby s příslušným oprávněním oznamovat, zda se jejich příslušné orgány těmito obecnými pokyny řídí nebo hodlají řídit. Jakoukoli změnu stavu dodržování obecných 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).

Předmět, oblast působnosti a definice

Předmět

5. Tyto obecné pokyny vycházejí z ustanovení článku 74 směrnice 2013/36/EU (směrnice o kapitálových požadavcích, CRD) týkajících se vnitřní správy a řízení a jsou vydány na základě mandátu vypracovat obecné pokyny, který uvádí čl. 95 odst. 3 směrnice (EU) 2015/2366 (2. směrnice o platebních službách, PSD2).

6. Tyto obecné pokyny upřesňují opatření k řízení rizik, která podle článku 74 směrnice CRD musí přijmout finanční instituce (vymezené v bodě 9 níže) k řízení svých rizik v oblasti IKT a bezpečnosti u všech činností a která musí podle čl. 95 odst. 1 směrnice PSD2 přijmout poskytovatelé platebních služeb (vymezení v bodě 9 níže) k řízení operačních a bezpečnostních rizik (ve smyslu „rizik v oblasti IKT a bezpečnosti“) souvisejících s jimi poskytovanými platebními službami. Obecné pokyny obsahují požadavky týkající se bezpečnosti informací, včetně kybernetické bezpečnosti, a to v rozsahu, v němž jsou tyto informace uchovávány v systémech IKT.

Oblast působnosti

7. Tyto obecné pokyny se použijí ve vztahu k řízení rizik v oblasti IKT a bezpečnosti v rámci finančních institucí (vymezených v bodě 9). Pro účely těchto obecných pokynů se výraz „rizika v oblasti IKT a bezpečnosti“ týká operačních a bezpečnostních rizik ve smyslu článku 95 směrnice PSD2 pro účely poskytování platebních služeb.

8. U poskytovatelů platebních služeb (vymezených v bodě 9) se tyto obecné pokyny použijí na poskytování platebních služeb v souladu s oblastí působnosti článku 95 směrnice PSD2 a mandátem na základě uvedeného článku. U institucí (vymezených v odstavci 9) se tyto obecné pokyny použijí na veškeré jimi zajišťované činnosti.

Subjekty, na které se tyto pokyny vztahují

9. Tyto obecné pokyny jsou určeny finančním institucím, které pro účely těchto obecných pokynů zahrnují 1) poskytovatele platebních služeb ve smyslu čl. 4 odst. 11 směrnice PSD2 a 2) instituce, které jsou úvěrovými institucemi a investičními podniky ve smyslu čl. 4 odst. 1 bodu 3 nařízení (EU) č. 575/2013. Tyto obecné pokyny se rovněž použijí na příslušné orgány ve smyslu čl. 4 odst. 1 bodu 40 nařízení (EU) č. 575/2013, mezi něž patří i Evropská centrální banka, pokud jde o záležitosti vztahující se k úkolům, které jí byly svěřeny nařízením (EU) č. 1024/2013, a na příslušné orgány podle směrnice PSD2 ve smyslu čl. 4 odst. 2 bodu i) nařízení (EU) č. 1093/2010.

Definice

10. Není-li uvedeno jinak, pojmy použité a vymezené ve směrnici 2013/36/EU (CRD), v nařízení (EU) č. 575/2013 (CRR) a ve směrnici (EU) 2015/2366 (PSD2) mají v těchto obecných pokynech stejný význam. Kromě toho se pro účely těchto obecných pokynů použijí tyto definice:

Riziko v oblasti IKT a bezpečnosti	Riziko ztráty v důsledku porušení důvěrnosti, selhání integrity systémů a dat, nevhodnosti nebo nedostupnosti systémů a dat nebo neschopnosti změnit IT v přiměřeném čase a s přiměřenými náklady, pokud se mění prostředí nebo požadavky vyplývající z obchodní činnosti (tj. flexibilita)[2]. Patří sem bezpečnostní rizika vyplývající z nedostatečnosti či selhání vnitřních postupů nebo z vnějších událostí včetně kybernetických útoků či z nedostatečného fyzického zabezpečení.
Vedoucí orgán	(a) Pro úvěrové instituce a investiční podniky má tento pojem stejný význam jako definice v čl. 3 odst. 1 bodě 7 směrnice 2013/36/EU. (b) Pro platební instituce nebo instituce elektronických peněz se pod tímto pojmem rozumí vedoucí pracovníci nebo osoby odpovědné za řízení platebních institucí nebo institucí elektronických peněz, případně osoby odpovědné za řízení činností v oblasti platebních služeb prováděných platebními institucemi nebo institucemi elektronických peněz. (c) Pro poskytovatele platebních služeb podle čl. 1 odst. 1 písm. c), e) a f) směrnice (EU) 2015/2366 má tento pojem význam, který mu přiznávají platné unijní nebo vnitrostátní právní předpisy.
Provozní nebo bezpečnostní incident	Jednorázová událost nebo řada souvisejících událostí neplánovaných finanční institucí, která má nebo pravděpodobně bude mít nepříznivý dopad na integritu, dostupnost, důvěrnost a/nebo autenticitu služeb.
Vrcholné vedení	(a) Pro úvěrové instituce a investiční podniky má tento pojem stejný význam jako definice v čl. 3 odst. 1 bodě 9 směrnice 2013/36/EU. (b) Pro platební instituce a instituce elektronických peněz se tímto pojmem rozumí fyzické osoby, které zastávají výkonné funkce v rámci instituce a které se zodpovídají vedoucímu orgánu za každodenní řízení instituce. (c) Pro poskytovatele platebních služeb podle čl. 1 odst. 1 písm. c), e) a f) směrnice (EU) 2015/2366 má tento pojem význam, který mu přiznávají platné unijní nebo vnitrostátní právní předpisy.

[2] Definice z obecných pokynů orgánu EBA ke společným postupům a metodikám procesu přezkumu a vyhodnocení ze dne 19. prosince 2014 (EBA/GL/2014/13) ve znění obecných pokynů EBA/GL/2018/03.

Ochota podstupovat riziko	Souhrnná míra a druhy rizika, které jsou poskytovatelé platebních služeb a instituce ochotni podstupovat v rámci své schopnosti nést riziko v souladu se svým obchodním modelem, aby dosáhli svých strategických cílů.
Funkce auditu	(a) Pro úvěrové instituce a investiční podniky funkce auditu odpovídá funkci podle oddílu 22 obecných pokynů orgánu EBA k vnitřnímu systému správy a řízení (EBA/GL/2017/11). (b) Pro jiné poskytovatele platebních služeb než úvěrové instituce musí být funkce auditu nezávislá v rámci tohoto poskytovatele platebních služeb nebo na tomto poskytovateli platebních služeb a může být funkcí interního a/nebo externího auditu.
Projekty v oblasti IKT	Jakýkoli projekt nebo část projektu, v němž dochází k výměně, náhradě, likvidaci nebo zavádění systémů a služeb v oblasti IKT. Projekty v oblasti IKT mohou být součástí širších programů transformace v oblasti IKT nebo obchodní činnosti.
Třetí strana	Organizace, která vstoupila do obchodních vztahů nebo smluv se subjektem za účelem poskytování produktu nebo služby[3].
Informační aktivum	Shromážděné informace, hmotné nebo nehmotné, které je třeba chránit.
Aktivum v oblasti IKT	Aktivum spočívající v softwaru nebo hardwaru, které se nachází v obchodním prostředí.
Systémy IKT[4]	Dílčí funkční celky zajišťující podporu procesů instituce pomocí informačních a komunikačních technologií.
Služby v oblasti IKT[5]	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.

Provádění

Datum použití

11. Tyto obecné pokyny se použijí ode dne 30. června 2020.

Zrušení

12. Těmito obecnými pokyny budou k datu jejich vstupu v platnost zrušeny obecné pokyny k bezpečnostním opatřením v souvislosti s operačními a bezpečnostními riziky (EBA/GL/2017/17) vydané v roce 2017.

[3] Definice základních prvků řízení rizika kybernetické bezpečnosti třetích stran ve finančním sektoru podle skupiny G7.
[4] Definice z obecných pokynů k posuzování rizik v oblasti IKT v rámci procesu přezkoumání a vyhodnocení (EBA/GL/2017/05).
[5] Tamtéž.

Obecné pokyny pro řízení rizik v oblasti IKT a bezpečnosti

1.1. Proporcionalita

1. Všechny finanční instituce by měly dodržovat ustanovení těchto obecných pokynů způsobem, který bude přiměřený velikosti finančních institucí, jejich vnitřní organizaci a povaze, rozsahu, složitosti a rizikovosti služeb a produktů, jež finanční instituce poskytují nebo hodlají poskytovat, a který bude uvedené aspekty brát v úvahu.

1.2. Správa, řízení a strategie

1.2.1. Správa a řízení

2. Vedoucí orgán by měl zajistit, aby finanční instituce měly zaveden odpovídající rámec vnitřní správy a řízení a vnitřní kontroly pro jejich rizika v oblasti IKT a bezpečnosti. Vedoucí orgán by měl stanovit jasné úkoly a povinnosti pro funkce v oblasti IKT, řízení rizik bezpečnosti informací a kontinuitu činnosti, a to i pro vedoucí orgán a jeho výbory.
3. Vedoucí orgán by měl zajistit, aby počet zaměstnanců finančních institucí a jejich dovednosti byly přiměřené pro průběžnou podporu provozních potřeb institucí a jejich postupů pro řízení rizik v oblasti IKT a bezpečnosti a pro zajištění realizace jejich strategie v oblasti IKT. Vedoucí orgán by měl zajistit, aby přidělený rozpočet odpovídal plnění výše uvedeného cíle. Finanční instituce by dále měly zajistit, aby všichni zaměstnanci včetně osob v klíčových funkcích jednou ročně nebo v případě potřeby častěji absolvovali vhodné školení odborné přípravy se zaměřením na rizika v oblasti IKT a bezpečnosti, včetně bezpečnosti informací (viz také oddíl 1.4.7).
4. Vedoucí orgán nese celkovou odpovědnost za stanovení a schvalování strategie finančních institucí v oblasti IKT v rámci celkové obchodní strategie institucí a za dohled nad prováděním této strategie, jakož i za vytvoření účinného rámce řízení rizik v oblasti IKT a bezpečnosti.

1.2.2. Strategie

5. Strategie v oblasti IKT by měla být v souladu s celkovou obchodní strategií finančních institucí a měla by vymezovat:
    a) jak by se měly IKT finančních institucí vyvíjet, aby účinně podporovaly jejich obchodní strategii a podílely se na ní, včetně vývoje organizační struktury, změn v systému IKT a klíčových vztahů závislosti na třetích stranách;
    b) plánovanou strategii a vývoj architektury IKT, včetně vztahů závislosti na třetích stranách;

c) jasné cíle v oblasti bezpečnosti informací se zaměřením na systémy IKT a služby, zaměstnance a procesy v oblasti IKT.

6. Finanční instituce by měly stanovit soubory akčních plánů, které budou obsahovat opatření, jež mají být přijata k dosažení cíle strategie v oblasti IKT. Tyto plány by měly být sděleny všem příslušným zaměstnancům (včetně dodavatelů a externích poskytovatelů, pokud jsou pro ně použitelné a významné). Akční plány by měly být pravidelně přezkoumávány, aby se zajistila jejich relevance a přiměřenost. Finanční instituce by také měly zavést procesy ke sledování a měření účinnosti provádění jejich strategie v oblasti IKT.

1.2.3. Využívání externích poskytovatelů

7. Aniž jsou dotčeny obecné pokyny orgánu EBA k outsourcingu (EBA/GL/2019/02) a článek 19 směrnice PSD2, měly by finanční instituce zajistit účinnost opatření ke zmírnění rizik, jak je definuje jejich rámec řízení rizik, včetně opatření stanovených v těchto obecných pokynech, pokud jsou provozní funkce platebních služeb nebo služeb v oblasti IKT a systémů IKT v jakékoli činnosti zajišťovány externě, a to i vůči subjektům ve skupině nebo při využívání třetích stran.
8. Aby byla zajištěna kontinuita služeb v oblasti IKT a systémů IKT, měly by finanční instituce zajistit, aby smlouvy a dohody o úrovni služeb (za běžných okolností i v případě přerušení služby – viz také oddíl 1.7.2) s poskytovateli (poskytovatelé v rámci outsourcingu, subjekty ve skupině nebo externí poskytovatelé) zahrnovaly:
    a) vhodné a přiměřené cíle a opatření související s bezpečností informací včetně požadavků, jako jsou minimální požadavky na kybernetickou bezpečnost; specifikace životního cyklu dat finanční instituce; veškeré požadavky týkající se šifrování dat, procesů zabezpečení sítě a sledování bezpečnosti a umístění datových center;
    b) provozní postupy a postupy pro řešení bezpečnostních incidentů včetně předávání na vyšší úroveň řízení a podávání zpráv.
9. Finanční instituce by měly sledovat, zda tito poskytovatelé zajišťují správnou úroveň bezpečnostních cílů, opatření a provozních úkolů finanční instituce, a měly by se snažit získat v tomto ohledu dostatečné ujištění.

1.3. Rámec řízení rizik v oblasti IKT a bezpečnosti

1.3.1. Organizace a cíle

10. Finanční instituce by měly identifikovat a řídit svá rizika v oblasti IKT a bezpečnosti. Funkce IKT odpovědné za systémy, procesy a bezpečnostní operace IKT by měly mít zavedeny vhodné postupy a kontroly, aby bylo zajištěno, že všechna rizika budou identifikována, analyzována, měřena, sledována, řízena, vykazována a udržována v mezích ochoty finanční instituce podstupovat riziko a že realizované projekty a systémy a prováděné činnosti budou v souladu s externími a interními požadavky.
11. Finanční instituce by měly odpovědností za řízení rizik v oblasti IKT a bezpečnosti a za dohled nad těmito riziky pověřit kontrolní funkci, která bude dodržovat požadavky oddílu 19 obecných pokynů orgánu EBA k vnitřnímu systému správy a řízení (EBA/GL/2017/11). Finanční instituce

by měly zajistit nezávislost a objektivitu této kontrolní funkce tak, že ji vhodným způsobem oddělí od procesů činnosti IKT. Tato kontrolní funkce by měla být přímo odpovědná vedoucímu orgánu a měla by odpovídat za sledování a kontrolu dodržování rámce řízení rizik v oblasti IKT a bezpečnosti. Měla by zajistit, aby byla rizika v oblasti IKT a bezpečnosti identifikována, měřena, hodnocena, řízena, sledována a vykazována. Finanční instituce by měly zajistit, aby tato kontrolní funkce nenesla odpovědnost za žádný interní audit.

Funkce interního auditu by na základě přístupu založeného na riziku měla mít schopnost samostatně přezkoumávat soulad všech činností a jednotek finanční instituce souvisejících s IKT a bezpečností se zásadami a postupy finanční instituce a s externími požadavky a poskytovat v tomto ohledu objektivní jistotu, a to při dodržení požadavků oddílu 22 obecných pokynů orgánu EBA k vnitřnímu systému správy a řízení (EBA/GL/2017/11).

12. Finanční instituce by měly vymezit a přiřadit klíčové úlohy a povinnosti a příslušné hierarchické vztahy, aby byl rámec pro řízení rizik v oblasti IKT a bezpečnosti účinný. Tento rámec by měl být plně integrován do celkových procesů řízení rizik finančních institucí a měl by s nimi být sladěn.

13. Rámec řízení rizik v oblasti IKT a bezpečnosti by měl zahrnovat procesy zavedené s cílem:

    a) určit ochotu podstupovat rizika v oblasti IKT a bezpečnosti v souladu s ochotou finanční instituce podstupovat riziko;
    b) identifikovat a posoudit rizika v oblasti IKT a bezpečnosti, jimž je finanční instituce vystavena;
    c) definovat zmírňující opatření (včetně kontrol) ke zmírnění rizik v oblasti IKT a bezpečnosti;
    d) sledovat účinnost těchto opatření a počet oznámených incidentů, včetně incidentů u poskytovatelů platebních služeb oznamovaných podle článku 96 směrnice PSD2, které mají dopad na činnosti související s IKT, a v případě potřeby přijmout kroky k nápravě opatření;
    e) oznamovat vedoucímu orgánu rizika a kontroly v oblasti IKT a bezpečnosti;
    f) identifikovat a posoudit, zda existují rizika v oblasti IKT a bezpečnosti vyplývající z jakékoli významné změny v systému IKT nebo službách, procesech či postupech v oblasti IKT nebo v návaznosti na jakýkoli významný provozní nebo bezpečnostní incident.

14. Finanční instituce by měly zajistit, aby rámec řízení rizik v oblasti IKT a bezpečnosti byl řádně zdokumentován a soustavně zdokonalován na základě poznatků získaných během jeho provádění a sledování. Vedoucí orgán by měl alespoň jednou ročně schvalovat a přezkoumávat rámec řízení rizik v oblasti IKT a bezpečnosti.

1.3.2. Identifikace funkcí, procesů a aktiv

15. Finanční instituce by měly identifikovat, zřídit a aktualizovat mapování svých obchodních funkcí, úloh a podpůrných procesů, aby identifikovaly jejich význam a jejich vzájemné závislosti související s riziky v oblasti IKT a bezpečnosti.

16. Kromě toho by finanční instituce měly identifikovat, zřídit a aktualizovat mapování informačních aktiv podporujících jejich obchodní funkce a podpůrné procesy, jako jsou systémy IKT, zaměstnanci, dodavatelé, třetí strany a závislosti na jiných interních a externích systémech

a procesech, aby byly schopny řídit alespoň informační aktiva, která podporují jejich kritické obchodní funkce a procesy.

1.3.3. Klasifikace a posouzení rizik

17. Finanční instituce by měly klasifikovat identifikované obchodní funkce, podpůrné procesy a informační aktiva podle bodů 15 a 16 z hlediska jejich kritičnosti.

18. Za účelem definování kritičnosti těchto identifikovaných obchodních funkcí, podpůrných procesů a informačních aktiv by finanční instituce měly zvážit alespoň požadavky týkající se důvěrnosti, integrity a dostupnosti. Měly by existovat jasně přiřazené povinnosti a odpovědnosti týkající se informačních aktiv.

19. Finanční instituce by při posuzování rizik měly přezkoumat přiměřenost klasifikace informačních aktiv a příslušné dokumentace.

20. Finanční instituce by měly identifikovat rizika v oblasti IKT a bezpečnosti, která mají dopad na identifikované a klasifikované obchodní funkce, podpůrné procesy a informační aktiva, a to podle jejich kritičnosti. Toto posouzení rizik by mělo být prováděno a zdokumentováno jednou ročně nebo v případě potřeby v kratších intervalech. Tato posouzení rizik by měla být rovněž prováděna při všech velkých změnách infrastruktury, procesů nebo postupů ovlivňujících obchodní funkce, podpůrných procesů nebo informačních aktiv, a na základě toho by mělo být aktualizováno současné posouzení rizik finančních institucí.

21. Finanční instituce by měly zajistit průběžné sledování hrozeb a zranitelností významných pro jejich obchodní procesy, podpůrné funkce a informační aktiva a pravidelně přezkoumávat scénáře rizik, které na ně mají dopad.

1.3.4. Zmírňování rizik

22. Na základě posouzení rizik by finanční instituce měly určit, jaká opatření jsou nutná ke zmírnění identifikovaných rizik v oblasti IKT a bezpečnosti na přijatelnou úroveň a zda jsou zapotřebí změny stávajících obchodních procesů, kontrolních opatření, systémů IKT a služeb v oblasti IKT. Finanční instituce by měla zvážit čas potřebný k provedení těchto změn a čas na přijetí příslušných prozatímních opatření ke zmírnění rizik, která budou minimalizovat rizika v oblasti IKT a bezpečnosti v mezích ochoty finanční instituce tato rizika podstupovat.

23. Finanční instituce by měly vymezit a provádět opatření ke zmírnění identifikovaných rizik v oblasti IKT a bezpečnosti a k ochraně informačních aktiv v souladu s jejich klasifikací.

1.3.5. Oznamování

24. Finanční instituce by měly vedoucímu orgánu jasně a včas oznamovat výsledky posouzení rizik. Tímto oznamováním není dotčena povinnost poskytovatelů platebních služeb předkládat příslušným orgánům aktualizované a komplexní posouzení rizik podle čl. 95 odst. 2 směrnice (EU) 2015/2366.

1.3.6. Audit

25. Správa a řízení, systémy a procesy finanční instituce týkající se jejích rizik v oblasti IKT a bezpečnosti by měly být předmětem pravidelného auditu, který provedou auditoři s dostatečnými znalostmi, dovednostmi a odborností týkající se rizik v oblasti IKT a bezpečnosti a plateb (v případě poskytovatelů platebních služeb), aby vedoucímu orgánu poskytli nezávislé ujištění o jejich účinnosti. Auditoři by měli být v rámci finanční instituce nebo na dané finanční instituci nezávislí. Četnost a zaměření těchto auditů by měly odpovídat příslušným rizikům v oblasti IKT a bezpečnosti.
26. Vedoucí orgán finanční instituce by měl schválit plán auditů, včetně všech auditů IKT a jakýchkoli jejich podstatných změn. Plán auditu a jeho provádění, včetně četnosti auditů, by měly odrážet přirozená rizika v oblasti IKT a bezpečnosti finanční instituce, měly by být těmto rizikům úměrné a měly by být pravidelně aktualizovány.
27. Měl by být zaveden formální návazný postup, který bude obsahovat opatření pro včasné ověření a nápravu kritických zjištění auditu IKT.

1.4. Bezpečnost informací

1.4.1. Politika bezpečnosti informací

28. Finanční instituce by měly vypracovat a zdokumentovat politiku bezpečnosti informací, která by měla vymezit nejdůležitější zásady a pravidla za účelem ochrany důvěrnosti, integrity a dostupnosti dat a informací finančních institucí a jejich zákazníků. Pro poskytovatele platebních služeb je tato politika určena v bezpečnostním předpisu, který má být přijat podle čl. 5 odst. 1 písm. j) směrnice (EU) 2015/2366. Politika bezpečnosti informací by měla být v souladu s cíli finanční instituce v oblasti bezpečnosti informací a měla by být založena na příslušných výsledcích procesu posouzení rizik. Politika by měla být schválena vedoucím orgánem.
29. Politika by měla zahrnovat popis hlavních úloh a povinností v oblasti řízení bezpečnosti informací a měla by stanovit požadavky na zaměstnance a dodavatele, procesy a technologie v souvislosti s bezpečností informačních systémů a uznat, že zaměstnanci a dodavatelé na všech úrovních mají určité povinnosti při zajišťování bezpečnosti informací finančních institucí. Politika by měla zajistit důvěrnost, integritu a dostupnost kritických logických a fyzických aktiv, zdrojů a citlivých údajů finanční instituce, ať už jsou uloženy, přenášejí se, nebo jsou využívány. Politika bezpečnosti informací by měla být sdělena všem zaměstnancům a dodavatelům finanční instituce.
30. Na základě politiky bezpečnosti informací by finanční instituce měly zavést a provádět bezpečnostní opatření ke zmírnění rizik v oblasti IKT a bezpečnosti, jimž jsou vystaveny. Tato opatření by měla zahrnovat:
    a) organizaci a správu a řízení v souladu s body 10 a 11;
    b) logická bezpečnost (oddíl 1.4.2);
    c) fyzická bezpečnost (oddíl 1.4.3);
    d) bezpečnost provozu IKT (oddíl 1.4.4);

e) bezpečnostní monitorování (oddíl 1.4.5);
f) přezkumy, hodnocení a testování bezpečnosti informací (oddíl 1.4.6);
g) odbornou přípravu a informovanost v oblasti bezpečnosti informací (oddíl 1.4.7).

1.4.2. Logická bezpečnost

31. Finanční instituce by měly definovat, zdokumentovat a provádět postupy kontroly logického přístupu (řízení totožnosti a přístupu). Tyto postupy by měly být prováděny, vymáhány, sledovány a pravidelně přezkoumávány. Jejich součástí by měly být i kontroly za účelem sledování anomálií. Tyto postupy by měly zavést alespoň dále uvedené prvky, přičemž výraz „uživatel“ zahrnuje i technické uživatele:

(a) **Vědět jen to potřebné, zásada minimálních práv a oddělení funkcí:** Finanční instituce by měly práva přístupu k informačním aktivům a ke svým podpůrným systémům spravovat na základě zásady „vědět jen to potřebné“, a to i v případě vzdáleného přístupu. Uživatelům by měla být udělena minimální přístupová práva, která jsou nezbytně nutná k plnění jejich povinností (zásada „minimálních práv“), aby se zabránilo neoprávněnému přístupu k velkému souboru dat nebo aby se předešlo přidělení kombinací přístupových práv, které lze použít k obcházení kontrolních prvků (zásada „oddělení funkcí“).
(b) **Individuální odpovědnost uživatele:** Finanční instituce by měly v co nejvyšší míře omezit používání obecných a sdílených uživatelských účtů a u akcí prováděných v systémech IKT by měly zajistit možnost identifikovat uživatele.
(c) **Privilegovaná přístupová práva:** Finanční instituce by měly zavést přísné prvky kontroly p**rivilegovaných přístupů** do systému pomocí přísného omezení účtů se zvýšenými právy přístupu k systému (např. účtů administrátora) a měly by nad těmito účty zajišťovat pečlivý dohled. Aby byla zajištěna bezpečná komunikace a snížena rizika, měl by být vzdálený administrativní přístup ke kritickým systémům IKT poskytován pouze na základě zásady „vědět jen to potřebné“, a měla by být používána účinná řešení pro ověřování identity.
(d) **Vedení záznamů o činnostech uživatelů:** Je třeba zajistit vedení auditních záznamů a monitorování týkající se alespoň veškerých činností privilegovaných uživatelů. Záznamy o přístupu by měly být zabezpečeny tak, aby se předešlo jejich neoprávněným úpravám nebo výmazu, a měly by být uloženy po dobu odpovídající kritičnosti identifikovaných obchodních funkcí, podpůrných procesů a informačních aktiv v souladu s oddílem 1.3.3, aniž by byly dotčeny požadavky na uchovávání údajů stanovené v unijních a vnitrostátních právních předpisech. Finanční instituce by měla tyto informace používat k usnadnění identifikace a vyšetřování neobvyklých činností, které byly zjištěny při poskytování služeb.
(e) **Řízení přístupu:** Přístupová práva by měla být udělována, odebírána nebo upravována včas, a to podle předdefinovaných postupů schvalování, které zahrnují obchodního vlastníka informací, k nimž se přistupuje (vlastník informačního aktiva). V případě ukončení pracovního poměru by měla být přístupová práva okamžitě odebrána.

(f) **Revize přístupových oprávnění**: Přístupová práva by měla být pravidelně přezkoumávána s cílem zajistit, aby uživatelé nepožívali nadměrných výsad a aby byla přístupová práva odebrána, jakmile již nebudou zapotřebí.

(g) **Metody ověření:** Finanční instituce by měly prosazovat metody ověření, které jsou dostatečně robustní, aby přiměřeně a účinně zajistily dodržování zásad a postupů kontroly přístupu. Metody ověření by měly odpovídat kritičnosti systémů IKT, informací nebo procesu, k nimž se přistupuje. Měly by zahrnovat přinejmenším složitá hesla nebo silnější metody ověření (například dvoufaktorové ověření) podle příslušného rizika.

32. Elektronický přístup prostřednictvím aplikací k datům a systémům IKT by měl být omezen na minimum, které je nutné k poskytování příslušné služby.

1.4.3. Fyzická bezpečnost

33. Je třeba vymezit, zdokumentovat a provádět opatření pro fyzické zabezpečení finančních institucí na ochranu jejich prostor, datových center a citlivých oblastí před neoprávněným přístupem a před riziky okolního prostředí.

34. Fyzický přístup k systémům IKT by měl být povolen pouze oprávněným osobám. Oprávnění by mělo být přiděleno v souladu s úkoly a povinnostmi dané osoby a mělo by být omezeno na osoby, které jsou řádně vyškoleny a sledovány. Fyzický přístup by měl být pravidelně přezkoumáván, aby bylo v případě potřeby zajištěno neprodlené zrušení nepotřebných přístupových práv.

35. Přiměřená opatření na ochranu před riziky okolního prostředí by měla být úměrná důležitosti budov a kritičnosti operací nebo systémů IKT umístěných v těchto budovách.

1.4.4. Bezpečnost provozu IKT

36. Finanční instituce by měly zavést postupy, které zabrání výskytu bezpečnostních incidentů v systémech IKT a službách v oblasti IKT, a měly by minimalizovat jejich dopad na poskytování služeb v oblasti IKT. Tyto postupy by měly zahrnovat následující opatření:

    a) identifikace potenciálních zranitelností, které by měly být vyhodnoceny a napraveny zajištěním aktualizace softwaru a firmwaru, včetně softwaru, který finanční instituce poskytují svým interním a externím uživatelům, provedením kritických bezpečnostních oprav nebo zavedením kompenzačních kontrol;
    b) zavedení požadavků na bezpečnostní konfiguraci všech síťových komponent;
    c) zavedení segmentace sítě, systémů prevence ztráty dat a šifrování síťového provozu (v souladu s klasifikací dat);
    d) zavedení ochrany koncových bodů včetně serverů, pracovních stanic a mobilních zařízení; finanční instituce by měly vyhodnotit, zda koncové body splňují jimi vymezené bezpečnostní standardy, než bude těmto bodům umožněn přístup do podnikové sítě;
    e) zajištění toho, aby byly zavedeny mechanismy pro ověření integrity softwaru, firmwaru a dat;
    f) šifrování uložených a přenášených dat (v souladu s klasifikací dat).

37. Finanční instituce by dále měly průběžně zjišťovat, zda změny stávajícího provozního prostředí ovlivňují stávající bezpečnostní opatření nebo vyžadují přijetí dalších opatření za účelem

zmírnění příslušných souvisejících rizik. Tyto změny by měly být součástí formálního procesu řízení změn finančních institucí, které by měly zajistit, aby byly změny řádně naplánovány, otestovány, zdokumentovány, schváleny a zavedeny.

1.4.5. Bezpečnostní monitorování

38. Finanční instituce by měly zavést a provádět zásady a postupy s cílem odhalovat neobvyklé činnosti, které mohou mít dopad na bezpečnost informací finančních institucí, a na tyto události vhodně reagovat. V rámci tohoto průběžného sledování by finanční instituce měly zavést vhodné a účinné možnosti pro odhalování a oznamování fyzického nebo logického narušení, jakož i porušení důvěrnosti, integrity a dostupnosti informačních aktiv. Průběžné procesy kontroly a odhalování neobvyklé činnosti by se měly zaměřit na:
    a) relevantní interní a externí faktory, včetně obchodních a správcovských funkcí v systému informačních a komunikačních technologií;
    b) transakce, aby bylo možné odhalit zneužití přístupu třetími stranami nebo jinými subjekty a interní zneužití přístupu;
    c) potenciální interní a externí hrozby.
39. Finanční instituce by měly stanovit a uplatňovat postupy a organizační struktury s cílem identifikovat a neustále sledovat bezpečnostní hrozby, které by mohly podstatně ovlivnit schopnost instituce poskytovat služby. Finanční instituce by měly aktivně sledovat technologický vývoj, aby zajistily, že si budou vědomy bezpečnostních rizik. Finanční instituce by měly zavést opatření například k identifikaci možných úniků informací, škodlivých kódů a dalších bezpečnostních hrozeb a veřejně známých zranitelností softwaru a hardwaru a měly by kontrolovat odpovídající nové aktualizace zabezpečení.
40. Proces sledování bezpečnosti by měl finanční instituci také pomáhat pochopit povahu provozních nebo bezpečnostních incidentů, identifikovat trendy a podporovat vyšetřování organizace.

1.4.6. Přezkumy, hodnocení a testování bezpečnosti informací

41. Finanční instituce by měly provádět nejrůznější přezkumy, hodnocení a testování bezpečnosti informací, aby zajistily účinnou identifikaci zranitelností ve svých systémech IKT a službách v oblasti IKT. Finanční instituce mohou například provádět diferenční analýzu podle standardů bezpečnosti informací, přezkumy dodržování předpisů, interní a externí audity informačních systémů nebo kontroly fyzického zabezpečení. Instituce by měla dále zvážit osvědčené postupy, jako jsou přezkumy zdrojového kódu, hodnocení zranitelností, penetrační testy a etický hacking.
42. Finanční instituce by měly stanovit a provádět rámec pro testování bezpečnosti informací, který ověřuje spolehlivost a účinnost jejich opatření v oblasti bezpečnosti informací, a měly by zajistit, aby tento rámec zohledňoval hrozby a zranitelnosti identifikované prostřednictvím sledování hrozeb a procesu posouzení rizik v oblasti IKT a bezpečnosti.
43. Rámec pro testování bezpečnosti informací by měl zajistit, že testy:

a) budou provádět nezávislé testovací subjekty s dostatečnými znalostmi, dovednostmi a odborností v oblasti testování opatření pro bezpečnost informací, které se nepodílí na vývoji opatření pro bezpečnost informací;
b) budou zahrnovat kontroly zranitelností a penetrační testy (včetně penetračního testování na základě hrozeb, bude-li to nutné a vhodné) úměrné úrovni rizika zjištěného u obchodních procesů a systémů.

44. Finanční instituce by měly provádět průběžné a opakované testy bezpečnostních opatření. U všech kritických systémů IKT (bod 17) by tyto testy měly být prováděny nejméně jednou ročně a v případě poskytovatelů platebních služeb budou součástí komplexního posouzení bezpečnostních rizik spojených s platebními službami, které tito poskytovatelé poskytují, podle čl. 95 odst. 2 směrnice PSD2. Jiné než kritické systémy by měly být testovány pravidelně na základě přístupu založeného na riziku, nejméně však každé tři roky.

45. Finanční instituce by měly zajistit, aby byly testy bezpečnostních opatření prováděny v případě změn infrastruktury, procesů nebo postupů a v případě, že dojde ke změnám v důsledku závažných provozních nebo bezpečnostních incidentů nebo v důsledku vydání nových nebo výrazně změněných kritických aplikací přímo dostupných ze sítě internet.

46. Finanční instituce by měly sledovat a vyhodnocovat výsledky bezpečnostních testů a odpovídajícím způsobem aktualizovat svá bezpečnostní opatření, v případě kritických systémů IKT bez zbytečného prodlení.

47. U poskytovatelů platebních služeb by měl rámec pro testování rovněž zahrnovat bezpečnostní opatření týkající se 1) platebních terminálů a zařízení používaných k poskytování platebních služeb; 2) platebních terminálů a zařízení používaných k ověřování uživatelů platebních služeb a 3) zařízení a softwaru poskytovaných uživateli poskytovatelem platebních služeb za účelem vygenerování/získání ověřovacího kódu.

48. Na základě zjištěných bezpečnostních hrozeb a uskutečněných změn by mělo být provedeno testování, které bude zahrnovat scénáře relevantních a známých potenciálních útoků.

1.4.7. Odborná příprava a povědomí týkající se bezpečnosti informací

49. Finanční instituce by měly zavést program odborné přípravy zahrnující pravidelné programy zvyšování povědomí v oblasti bezpečnosti pro všechny zaměstnance a dodavatele, aby zajistily, že zaměstnanci a dodavatelé budou vyškoleni k plnění svých úkolů a povinností v souladu s příslušnými bezpečnostními zásadami a postupy, jejichž cílem je odstranit lidské chyby, krádeže, podvody, zneužití nebo ztráty a řešit rizika spojená s bezpečností informací. Finanční instituce by měly zajistit, aby program odborné přípravy zajišťoval školení pro všechny zaměstnance a dodavatele nejméně jednou ročně.

1.5. Řízení provozu IKT

50. Finanční instituce by měly řídit svůj provoz IKT na základě zdokumentovaných a zavedených procesů a postupů (které v případě poskytovatelů platebních služeb zahrnují bezpečnostní předpis podle čl. 5 odst. 1 písm. j) směrnice PSD2), které schvaluje vedoucí orgán. Tento soubor

dokumentů by měl vymezit, jak finanční instituce provozují, sledují a kontrolují své systémy a služby v oblasti IKT včetně dokumentování kritických operací IKT, a měl by finančním institucím umožnit, aby udržovaly aktuální soupis aktiv v oblasti IKT.

51. Finanční instituce by měly zajistit, aby výkon jejich provozu IKT byl v souladu s jejich provozními požadavky. Finanční instituce by měly udržovat a pokud možno zlepšovat účinnost svého provozu IKT, mimo jiné včetně nutnosti zvážit, jak minimalizovat možné chyby vznikající při provádění manuálních úkolů.

52. Finanční instituce by měly u kritických částí provozu IKT zavést postupy logování a sledování, které umožní odhalit, analyzovat a opravit chyby.

53. Finanční instituce by měly udržovat aktuální soupis aktiv v oblasti IKT (včetně systémů IKT, síťových zařízení, databází atd.). Soupis aktiv v oblasti IKT by měl uchovávat konfiguraci aktiv v oblasti IKT a vazby a vzájemné závislosti mezi jednotlivými aktivy v oblasti IKT, aby byl možný správný proces konfigurace a řízení změn.

54. Soupis aktiv v oblasti IKT by měl být dostatečně podrobný, aby umožnil okamžitou identifikaci aktiva v oblasti IKT, jeho umístění, bezpečnostní klasifikace a odpovědnosti za aktivum. Vzájemná závislost mezi aktivy by měla být zdokumentována s cílem napomoci reakci na bezpečnostní a provozní incidenty, včetně kybernetických útoků.

55. Finanční instituce by měly sledovat a řídit životní cykly aktiv v oblasti IKT, aby zajistily, že aktiva budou i nadále splňovat a podporovat požadavky týkající se obchodu a řízení rizik. Finanční instituce by měly sledovat, zda jejich externí nebo interní dodavatelé a vývojáři podporují jejich aktiva v oblasti IKT a zda jsou všechny příslušné opravy a aktualizace prováděny na základě zdokumentovaných procesů. Je třeba posuzovat a zmírňovat rizika vyplývající ze zastaralých nebo nepodporovaných aktiv v oblasti IKT.

56. Finanční instituce by měly zavést procesy plánování a monitorování výkonnosti a kapacity, aby včas předešly závažným problémům v oblasti výkonnosti systémů IKT a nedostatkům kapacity v oblasti IKT, a aby tyto problémy včas zjišťovaly a reagovaly na ně.

57. Finanční instituce by měly definovat a provádět postupy zálohování a obnovy dat a systémů IKT, aby bylo zajištěno, že tato data a systémy bude možné v případě potřeby obnovit. Rozsah a četnost záloh by měly být stanoveny podle požadavků na obnovení činnosti a kritičnosti dat a systémů IKT a měly by být hodnoceny podle provedeného posouzení rizik. Pravidelně by mělo být prováděno testování postupů zálohování a obnovy.

58. Finanční instituce by měly zajistit, aby zálohy dat a systémů IKT byly bezpečně uloženy a dostatečně vzdáleny od primárního místa, díky čemuž nebudou vystaveny stejným rizikům.

3.5.1 Řízení incidentů a problémů v oblasti IKT

59. Finanční instituce by měly stanovit a provádět proces řízení incidentů a problémů s cílem sledovat a zaznamenávat provozní a bezpečnostní incidenty v oblasti IKT a umožnit finančním institucím včasné pokračování nebo obnovení kritických obchodních funkcí a procesů v případě narušení. Finanční instituce by měly stanovit příslušná kritéria a prahové hodnoty ke klasifikaci události jako provozního nebo bezpečnostního incidentu, jak je stanoveno v oddíle „Definice“ těchto obecných pokynů, a také indikátory včasného varování, které by měly sloužit jako

upozornění umožňující tyto incidenty včas odhalit. Těmito kritérii a prahovými hodnotami není v případě poskytovatelů platebních služeb dotčena klasifikace významných incidentů podle článku 96 směrnice PSD2 a obecných pokynů k oznamování významných incidentů podle směrnice PSD2 (EBA/GL/2017/10).

60. Aby minimalizovaly dopad nepříznivých událostí a umožnily včasnou obnovu, měly by finanční instituce stanovit vhodné postupy a organizační struktury, které zajistí jednotné a integrované sledování, řešení a návazné sledování provozních a bezpečnostních incidentů a zabezpečí, aby byly identifikovány a odstraněny hlavní příčiny a předešlo se výskytu opakovaných incidentů. Postup řízení incidentů a problémů by měl stanovit:

    a) postupy pro identifikaci, zpětné sledování, zaznamenávání, kategorizaci a klasifikaci incidentů podle priority na základě kritičnosti z hlediska obchodní činnosti;
    b) úlohy a povinnosti pro různé scénáře incidentů (např. chyby, poruchy, kybernetické útoky);
    c) postupy řízení problémů s cílem identifikovat, analyzovat a vyřešit hlavní příčinu jednoho nebo více incidentů – finanční instituce by měla analyzovat provozní nebo bezpečnostní incidenty s pravděpodobným vlivem na finanční instituci, které byly identifikovány nebo se vyskytly uvnitř nebo vně organizace, a měla by zvážit hlavní poznatky získané z těchto analýz a odpovídajícím způsobem aktualizovat bezpečnostní opatření;
    d) účinné plány interní komunikace včetně postupů pro oznamování incidentů a jejich předání na vyšší úroveň řízení (zahrnující i stížnosti zákazníků související s bezpečností), které zajistí:
        i) aby byly incidenty s potenciálně velkým nepříznivým dopadem na kritické systémy IKT a služby v oblasti IKT oznamovány příslušnému vrcholnému vedení a vrcholnému vedení pro IKT;
        ii) aby byl v případě závažných incidentů vedoucí orgán informován ad hoc a aby byl vyrozuměn přinejmenším o dopadu, reakci a dodatečných kontrolách, které mají být stanoveny v důsledku incidentů;
    e) postupy reakce na incidenty ke zmírnění dopadů souvisejících s incidenty a zajištění včasného obnovení činnosti a bezpečnosti služby;
    f) specifické plány externí komunikace pro kritické obchodní funkce a procesy s cílem:
        i) spolupracovat s příslušnými zainteresovanými subjekty za účelem účinné reakce na incident a obnovy po incidentu;
        ii) poskytnout včasné informace externím stranám (např. zákazníkům, ostatním účastníkům trhu, orgánu dohledu) podle potřeby a v souladu s platnými předpisy.

1.6. Řízení projektů a změn v oblasti IKT

1.6.1. Řízení projektů v oblasti IKT

61. Finanční instituce by měla provádět program nebo proces správy a řízení projektů, který vymezí úlohy, povinnosti a odpovědnosti pro účinnou podporu provádění strategie v oblasti IKT.

62. Finanční instituce by měla náležitě sledovat a zmírňovat rizika vyplývající z jejího portfolia projektů v oblasti IKT (řízení programů) a brát v úvahu také rizika, která mohou vyplývat ze vzájemných závislostí mezi různými projekty a ze závislostí více projektů na týchž zdrojích nebo odborných znalostech.

63. Finanční instituce by měla zavést a provádět politiku řízení projektů v oblasti IKT, která zahrnuje alespoň:

    a) cíle projektu;

    b) role a povinnosti;

    c) posouzení rizik projektu;

    d) plán, časový rámec a kroky projektu;

    e) hlavní milníky;

    f) požadavky týkající se řízení změn.

64. Politika řízení projektů v oblasti IKT by měla zajistit, aby požadavky na bezpečnost informací byly analyzovány a schváleny funkcí, která je nezávislá na funkci vývoje.

65. Finanční instituce by měla zajistit, aby byly v projektovém týmu zastoupeny všechny oblasti ovlivněné projektem v oblasti IKT a aby měl projektový tým znalosti potřebné k zajištění bezpečné a úspěšné realizace projektu.

66. Vytvoření a pokrok projektů v oblasti IKT a s nimi související rizika by měly být oznamovány vedoucímu orgánu, a to jednotlivě nebo souhrnně, podle významu a velikosti projektů v oblasti IKT, pravidelně a dle potřeby ad hoc. Finanční instituce by měly zahrnout riziko projektů do svého rámce řízení rizik.

1.6.2. Pořizování a vývoj systémů IKT

67. Finanční instituce by měly vyvinout a zavést postup upravující pořízení, vývoj a údržbu systémů IKT. Tento postup by měl být navržen pomocí přístupu založeného na riziku.

68. Finanční instituce by měla zajistit, aby před provedením jakéhokoli nákupu nebo vývoje systémů IKT příslušné vedení jasně vymezilo a schválilo funkční a jiné než funkční požadavky (včetně požadavků na bezpečnost informací).

69. Finanční instituce by měla zajistit, aby byla zavedena opatření ke zmírnění rizika nezáměrné změny nebo záměrného zmanipulování systémů IKT během vývoje a zavádění v produkčním prostředí.

70. Finanční instituce by měly mít zavedenu metodiku testování a schvalování systémů IKT před jejich prvním použitím. Tato metodika by měla brát v úvahu kritičnost obchodních procesů a aktiv. Testování by mělo zajistit, aby nové systémy IKT fungovaly tak, jak bylo zamýšleno. Finanční instituce by také měly používat testovací prostředí, které bude přiměřeně odrážet jejich produkční prostředí.

71. Finanční instituce by měly testovat systémy IKT, služby v oblasti IKT a opatření pro bezpečnost informací tak, aby identifikovaly možná slabá místa, narušení a incidenty v oblasti bezpečnosti.

72. Finanční instituce by měla zavést samostatná prostředí IKT, aby zajistila odpovídající oddělení funkcí a zmírnila dopad neověřených změn na produkční systémy. Konkrétně by finanční instituce měla zajistit oddělení produkčních prostředí od vývojových, testovacích a ostatních neprodukčních prostředí. Finanční instituce by měla zajistit integritu a důvěrnost produkčních dat v neprodukčních prostředích. Přístup k datům z produkčního prostředí je omezen na oprávněné uživatele.

73. Finanční instituce by měly zavést opatření na ochranu integrity zdrojových kódů systémů IKT, které jsou vyvíjeny interně. Měly by také komplexně dokumentovat vývoj, zavádění, provoz nebo konfiguraci systémů IKT, aby se snížila jakákoli nadbytečná závislost na odbornících v dané oblasti. Dokumentace systému IKT by měla případně obsahovat alespoň uživatelskou dokumentaci, dokumentaci technického systému a provozní postupy.

74. Postupy finanční instituce pro pořízení a vývoj systémů IKT by se měly vztahovat i na systémy IKT vyvinuté nebo řízené koncovými uživateli obchodních funkcí mimo organizaci IKT (např. počítačové aplikace koncových uživatelů) s využitím přístupu založeného na riziku. Finanční instituce by měla vést evidenci aplikací, které podporují kritické obchodní funkce nebo procesy.

1.6.3. Řízení změn v oblasti IKT

75. Finanční instituce by měly stanovit a zavést proces řízení změn v oblasti IKT, aby zajistily, že všechny změny systémů IKT budou zaznamenávány, testovány, posuzovány, schvalovány, prováděny a ověřovány kontrolovaným způsobem. Finanční instituce by měly změny během mimořádných událostí (tj. změny, které musí být zavedeny co nejdříve) zpracovat podle postupů, které poskytují odpovídající záruky.

76. Finanční instituce by měly průběžně zjišťovat, zda změny stávajícího provozního prostředí ovlivňují stávající bezpečnostní opatření nebo vyžadují přijetí dalších opatření, aby se zmírnila příslušná rizika. Tyto změny by měly být v souladu s formálním procesem finančních institucí pro řízení změn.

1.7. Řízení kontinuity činnosti

77. Finanční instituce by měly v souladu s čl. 85 odst. 2 směrnice 2013/36/EU a hlavou VI obecných pokynů orgánu EBA k vnitřnímu systému správy a řízení (EBA/GL/2017/11) zavést řádný proces řízení kontinuity činnosti, aby maximalizovaly svou schopnost poskytovat dále služby a omezit ztráty v případě závažného přerušení podnikatelské činnosti.

1.7.1. Analýza dopadu na podnikatelskou činnost

78. V rámci řádného řízení kontinuity činnosti by finanční instituce měly provádět analýzu dopadu na podnikatelskou činnost analyzováním své expozice vůči závažným narušením činnosti a posouzením jejich možných dopadů (včetně dopadů v oblasti důvěrnosti, integrity a dostupnosti), a to kvantitativně i kvalitativně, pomocí interních nebo externích údajů (např. údajů externích poskytovatelů významných pro obchodní proces nebo veřejně dostupných údajů, které mohou být z hlediska analýzy dopadu na podnikatelskou činnost

relevantní), a analýzu scénářů. Analýza dopadu na podnikatelskou činnost by také měla zvážit kritičnost identifikovaných a klasifikovaných obchodních funkcí, podpůrných procesů, třetích stran a informačních aktiv a jejich vzájemné závislosti v souladu s oddílem 1.3.3.

79. Finanční instituce by měly zajistit, aby jejich systémy IKT a služby v oblasti IKT byly navrženy a sladěny s jejich analýzou dopadu na podnikatelskou činnost, například pokud jde o redundanci určitých kritických složek, aby se zabránilo narušením způsobeným událostmi, které mají na tyto složky dopad.

1.7.2. Plánování kontinuity činnosti

80. Na základě svých analýz dopadu na podnikatelskou činnost by finanční instituce měly vypracovat plány k zajištění kontinuity činnosti (plány kontinuity činnosti), které by měly být zdokumentovány a měl by je schválit vedoucí orgán finanční instituce. Plány by měly brát v úvahu zvláště rizika, která by mohla mít nepříznivý dopad na systémy IKT a služby v oblasti IKT. Plány by měly podporovat cíle týkající se ochrany a v případě potřeby obnovy důvěrnosti, integrity a dostupnosti obchodních funkcí finančních institucí, podpůrných procesů a informačních aktiv. Finanční instituce by měly při sestavování těchto plánů podle potřeby koordinovat svou činnost s příslušnými interními a externími zainteresovanými stranami.

81. Finanční instituce by měly zavést plány kontinuity činnosti, aby zajistily, že budou moci přiměřeně reagovat na případné scénáře selhání a že budou schopny obnovit provoz svých kritických obchodních činností po přerušení v rámci cílové doby obnovy (maximální doba, během níž musí být po incidentu obnoven systém nebo proces) a cílového bodu obnovy (maximální lhůta, během níž je přijatelná ztráta dat v případě incidentu). V případě vážného narušení činnosti, které spustí konkrétní plány kontinuity činnosti, by měly finanční instituce stanovit přednost opatření pro kontinuitu činnosti pomocí přístupu založeného na riziku, který může vycházet z posouzení rizik provedených podle oddílu 1.3.3. U poskytovatelů platebních služeb to může například zahrnovat usnadnění dalšího zpracování kritických transakcí při pokračujícím úsilí o nápravu.

82. Finanční instituce by měla ve svém plánu kontinuity činnosti zvážit řadu různých scénářů, včetně extrémních, ale věrohodných scénářů, kterým může být vystavena, a to včetně scénáře kybernetického útoku, a měla by posoudit možný dopad takových scénářů. Na základě těchto scénářů by finanční instituce měla popsat, jak je zajištěna kontinuita systémů IKT a služeb v oblasti IKT, jakož i bezpečnost informací finanční instituce.

1.7.3. Plány reakce a obnovy

83. Na základě analýz dopadu na podnikatelskou činnost (bod 78) a věrohodných scénářů (bod 82) by finanční instituce měly vypracovat plány reakce a obnovy. Tyto plány by měly specifikovat, jaké podmínky mohou urychlit aktivaci plánů a jaká opatření by měla být přijata k zajištění dostupnosti, kontinuity a obnovy přinejmenším kritických systémů IKT a služeb v oblasti IKT provozovaných finančními institucemi. Cílem plánů reakce a obnovy by mělo být splnění cílů obnovy operací finančních institucí.

84. Plány reakce a obnovy by měly zohledňovat krátkodobé i dlouhodobé možnosti obnovy. Tyto plány:

a) by se měly zaměřit na obnovu činnosti kritických obchodních funkcí, podpůrných procesů, informačních aktiv a jejich vzájemných závislostí, aby se zabránilo nepříznivým dopadům na fungování finančních institucí a na finanční systém, včetně dopadů na platební systémy a na uživatele platebních služeb, a aby se zajistilo provedení čekajících platebních transakcí;
b) by měly být zdokumentovány a zpřístupněny obchodním a podpůrným útvarům a být snadno dostupné v případě mimořádné situace,
c) by měly být aktualizovány v souladu s poznatky získanými z incidentů, testování, s nově identifikovanými riziky či hrozbami a se změněnými cíli a prioritami obnovy.

85. Plány by také měly zvážit alternativní možnosti v případech, kdy obnova nemusí být z krátkodobého hlediska proveditelná z důvodu nákladů, rizik, logistiky nebo nepředvídaných okolností.

86. Kromě toho by v rámci plánů reakce a obnovy měla finanční instituce zvážit a provádět opatření pro kontinuitu činnosti, aby zmírnila selhání externích poskytovatelů, kteří mají klíčový význam pro kontinuitu služeb v oblasti IKT finanční instituce (v souladu s ustanoveními obecných pokynů orgánu EBA k outsourcingu (EBA/GL/2019/02).

1.7.4. Testování plánů

87. Finanční instituce by měly své plány kontinuity činnosti pravidelně testovat. Zejména by měly zajistit, aby plány kontinuity činnosti jejich kritických obchodních funkcí, podpůrných procesů, informačních aktiv a jejich vzájemných závislostí (včetně těch, které případně poskytly třetí strany) byly v souladu s bodem 89 testovány nejméně jednou ročně.

88. Plány kontinuity činnosti by se měly aktualizovat nejméně jednou ročně na základě výsledků testování, aktuálních informací o hrozbách a zkušeností získaných z předchozích událostí. Jakékoli změny cílů obnovy (včetně cílové doby obnovy a cílového bodu obnovy) nebo změny obchodních funkcí, podpůrných procesů a informačních aktiv by měly být rovněž dle potřeby zohledněny jako základ aktualizace plánů kontinuity činnosti.

89. Testování plánů kontinuity činnosti finančních institucí by mělo prokázat, že instituce jsou schopny zachovat životaschopnost své činnosti, dokud nebudou obnoveny kritické operace. Zejména by měly:

a) zahrnovat testování vhodného souboru závažných, ale pravděpodobných scénářů, včetně scénářů zvažovaných pro vývoj plánů kontinuity činnosti (a případně testování služeb poskytovaných třetími stranami); měl by sem spadat převod důležitých obchodních funkcí, podpůrných procesů a informačních aktiv do prostředí pro obnovu po havárii a prokázání toho, že je lze takto provozovat po dostatečně reprezentativní časové období a že poté lze obnovit obvyklou činnost;
b) navrhnout testování tak, aby prověřilo předpoklady, na nichž spočívají plány pro zajištění kontinuity činnosti, včetně systémů správy a řízení a plánů krizové komunikace, a
c) zahrnovat postupy k ověření schopnosti zaměstnanců a dodavatelů, systémů IKT a služeb v oblasti IKT provozovaných finančními institucemi přiměřeně reagovat na scénáře vymezené v bodě 89 písm. a).

90. Výsledky testů by měly být zdokumentovány a veškeré zjištěné nedostatky vyplývající z testů by měly být analyzovány, řešeny a oznámeny vedoucímu orgánu.

1.7.5. Krizová komunikace

91. V případě narušení nebo mimořádné situace a během provádění plánů pro zajištění kontinuity činnosti by měly finanční instituce zajistit, aby byla zavedena účinná komunikační opatření pro případ krize, aby byly včas a vhodným způsobem informovány všechny příslušné interní i externí zainteresované strany, včetně příslušných vnitrostátních orgánů, pokud to vyžadují vnitrostátní právní předpisy, a příslušných poskytovatelů (poskytovatelů v rámci outsourcingu, subjektů ve skupině nebo externích poskytovatelů).

1.8. Řízení vztahů s uživateli platebních služeb

92. Poskytovatelé platebních služeb by měli stanovit a uplatňovat postupy za účelem zvýšení povědomí uživatelů platebních služeb o bezpečnostních rizicích spojených s platebními službami, a to prostřednictvím asistenčních služeb a poradenství pro uživatele platebních služeb.

93. Asistenční služby a poradenství nabízené uživatelům platebních služeb by měly být aktualizovány s ohledem na nové hrozby a zranitelnosti a uživatelé by měli být informováni o všech změnách.

94. V případě, že to umožňuje funkčnost produktu, by poskytovatelé platebních služeb měli umožnit uživatelům deaktivovat konkrétní platební funkce, které souvisí s platebními službami nabízenými uživateli poskytovatelem platebních služeb.

95. Pokud se poskytovatel platebních služeb v souladu s čl. 68 odst. 1 směrnice (EU) 2015/2366 dohodl s plátcem na omezení výdajů u platebních transakcí prováděných prostřednictvím zvláštních platebních prostředků, měl by poskytovatel platební služby poskytnout plátci možnost tento stanovený maximální limit upravit.

96. Poskytovatelé platebních služeb by měli uživatelům platebních služeb poskytnout možnost dostávat upozornění o provedených a/nebo neúspěšných pokusech o zadání příkazu k platební transakci, což jim umožní odhalit podvodné nebo neoprávněné používání jejich účtů.

97. Poskytovatelé platebních služeb by měli uživatele informovat o aktuálních změnách bezpečnostních postupů, které mají vliv na poskytování platebních služeb uživateli.

98. Poskytovatelé platebních služeb by měli uživatelům poskytnout pomoc v případě jakéhokoli dotazu, žádosti o podporu a oznámení anomálií nebo potíží týkajících se bezpečnostních záležitostí, které se vztahují na platební služby. Uživatelé platebních služeb by měli být náležitě informováni o tom, jak mohou tuto pomoc získat.