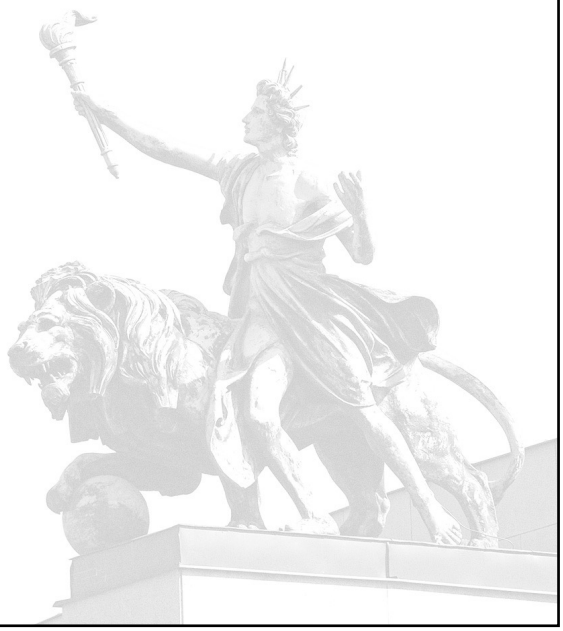
ČNB ČESKÁ NÁRODNÍ BANKA

Právní úprava a působnost nařízení DORA – zkušenosti po jednom roce licencování



1

ČNB ČESKÁ NÁRODNÍ BANKA

Právní úprava (regulatorní rámec)

Zkratka	Plný název / Obsah
„nařízení DORA“	Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011.
„RTS 2024/1502“	Nařízení Komise v přenesené pravomoci (EU) 2024/1502 ze dne 22. února 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554 upřesněním kritérií pro určení poskytovatelů služeb IKT z řad třetích stran za kritické pro finanční subjekty.
„RTS 2024/1505“	Nařízení Komise v přenesené pravomoci (EU) 2024/1505 ze dne 22. února 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554 stanovením výše poplatků za dohled, které má hlavní orgán dohledu účtovat kritickým poskytovatelům služeb IKT z řad třetích stran, a způsobu úhrady těchto poplatků.
„RTS k řízení rizik“	Nařízení Komise v přenesené pravomoci (EU) 2024/1774 ze dne 13. března 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy upřesňující nástroje, metody, postupy a politiky řízení rizika v oblasti IKT a zjednodušený rámec pro řízení rizika v oblasti IKT.
„RTS ke klasifikaci incidentů“	Nařízení Komise v přenesené pravomoci (EU) 2024/1772 ze dne 13. března 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy, v nichž jsou upřesněna kritéria klasifikace incidentů souvisejících s IKT a kybernetických hrozeb, stanoveny prahové hodnoty významnosti a upřesněny údaje v hlášeních závažných incidentů, které upřesňuje kritéria pro klasifikaci IKT incidentů a kybernetických hrozeb.
„RTS ke smlouvám s poskytovateli služeb“	Nařízení Komise v přenesené pravomoci (EU) 2024/1773 ze dne 13. března 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy upřesňující podrobný obsah politiky týkající se smluvních ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran

2

2

ČNB ČESKÁ NÁRODNÍ BANKA

Právní úprava (regulatorní rámec) - pokračování

Zkratka	Plný název / Obsah
„ITS k registru informací“	Prováděcí nařízení Komise (EU) 2024/2956 ze dne 29. listopadu 2024, kterým se stanoví prováděcí technické normy pro uplatňování nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o standardní vzory pro registr informací.
„RTS k provádění činností dohledu“	Nařízení Komise v přenesené pravomoci (EU) 2025/295 ze dne 24. října 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy týkající se harmonizace podmínek umožňujících provádění činností dohledu.
„RTS k hlášení incidentů“	Nařízení Komise v přenesené pravomoci (EU) 2025/301, ze dne 23. října 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy, jež které stanoví obsah a lhůty pro prvotní oznámení a průběžnou a závěrečnou zprávu o závažných incidentech souvisejících s IKT a obsah dobrovolného oznámení o významných kybernetických hrozbách. (dle DORA).
„ITS k hlášení incidentů“	Prováděcí nařízení Komise v přenesené pravomoci (EU) 2025/302 ze dne 23. října 2024, kterým se stanoví prováděcí technické normy pro uplatňování nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o standardní formuláře, vzory a postupy pro hlášení závažného incidentu souvisejícího s IKT a oznamování významné kybernetické hrozby finančními orgány.
„RTS k subkontrahování“	Nařízení Komise v přenesené pravomoci (EU) 2025/532 ze dne 24. března 2025, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy upřesňující prvky, které musí finanční subjekt určit a posoudit při subdodávkách služeb IKT podporujících zásadní nebo důležité funkce.
„RTS k penetračnímu testování“	Nařízení Komise v přenesené pravomoci (EU) 2025/1190 ze dne 13. února 2025, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy upřesňující kritéria, která se použijí pro určení finančních subjektů, které jsou povinny provádět penetrační testování na základě hrozeb, požadavky a normy, kterými se řídí využívání interních subjektů provádějících testování, požadavky týkající se rozsahu testování, metodiky a postupů testování pro jednotlivé fáze procesu testování, výsledků a fáze ukončení testování a nápravy a druhu spolupráce v oblasti dohledu a jiné relevantní spolupráce, která je zapotřebí k provádění penetračního testování na základě hrozeb a pro usnadnění vzájemného uznávání těchto testů.

ČNB ČESKÁ NÁRODNÍ BANKA

Zásada proporcionality

Finanční subjekty:

- *uplatní pravidla* s přihlédnutím **k *velikosti* a celkovému *rizikovému profilu* a *povaze*, *rozsahu* a *složitosti* poskytovaných služeb, činností a operací**;
- v *rozsahu*:
  - na pravidla stanovená v kapitole II a
  - na pravidla v kapitolách III, IV a V oddílu I (explicitně)
- ***za předpokladu*, že budou schopny *doložit hodnocení* provedená za tímto účelem**

Příslušné orgány (ČNB):

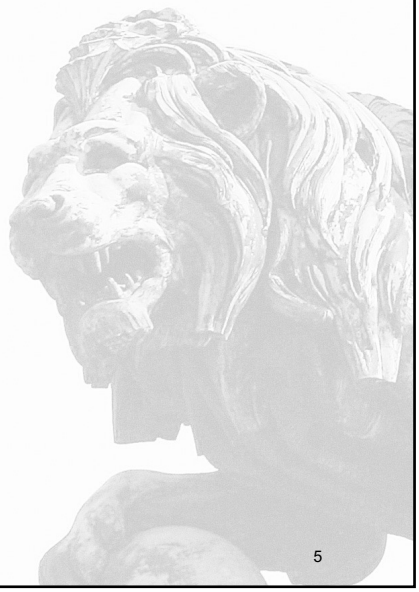
- ***zváží*** uplatňování zásady proporcionality finančními subjekty
- ***uplatní*** přiměřenost (proporcionalitu) také podle svých kritérií

ČNB ČESKÁ NÁRODNÍ BANKA

Zásada proporcionality - zohlednění

Příslušné orgány (ČNB):

- *zváží* její uplatňování finančními subjekty při přezkumu soudržnosti rámce pro řízení rizika v oblasti IKT na *základě zpráv* předložených na žádost příslušných orgánů podle čl. 6 odst. 5 a čl. 16 odst. 2.
- ČNB *bude uplatňovat* přiměřenost (proporcionalitu) i nadále také podle dalších kritérií jako je rizikový profil (interní rating stanovený ČNB) a hodnocení systémového významu finanční instituce

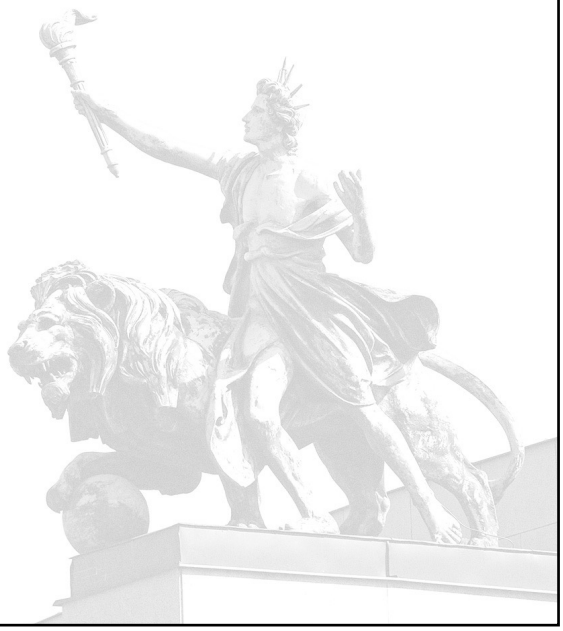


5

5

ČNB ČESKÁ NÁRODNÍ BANKA

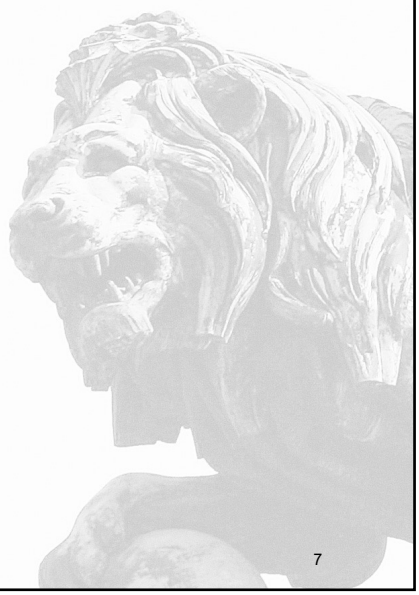
Požadavky na Řízení finančního subjektu a jeho organizaci



6

ČNB ČESKÁ NÁRODNÍ BANKA

Úvodní vysvětlení – ŘKS a DORA



Řídicí kontrolní systém (ŘKS) finanční instituce

- souhrn prvků vytvářejících obecné předpoklady řádné správy a řízení společnosti
- součástí je také systém řízení rizik, interní kontroly, informační systém (IKT) apod.

Nařízení DORA se zabývá částí ŘKS

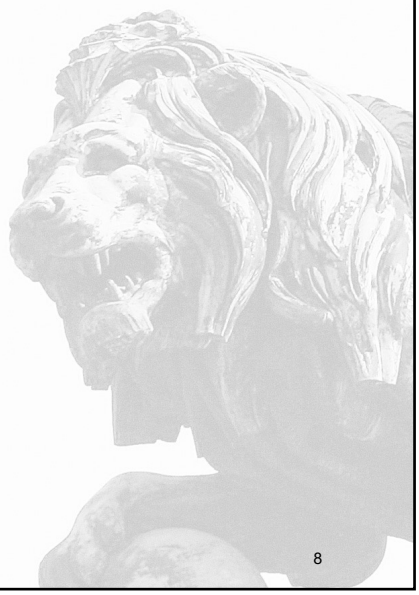
- dosažení vysoké a společné úrovně digitální provozní odolnosti subjektů finančního sektoru
- začleněním prvků IKT, bezpečnosti a provozní odolnosti do *celkového rámce* řízení a kontroly společnosti (tj. ŘKS)

7

7

ČNB ČESKÁ NÁRODNÍ BANKA

DORA – uplatňovaný princip



- Odpovědnost vedoucího orgánu
  - nese konečnou odpovědnost za řízení rizika (vč. IKT)
  - stanoví úlohy a povinnosti pro všechny funkce související s IKT
  - rozhoduje, tj. stanovuje a schvaluje veškerá související opatření, přezkumy, uplatňování strategií, plány a výstupy auditů apod.
  - přiděluje odpovídající rozpočtové prostředky
- Členové vedoucího orgánu
  - aktivně usilují o dostatečné a aktuální znalosti a dovednosti
  - splňují nutné obecné znalostní a kvalifikační předpoklady, zejm. pro pochopení a hodnocení rizika a pro přezkum fungování a efektivity rámce řízení IKT rizik

8

8

ČNB ČESKÁ NÁRODNÍ BANKA

Funkce související s IKT

- DORA počítá s následujícími funkcemi / rolemi
  - vedoucí pracovníci (vymezené role s odpovědností vůči vedoucímu orgánu)
  - kontrolní funkce a interní auditní funkce v oblasti rizika IKT*)
  - standarní IKT uživatelské, provozní a bezpečnostní role
  - pracovníci s odpovědostí za reakce na incidenty související s IKT
  - pracovníci s odpovědností zajistit kontinuitu zásadních nebo důležitých funkcí v případě, že primární místo zpracování přestane být dostupné

+ výslovně vyžaduje*):
  - zavedení funkce nebo pověření vedoucího pracovníka s odpovědností za sledování výkonu politiky a ujednání týkajících se využívání IKT služeb od dodavatelů z řad třetích stran a za *„dohled nad expozicí souvisejícím rizikům a příslušnou dokumentací“*
  - zavedení funkce odpovědné za přípravu, testování a výkon krizových komunikačních plánů interní a externí krizové komunikace

*) pro finanční subjekty, jiné než mikropodniky

9

9

ČNB ČESKÁ NÁRODNÍ BANKA

Organizační uspořádání – pozice a role

- Zakotvení ve vnitřních předpisech
  - stanovení pozic nebo rolí s vymezením jejich činností, pravomocí a odpovědností
  - v případě ‚rolí‘ pravidla pro jejich přiřazování a odebírání a pravidla zaručující jejich aktuální výkon
  - stanovení a naplňování kvalifikačních předpokladů pro výkon činností, včetně účasti na pravidelných školeních
- Zajištění nezávislosti a oddělení funkcí
  - vedoucích, kontrolních a interních auditních funkcí podle modelu tří linií obrany nebo interního modelu řízení a kontroly rizika
  - musí být zajištěné i v případě přidělování rolí a garantované v případě svěření více činností jednomu externímu postytovateli služeb na straně tohoto poskytovatele (jeho poskytovatelů)

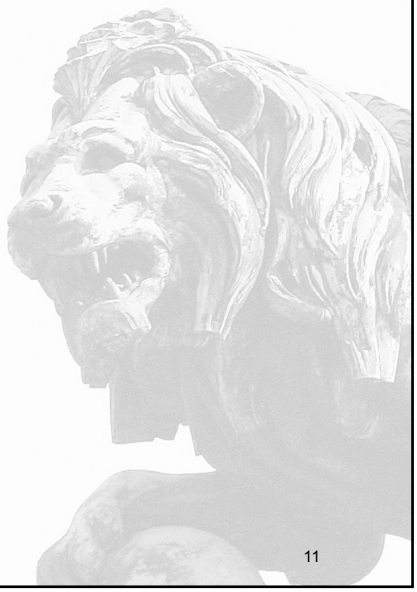
10

10

ČNB ČESKÁ NÁRODNÍ BANKA

Organizační uspořádání – návaznosti

- Bezpečnost je založená na osobách
  - lidský faktor je klíčovým aspektem bezpečnosti a odolnosti
  - dosahování cílů není možné bez náležitého povědomí a péče o kulturní vzorce ve společnosti
  - bezpečnostní a kontrolní mechanismy často nejsou účinné bez konkrétní identifikace jednajících a odpovědných osob
- Osoby a jejich oprávnění v IKT nástrojích
  - musí být založené na ověřené identitě osob
  - musí respektovat pravidlo přidělení nejmenšího rozsahu oprávnění, který je potřebný k výkonu svěřené činnosti



11

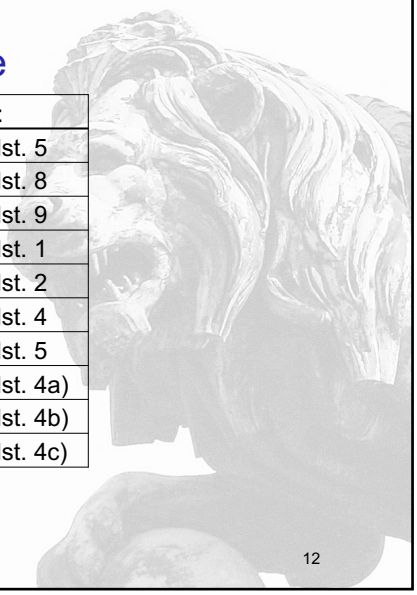
11

ČNB ČESKÁ NÁRODNÍ BANKA

48 oblastí, které DORA samostatně vymezuje

PČ	Jméno dokumentu nebo části dokumentu	Výskyt
1	Zpráva o přezkumu rámce pro řízení rizika v oblasti IKT	čl. 6 odst. 5
2	Strategie digitální provozní odolnosti	čl. 6 odst. 8
3	Strategie více dodavatelů IKT	čl. 6 odst. 9
4	Dokumentace aktiv vůči podporovaným funkcím	čl. 8 odst. 1
5	Katalog rizik	čl. 8 odst. 2
6	Konfigurační DB aktiv	čl. 8 odst. 4
7	Procesy podporované dodavateli IKT	čl. 8 odst. 5
8	Politika zabezpečení informací	čl. 9 odst. 4a)
9	Arch., postupy a protokoly řízení sítí a infrastruktury	čl. 9 odst. 4b)
10	Politika a postupy fyzické a logické bezpečnosti	čl. 9 odst. 4c)

*Výčet dokumentace nemusí být úplný



12

12

ČNB ČESKÁ NÁRODNÍ BANKA

Pokračování

PČ	Jméno dokumentu nebo části dokumentu	Výskyt
11	Politika a protokoly pro silné ověřovací mechanismy	čl. 9 odst. 4d)
12	Politika a postupy pro řízení změn IKT	čl. 9 odst. 4e)
13	Politika pro dočasné opravy a aktualizace	čl. 9 odst. 4f)
14	Popis postupů včasné detekce neobvyklých aktivit	čl. 10 odst. 1
15	Politika zachování provozu IKT	čl. 11 odst. 1
16	Plány reakce a obnovy	čl. 11 odst. 3
17	Plány na zachování provozu	čl. 11 odst. 4
18	Analýza dopadu na činnost	čl. 11 odst. 5
19	Záznamy činnosti před výpadky a během výpadků po aktivaci plánů	čl. 11 odst. 8

*Výčet dokumentace nemusí být úplný

13

13

ČNB ČESKÁ NÁRODNÍ BANKA

Pokračování

PČ	Jméno dokumentu nebo části dokumentu	Výskyt
20	Odhad souhrnných ročních nákladů IKT incidentů	čl. 11 odst. 10
21	Politika a postupy zálohování	čl. 12 odst. 1a)
22	Postupy a metody obnovy	čl. 12 odst. 1b)
23	Programy zvyšování povědomí o bezpečnosti v oblasti IKT a školení o digitální provozní odolnosti	čl. 13 odst. 6
24	Krizové komunikační plány	čl. 14 odst. 1
25	Komunikační politika pro interní zaměstnance a externí zainteresované strany	čl. 14 odst. 2
26	Postupy pro zajištění bezpečnosti údajů a systémů	RTS, čl. 11
27	Postupy řízení kapacity a výkonu	RTS, čl. 9

*Výčet dokumentace nemusí být úplný

14

14

ČNB ČESKÁ NÁRODNÍ BANKA

Pokračování

PČ	Jméno dokumentu nebo části dokumentu	Výskyt
28	Postupy řízení zranitelností	RTS, čl. 10
29	Postupy pro vedení protokolů	RTS, čl. 12
30	Politika, postupy a protokoly na ochranu informací během přenosu	RTS, čl. 14
31	Politika pro řízení projektů v oblasti IKT	RTS, čl. 15
32	Politika upravující pořizování, vývoj a údržbu systému IKT	RTS, čl. 16
33	Politika fyzické a environmentální bezpečnosti	RTS, čl. 18
34	Politika v oblasti lidských zdrojů	RTS, čl. 19
35	Politika a postupy správy identit	RTS, čl. 20
36	Politika správy přístupů	RTS, čl. 21

*Výčet dokumentace nemusí být úplný

15

15

ČNB ČESKÁ NÁRODNÍ BANKA

Pokračování

PČ	Jméno dokumentu nebo části dokumentu	Výskyt
37	Politika a postupy řízení IKT incidentů; pro subjekty platebního styku včetně řízení provozních a bezpečnostních incidentů souvisejících s platbami	čl. 17 odst. 1
38	Záznamy veškerých incidentů souvisejících s IKT a závažné kybernetické hrozby	čl. 17 odst. 2
39	Postupy pro konzistentní a integrované sledování, řešení a následná opatření pro incidenty související s IKT	čl. 17 odst. 2
40	Postupy klasifikace IKT incidentů a kyb. hrozeb	čl. 18 odst. 1
41	Program a postupy testování digitální provozní odolnosti	čl. 24 odst. 1
42	Postupy pro stanovení priorit, klasifikaci a nápravu všech problémů zjištěných při provádění testů	čl. 24 odst. 5
43	Metodiky ověřování, zda všechny zjištěné slabiny, nedostatky či vady byly plně odstraněny	čl. 24 odst. 5
44	TLPT: rámec TIBER-EU	čl. 26

*Výčet dokumentace nemusí být úplný

16

16

ČNB ČESKÁ NÁRODNÍ BANKA

Dokončení

PČ	Jméno dokumentu nebo části dokumentu	Výskyt
45	Strategie/politika pro riziko v oblasti IKT spojené s třetími stranami	čl. 28 odst. 2
46	Registr ujednání s třetími stranami v oblasti IKT	čl. 28 odst. 3
47	Strategie a plány ukončení smluvního vztahu	čl. 28 odst. 8
48	Plány přechodu k alternativnímu poskytovateli	čl. 28 odst. 8

Nutno podotknout že navíc jsou ještě hodnoceny oblasti spojené se souladem vnitřních předpisů a Obchodního záměru a soulad Obchodního záměru a vnitřního řídícího systému společnosti. Technicky vzato se tak posuzuje ne 48 samostatných oblastí ale další 4 oblasti které z DORA pouze kontextově souvisí a hlavně se navíc posuzuje soulad dokumentů navzájem.

*Výčet dokumentace nemusí být úplný

17

17

ČNB ČESKÁ NÁRODNÍ BANKA

Nejčastější problémy se kterými se setkáváme

- Terminologická nejednotnost.
- Architektura – referenční architektura
- Aktiva
- Tříúrovňová ochrana proti selhání – vzájemně neslučitelné funkce
- Zastupitelnost
- Přenos zodpovědnosti
- IKT dodávky třetích stran

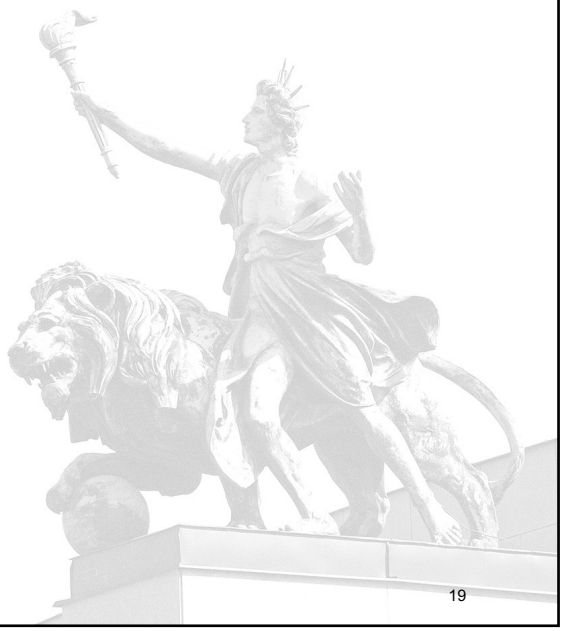
18

18

ČNB ČESKÁ NÁRODNÍ BANKA

Terminologická nejednotnost

- ISO 27xxx a popisy aktiv, rizik
  - Přiměřenost posuzování
  - Míra detaily x skupinová aktiva a rizika
- Referenční architektura
  - Pohled IT metodiky
  - Pohled DORA
- Outsourcing
  - Služby třetích stran
  - Outsourcing



19

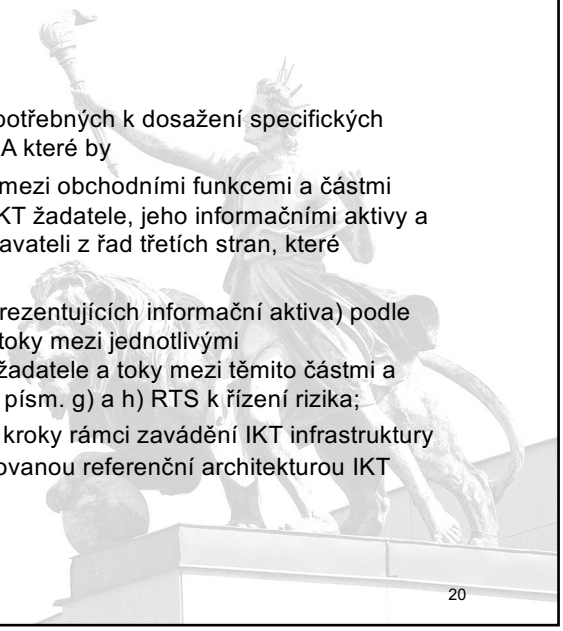
19

ČNB ČESKÁ NÁRODNÍ BANKA

Referenční architektura

Vysvětlení referenční architektury IKT a veškerých změn potřebných k dosažení specifických obchodních cílů podle písm. čl. 6 odst. 8 d) Nařízení DORA které by

- ve spojení s čl. 8 Nařízení DORA objasnilo souvislosti mezi obchodními funkcemi a částmi (vymezenými komponentami) referenční architektury IKT žadatele, jeho informačními aktivy a aktivy v oblasti IKT a službami IKT poskytovanými dodavateli z řad třetích stran, které obchodní funkce žadatele podporují a
- poskytlo přehled o datových tocích (přenosech dat reprezentujících informační aktiva) podle čl. 13 písm. b) RTS k řízení rizika zachycující alespoň toky mezi jednotlivými dekomponovanými částmi referenční architektury IKT žadatele a toky mezi těmito částmi a internetem a dalšími externími připojeními podle čl. 13 písm. g) a h) RTS k řízení rizika;
- ohledně potřebných změn představilo časový rámec a kroky rámci zavádění IKT infrastruktury a implementací řešení IKT Žadatele v souladu s popisovanou referenční architekturou IKT



20

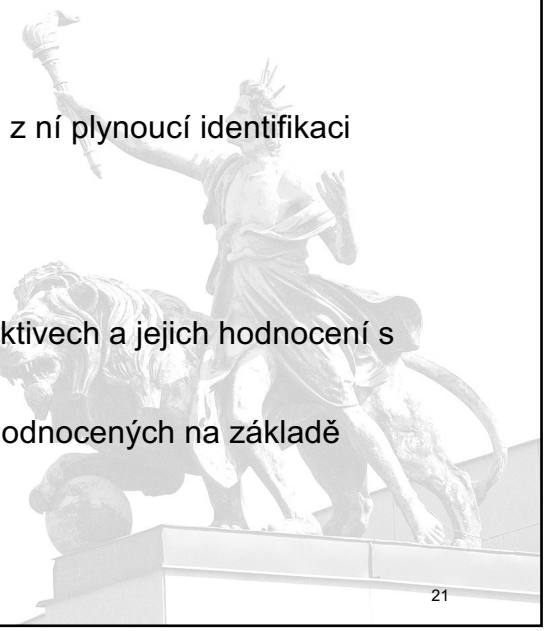
20

ČNB ČESKÁ NÁRODNÍ BANKA

Aktiva

Dora klade velký důraz na procesní analýzu a z ní plynoucí identifikaci Informačních aktiv:

- Proces jejich vyhledávání a hodnocení
- Vlastníci Informačních aktiv
- Výskyt Informačních aktiv na podpůrných aktivech a jejich hodnocení s ohledem na BIA analýzy
- Konstrukce rizik vycházejících z hrozeb a hodnocených na základě závažnosti Aktiv která ohrožují.



21

21

ČNB ČESKÁ NÁRODNÍ BANKA

3 úrovně ochrany, zastupitelnost a přenos zodpovědnosti

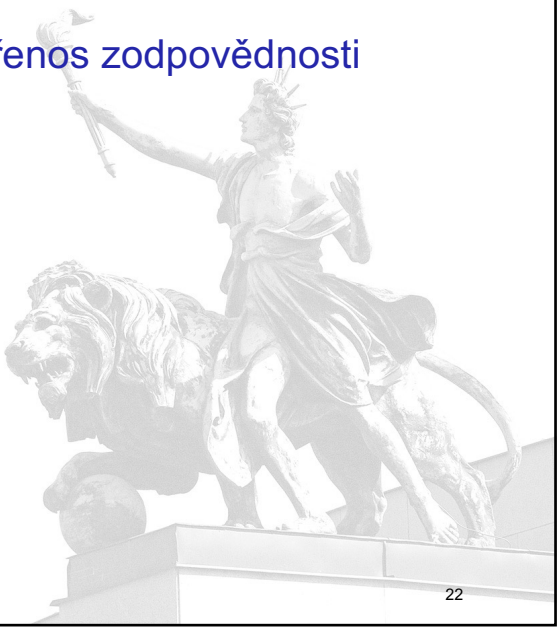
Tři úrovně ochrany proti selhání

- Řídící úroveň
- Kontrolní úroveň
- Auditní úroveň

Zastupitelnost

- Procesní pohled
- Provozní pohled s ohledem na SLA

Přenos zodpovědnosti



22

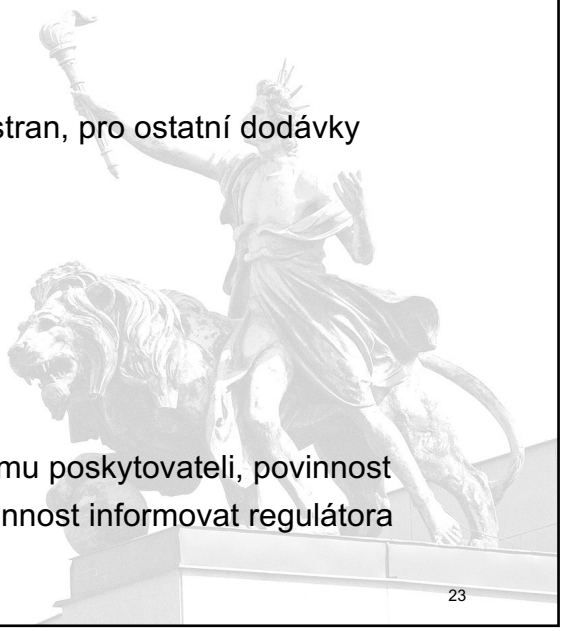
22

ČNB ČESKÁ NÁRODNÍ BANKA

Outsourcing x Služby třetích stran

Pro IT služby DORA používá Služby třetích stran, pro ostatní dodávky Outsourcing.

- Dodávkou se nepřenáší zodpovědnost
- Minima která musí být smluvně ošetřena
  - SLA a její měření
  - Vlastníci
  - Ukončení spolupráce
- Rizika koncentrace, rizika přechodu k jinému poskytovateli, povinnost hodnotit na základě vědomé znalosti, povinnost informovat regulátora

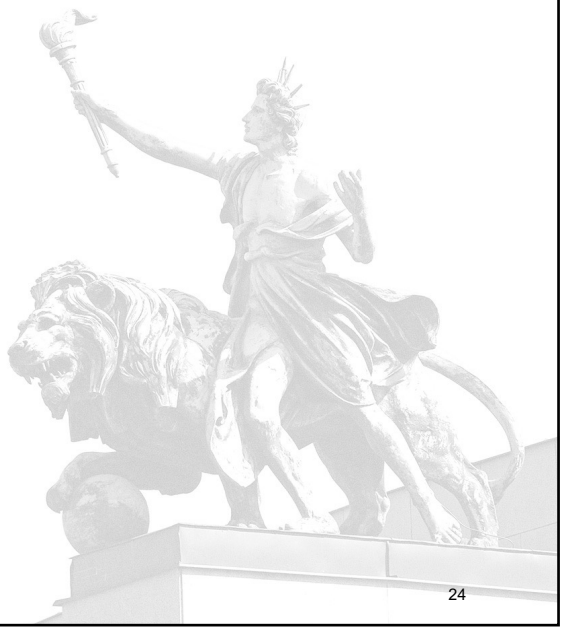


23

23

ČNB ČESKÁ NÁRODNÍ BANKA

Děkujeme za pozornost



24

24