DORA

Nařízení o digitální provozní odolnosti finančního sektoru

1

1

STRUKTURA PŘEDNÁŠKY

- Působnost nařízení
- Řízení rizik v oblasti ICT
- Hlášení ICT incidentů
- Testování
- Řízení rizik ICT od třetích stran
- Sdílení informací
- Prováděcí předpisy
- Implementační zákon

2

2

ÚVOD

3

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

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) **2022/2556** ze dne 14. prosince 2022, kterou se mění směrnice 2009/65/ES, 2009/138/ES, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 a (EU) 2016/2341, pokud jde o digitální provozní odolnost finančního sektoru

4

INSPIRACE

- Nařízení se částečně inspiruje řadou norem ISO/IEC 27000 (systémy řízení bezpečnosti informací)
- Explicitně nevyžaduje certifikaci
- Výjimky subjekty provádějící penetrační testování (čl. 27)
- Prováděcí legislativa má přihlédnout k mezinárodním normám

5

5

PŮSOBNOST

6

6

PŮSOBNOST

Čl. 2

- Banky, spořitelní a úvěrní družstva
- Pojišťovny, zajišťovny
- Obchodníci s CP
- Platební instituce, instituce elektronických peněz, včetně PPSMR a VEPMR, správce informací o platebním účtu

7

7

PŮSOBNOST

Čl. 2

- Centrální depozitář
- Obhospodařovatel, administrátor (ZiSIF)
- Poskytovatelé služeb související s kryptoaktivy, vydavatelé ART
- Zprostředkovatelé pojištění a zajištění
- Crowdfundingové platformy

8

8

PŮSOBNOST - VÝJIMKY

Čl. 2 odst. 2

- Zprostředkovatele pojištění a zajištění, kteří jsou SMEs
- § 3 odst. 2 ZPDZ
- V textu nařízení dílčí výjimky pro SMEs
- Výjimky pro PPSMR, VEPMR (např. čl.16)

9

9

MIMO PŮSOBNOST

- nebankovní poskytovatel spotřebitelského úvěru (§ 9 ZSÚ)
- penzijní společnost (§ 29 ZDPS)
- Investiční zprostředkovatel (§ 29 ZPKT)
- Směnárník (§ 4 ZSČ)

10

10

VYBRANÉ DEFINICE

- „informačním aktivem“ soubor informací, v hmotné i nehmotné formě, které je potřeba chránit;
- „aktivem v oblasti IKT“ softwarové nebo hardwarové aktivum v síti a informačních systémech používané finančním subjektem

11

11

Q&A

- Q&A ESAs

12

12

ŘÍZENÍ RIZIK V OBLASTI ICT

13

PROPORCIONALITA

Čl. 4

- Finanční subjekty uplatňují proporcionálně
- S ohledem na svou velikost, rizikový profil, povahu, rozsah a složitost služeb, činností a operací
- Obecný princip
- Čl. 16

14

ŘÍZENÍ A ORGANIZACE

Čl. 5

Povinnosti vedoucího orgánu

- Nese odpovědnost za veškeré postupy a řízení rizik
- Schvaluje a pravidelně přezkoumává strategie pro využití ICT
- Zavede komunikační kanál
  - o využití služeb ICT třetích stran
  - o dopadech změn na zásadní a důležité funkce
- Schvaluje a přezkoumává plány ICT auditu
- Pravidelná školení
- Definice vedoucího orgánu – sektorová legislativa

15

15

ŘÍZENÍ A ORGANIZACE

Čl. 5

- FI vytvoří funkci „manažera pro sledování ujednání o využití ICT třetích stran“

nebo

- pověří člena „senior managementu“ ke sledování souvisejících rizik a dokumentace

16

16

RÁMEC PRO ŘÍZENÍ ICT RIZIK

Čl. 6

- Rámec je součástí celkového řízení rizik
- Rámec zahrnuje:
  - Strategie
  - Politiky (programy)
  - Postupky (plán, metodika)
  - Protokoly

  Nezbytné pro ochranu informačních aktiv (co je třeba chránit) a aktiv v oblasti ICT (využívaný SW, HW)

17

17

RÁMEC PRO ŘÍZENÍ RIZIK

Čl. 6

- FI pověří kontrolní funkci za řízení a kontrolu rizika v oblasti ICT (assign the responsibility for managing and overseeing ICT risk to a control function) a zajistí její nezávislost
- FI zajistí oddělení a nezávislosti vedoucích, kontrolních fcí. a auditu (3 linie obrany)

18

18

RÁMEC PRO ŘÍZENÍ RIZIK

Čl. 6

- Rámec pro řízení ICT rizika se reviduje alespoň 1x ročně
  - Zpráva o přezkumu na žádost [čl. 27 prov. nař. 2024/1774]
- Podléhá internímu auditu
- Strategie digitální provozní odolností [6(8)]

19

19

IDENTIFIKACE

Čl. 8

- Obchodních funkcí, úloh a povinností podporovaných ICT a informačních aktiv a aktiv v oblasti ICT (1x ročně přezkum)
- Zdrojů rizik, vyhodnocení hrozeb a zranitelnosti, revize 1x ročně
- Kritická informační aktiva a aktiva v oblasti ICT
- Procesů závislých na ICT 3. stran; důraz na kritické fce.
- 1x ročně posouzení rizik u vlastních ICT

20

20

OCHRANA A PREVENCE

Čl. 9

Zajistit odolnost, kontinuitu provozu a dostupnost zásadních a důležitých funkcí

- Bezpečnost přenosu dat
- Minimalizovat riziko poškození nebo ztráty dat
- Předcházení narušení dostupnosti, hodnověrnosti, integrity a důvěrnosti dat
- Ochrana před poškozením/neadekvátní správou

21

21

OCHRANA A PREVENCE

Čl. 9

- Rozvedení politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2
  - čl. 8 a násl. prov. nař. 2024/1774

22

22

DETEKCE

Čl. 10

- Zavedení detekce neobvyklých aktivit (čl. 17)
- Monitoring aktivit uživatelů a výskytu anomálií ICT
- Stanovení prahových hodnot a kritérií pro spuštění reakce na incidenty; např. automatické výstražné mechanismy
- Monitoring incidentů

23

23

DETEKCE

Čl. 10

– čl. 23 prov. nař. 2024/1774

– Sektorové předpisy – návrh PSR: Article 83 Transaction monitoring mechanisms and fraud data sharing

– § 222 ZPS zůstává v účinnosti

– EBA Guidelines on ICT and security risk management 04/2019

24

24

REAKCE A OBNOVA

Čl. 11

Politika zachování provozu ICT

- Zajištění kontinuity zásadních a důležitých funkcí
- Rychlou a účinnou detekci incidentů a jejich vyřešení (omezení škod, obnovení činnosti)
- Aktivaci plánů – izolační opatření odpovídající různým typům incidentů a zamezení škodám
- Odhad předběžných dopadů a škod
- Komunikační kanály
- Plán (politika) podléhá internímu auditu (kromě malých)
- Testují plány (1x ročně, přechod na rezervní kapacitu) a testují i komunikační kanály
- Odhad ročních nákladů a ztrát způsobených incidenty (na žádost dohledu)
- čl. 24 až 26 prov. nař. 2024/1774

25

ZÁLOHOVÁNÍ A OBNOVA

Čl. 12

Politika zálohování a politika obnovy + postupy a metody obnovy

- Povinnost zřídit záložní systémy
- Obnova: využití syst. fyzicky oddělených od zdrojového ICT systému
- CCP – umožňují obnovit všechny obchody do okamžiku přerušení
- APA, ARM a CTP – zvláštní systémy a přiměřené zdroje (aby nedošlo k přerušení poskytování služeb)
- CSD – jedno sekundární místo (odst. 5) – fyzicky odděleno; zajištění kontinuity – provádění zásadních operací; ihned přístupné
- Všichni (kromě malých) rezervní kapacita pro zajištění jejich činnosti – malé podle rizikového profilu

26

POUČENÍ A ROZVOJ

Čl. 13

Prostředky na monitoring a přezkumy po incidentech

- Na žádost dohledu sdělí změny přijaté po incidentech (kromě malých)
- Co takový přezkum má obsahovat (odst. 2 třetí pododst.)
- Analýza incidentů, vzorců – míra expozice vůči riziku
- Školení zaměstnanců (všichni a vedoucí zaměstnanci)

27

27

KOMUNIKACE

Čl. 14

- Krizové komunikační plány s klienty, protistranami případně veřejností
- Komunikační strategie pro interní zaměstnance a externí zainteresované strany – rozlišení mezi pracovníky, kteří incident řeší a ostatními

28

28

PROPORCIONALITA

čl. 16

Čl. 5 až 15 se nepoužijí na:

- Malé OCP [čl. 12 IFR, resp. § 2 odst. 3 písm. u) ZPKT]
- Poskytovatel platebních služeb malého rozsahu (§ 58 ZoPS)
- Vydavatel elektronických peněz malého rozsahu (§ 99 ZoPS)
- Malou instituci zaměstnaneckého penzijního pojištění (do 100 účastníků)

29

29

ČL. 16

Je třeba zavést:

- Rámec pro řízení rizik
- Sledování bezpečnosti a funkčnosti systémů
- Minimalizovat rizika
- Rychlá identifikace a detekce zdrojů rizik
- Identifikace závislostí z řad třetích stran
- Zajištění provozu zásadních a důležitých funkcí
- Pravidelné testování a přijetí závěrů z testování

30

30

RTS

Čl. 15 a 16 odst. 3

ESMA, EBA a EIOPA ve spolupráci s ENISA

- Final draft report publikován 17. ledna 2024
- EUR-LEX

31

31

INCIDENTY SOUVISEJÍCÍ S ICT

32

32

PROCES ŘÍZENÍ INCIDENTŮ

- Povinnost zavést a uplatňovat proces řízení incidentů souvisejících s ICT (čl. 17)
- Proces obsahuje detekci, řízení a hlášení incidentů

33

33

PROCES ŘÍZENÍ INCIDENTŮ

Proces obsahuje

- Ukazatele včasného varování
- Postupy k identifikaci, sledování, evidenci, kategorizace a klasifikaci ICT incidentů
- Rozdělení odpovědnosti a úloh
- Plány komunikace
- Závažné incidenty hlášeny vedoucím osobám
- Postupy ke zmírnění dopadů

34

34

KLASIFIKACE INCIDENTŮ

- Čl. 18
- Počet dotčených klientů, transakcí
- Doba trvání
- Územní rozsah
- Ztráta údajů – dostupnost, hodnověrnost
- Význam zasažených služeb
- Ekonomický dopad

35

35

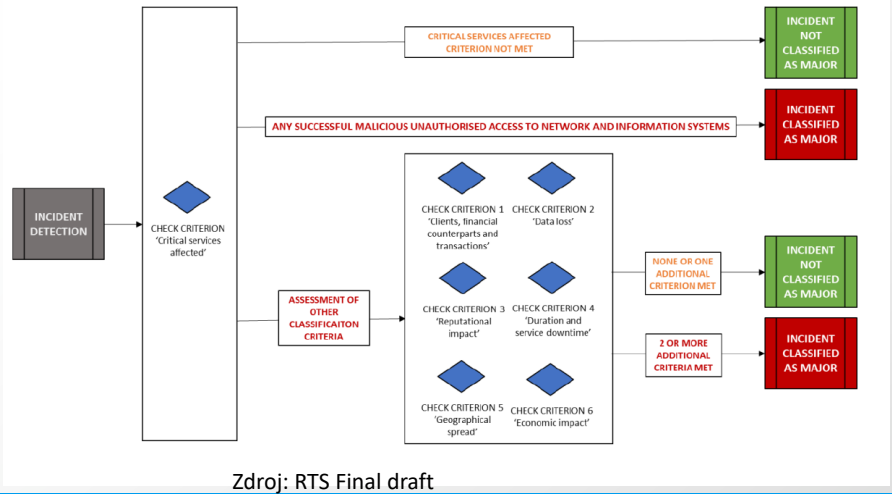
ZÁVAŽNÉ INCIDENTY

- Čl. 19
- Prahové hodnoty pro klasifikaci
- Závažné incidenty hlášeny dohledovému orgánu
- Předkládá se (formuláře čl. 20):
  - Prvotní oznámení
  - Průběžné oznámení
  - Závěrečná zpráva

36

36

RTS klasifikace incidentů



Zdroj: RTS Final draft

37

37

PROVÁDĚCÍ LEGISLATIVA

- ESAs, ECB a ENISA
- Návrh regulačních technických norem
- Prováděcí nařízení Evropské komise
  - Klasifikace incidentů
  - Harmonizace obsahu a vzorů hlášení
- EUR-lex a Final report 17. ledna 2024
- Formuláře hlášení 17. července 2024

38

38

V ČR

- Hlášení pouze dohledu – ČNB – ten posílá dál – nevyužito diskrece podle čl. 19 odst. 6 písm. e) DORA.
- Nový zákon o kybernetické bezpečnosti
- DORA lex specialis
- ZKB – registrace regulované služby, kontaktní údaje, protiopatření

39

39

ZKB - § 70

- **(1)** Pokud přímo použitelný předpis Evropské unie nebo jiný právní předpis, který zapracovává příslušný předpis Evropské unie, stanoví povinnosti v oblasti zavádění a provádění bezpečnostních opatření nebo hlášení kybernetických bezpečnostních incidentů a tyto povinnosti **mají alespoň srovnatelný účinek jako povinnosti podle tohoto zákona, ustanovení tohoto zákona upravující povinnosti zavádět a provádět bezpečnostní opatření a hlásit kybernetické bezpečnostní incidenty se neuplatní, a to včetně ustanovení o dozoru nad dodržováním uvedených povinností.**
- **(2)** Za ustanovení se srovnatelným účinkem jako povinnosti obsažené v tomto zákoně podle odstavce 1 se považují taková ustanovení přímo použitelného předpisu Evropské unie nebo jiného právního předpisu, který zapracovává příslušný předpis Evropské unie, která
- **a)** ve vztahu k povinnosti zavádět a provádět bezpečnostní opatření odpovídají alespoň požadavkům stanoveným v § 13 a 14, nebo
- **b)** ve vztahu k povinnosti hlásit kybernetické bezpečnostní incidenty odpovídají alespoň požadavkům stanoveným v § 15 a 16.
- **(3)** Za ustanovení se srovnatelným účinkem jako povinnosti obsažené v tomto zákoně podle odstavce 1 se dále považují taková ustanovení přímo použitelného předpisu Evropské unie, o nichž to **přímo použitelný předpis Evropské unie sám stanoví**.

40

40

INTERAKCE ORGÁNU DOHLEDU

- Potvrzení přijetí hlášení o incidentu
- Možnost poskytnout zpětnou vazbu
- Nenahrazuje „incident handling“ ze strany CSIRT/CERT týmů.

41

41

PLATEBNÍ SLUŽBY

- V případě úvěrových institucí, PI, EMI, správce informací o platebních účtu

+

- Působnost části týkající se incidentů rozšířena i na provozní a bezpečnostní incidenty související s platbami

42

42

TESTOVÁNÍ DIGITÁLNÍ PROVOZNÍ ODOLNOSTI

43

TESTOVÁNÍ

Čl. 24

- Obecné principy testování
- Proporcionalita
- Interní vs. externí testování
- 1-krát ročně všechny systémy a aplikace podporující zásadní a důležité funkce (výjimka malé entity)

44

TESTOVÁNÍ

Čl. 25

- Odst. 1 vyjmenovány testy, které se vztahují na všechny finanční subjekty (kromě malých)
- CSD a CCP speciální režim (odst. 2)
- Úlevy pro malé odst. 3

45

45

TLPT

Čl. 26

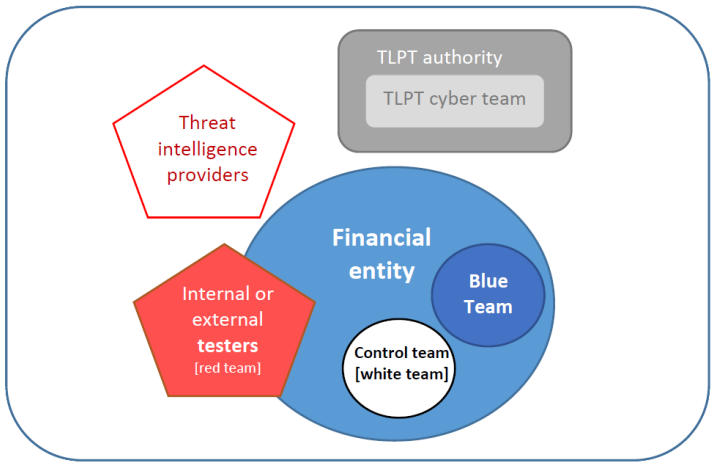
Penetrační testování na základě hrozeb

- Kdo: Other systemically important institutions, velké PI, EMI, CSD (čl. 2 RTS)
- Alespoň jednou za 3 roky (nevztahuje se na malé a čl. 16)
- Jeden ze tří testů musí být proveden externím subjektem
- Na reálných systémech
- Finanční subjekty vytypují důležité a zásadní funkce, které budou zahrnuty do testování (potvrzeno dohledovým orgánem) – odst. 2
- Může zadat přímo třetí strana ICT poskytovatel (podmínky odst. 4) a je možno spojit pro několik finančních subjektů (např. cloudový poskytovatel)
- Osvědčení o provedeném testu dohledem (odst. 7)

46

46

TLPT - RTS



Zdroj: RTS Final draft

47

47

TLPT - RTS

Čl. 26

Penetrační testování na základě hrozeb

- ESMA, EBA, EIOPA ve spolupráci s ENISA
- TIBER-EU
- Final draft 17. července 2024
- Nařízení EK 2025/1190

48

48

TLPT - TESTER

Čl. 27

Požadavky na osoby provádějící TLPT

- Požadavky na osoby (odst. 1)
- Dodatečné požadavky na interní osoby (odst. 2)
- Externí tester to musí být jednou za 3 testy

49

49

ŘÍZENÍ RIZIK ICT VE SPOJENÍ SE TŘETÍMI STRANAMI

50

50

HLAVNÍ ZÁSADY

Čl. 28

- Strategie pro riziko v obl. ICT spojené s třetími stranami
- Registr informací – všechna smluvní ujednání o využíváni ICT (individuální, subkonsolidovaný i konsolidovaný základ)
- 1-krát ročně počet nových ujednání se hlásí dohledu (odst. 3) včetně kategorie poskytovatele, druh smluvního ujednání a co je to za služby ICT
- Registr zpřístupní dohledu na žádost
- Informují dohled o plánovaném využití ICT služeb třetích stran pro zásadní a důležité funkce (pozor – pokud v sektorovém předpise je povolení (např. u CSD čl. 16 a 30 CSDR) má přednost sektorový předpis)

51

51

HLAVNÍ ZÁSADY

Čl. 28

- Před uzavřením smlouvy se posuzuje (odst. 4)
  - Zásadní a důležitá funkce
  - Soulad s dohledem
  - Relevantní rizika – zda přispívá k zesílení rizika koncentrace (čl. 29)
  - Přezkoumá potenciálního poskytovatele
  - Posoudí střet zájmů
- Smí uzavřít pouze s tím, které naplňuje nezbytné normy v oblasti bezpečnosti informací (odst. 5)
- Stanoví četnost auditů vůči poskytovateli (odst. 6)

52

52

HLAVNÍ ZÁSADY

Čl. 28

Možnost ukončení vztahu

- Poskytovatel ICT zásadním způsobem poruší platné předpisy nebo smluvní podmínky
- Při sledování rizika ICT se zjistí okolnosti, mohou změnit plnění funkcí nebo podstatných změn v ujednání či situaci u ICT poskytovatele
- U poskytovatele zjištěna slabá místa
- Není možno zajistit dohled
- U zásadních a důležitých funkcí strategie ukončení smluvního vztahu
- Finanční subjekt zajistí, že nedojde k narušení činnosti, narušení dodržování regulatorních požadavků, zhoršení kontinuity a kvality (při ukončení vztahu (odst. 8)
- RTS – třetí strany podporující zásadní a důležité funkce

53

53

RIZIKO KONCENTRACE

Čl. 29

Posuzování rizika koncentrace

- Není snadné ICT poskytovatele nahradit
- Podporují zásadní a důležité funkce se stejným poskytovatelem služeb ICT

- V takovém případně nutno zvážit alternativu
- U zásadních a důležitých funkci zhodnotit – Insolvenční právo, kontinuita, i zda z non-EU země + limitace třetích stran

54

54

SMLUVNÍ UJEDNÁNÍ

Čl. 30

Požadavky na smlouvy s ICT poskytovatelem

- Písemná, v jednom dokumentu (nebo trvalý nosič)
- Co musí obsahovat:
  - Popis všech funkcí
  - Místa, kde mají nasmlouvané funkce poskytovat, zpracovávat data i uchovávání dat
  - Ochrana dat a splnění D/H/I/D
  - Zajištění přístupu, obnovy a vracení v případě defaultu
  - Popis úrovně služeb, aktualizací a revizí
  - Poskytovatel se zaváže poskytnout pomoc v případě incidentu
  - Spolupráce s dohledem
  - Práva na ukončení smlouvy, výpověď …
  - Zapojení do školení dle čl. 13

55

55

SMLUVNÍ UJEDNÁNÍ

Čl. 30 odst. 3

Požadavky na smlouvy s ICT poskytovatelem

U zásadních a důležitých funkcí

- Detailní popis služby, aktualizace, revize, kvantitativní a kvalitativní výkonností cíle
- Výpovědní lhůta
- Uplatňovat a testovat plány zachování provozu a politika v oblasti ICT
- Povinnost pro poskytovatele ICT testovat – čl. 26 a 27
- Právo sledovat nepřetržitě poskytovatele – neomezené právo na audit, kontrolu pro finanční subjekt nebo dohled, alternativní úroveň záruky, spolupráce při kontrole na místě
- Strategie ukončení

56

56

RTS

Čl. 28 odst. 9 a 10 a čl. 30 odst. 5

- ESMA, EBA, EIOPA
- Nařízení EK 2025/532

57

57

DOHLED NAD KRITICKÝMI POSKYTOVATELI ICT

58

58

KRITICKÝ ICT POSKYTOVATEL

Kritický ICT TPP a dohled (oversight)

- Určený podle kritérií čl. 31 odst. 2 a RTS odst. 6 (do 17. července 2024 - EK)
- Hlavní orgán dohledu jeden z ESAs (EBA, ESMA nebo EIOPA) – největší podíl celkových aktiv
- Výjimky odst. 7
- U ICT TPP ze třetích zemí povinnost mít dceru do 1 roka od určení

59

59

KRITICKÝ ICT POSKYTOVATEL

Fórum dohledu

- EBA, ESMA a EIOPA
- Zástupce dohledového orgánu z každého státu
- ECB, ESRB, Komise, ENISA
- Případně zástupci NIS úřadů (NÚKIB)
- Seznam na webech ESAs

60

60

KRITICKÝ ICT POSKYTOVATEL

Pravomoc dohledu

- Posouzení (čl. 33 odst. 3)
- Plány dohledu
- Možnost požádat o informace
- Provádět obecná šetření a kontroly i na místě
- Vydávat doporučení

61

61

KRITICKÝ ICT POSKYTOVATEL

Doporučení a následky (čl. 42)

- Reakce na doporučení v 60 dnech
- V případě non-compliance
- Dohled informuje příslušné finanční subjekty
- Ty přijmou opatření na řešení rizik plynoucích z nezahrnutí doporučení
- V krajním případně to může vést k rozhodnutí (do 60 dnů od upozornění) o částečném nebo úplném využívání služeb ICT od daného poskytovatele (odst. 4 a 6)

62

62

SDÍLENÍ INFORMACÍ O KYBERNETICKÝCH HROZBÁCH

63

SDÍLENÍ INFORMACÍ O ICT HROZBÁCH

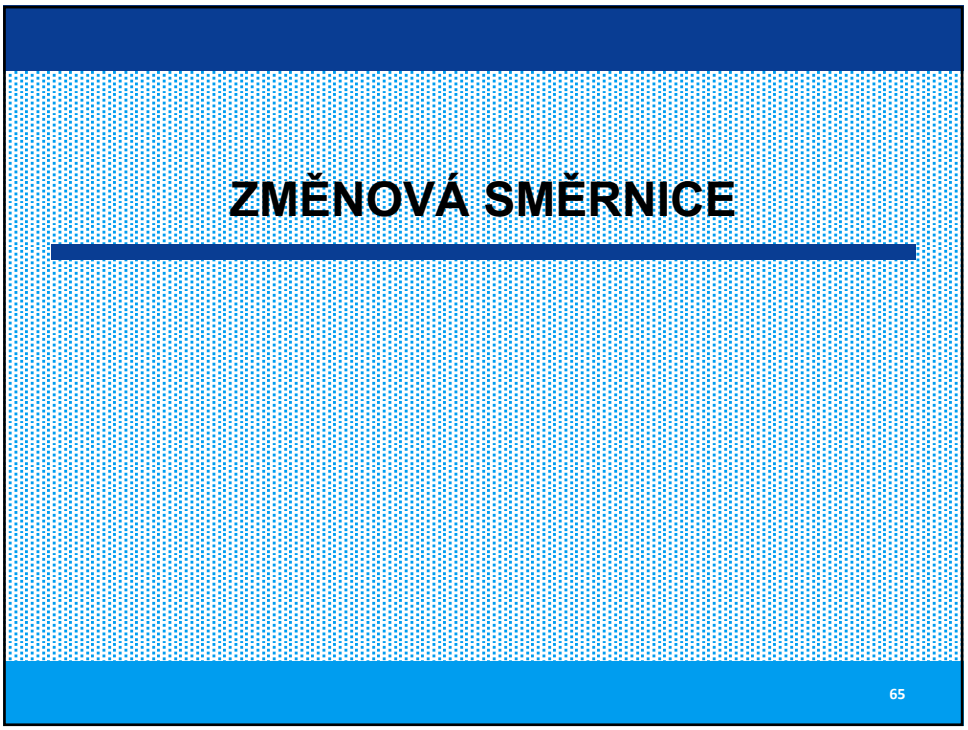
Čl. 45

Podmínky pro sdílení informací o operativních a kybernetických hrozbách mezi finančními institucemi

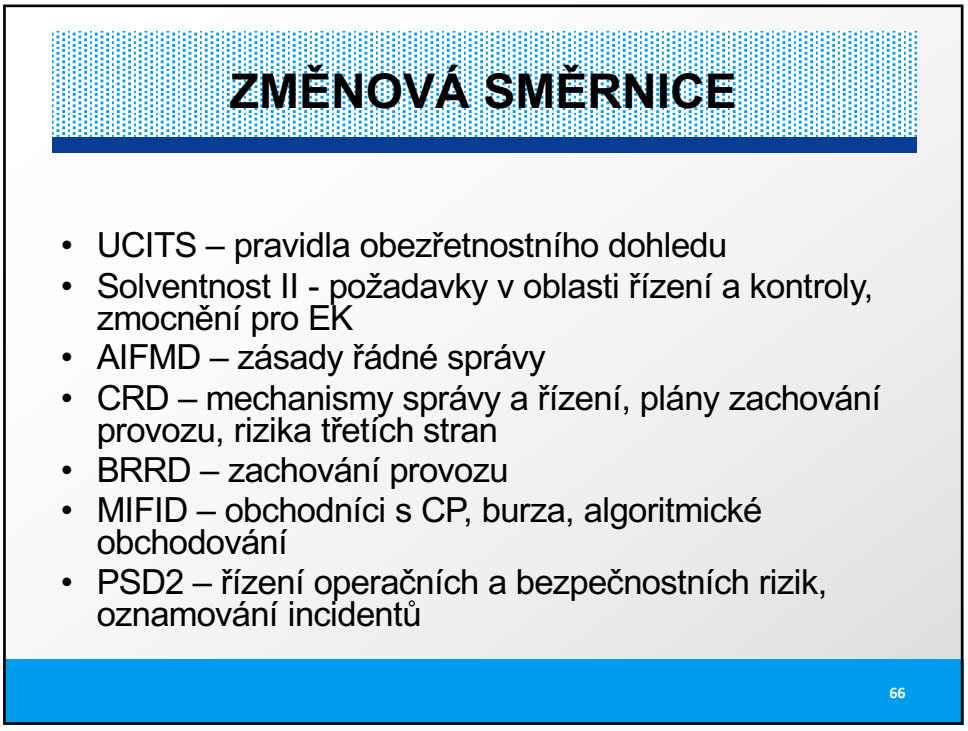
x

Návrh PSR (čl. 83)

64


ZMĚNOVÁ SMĚRNICE
65

65


ZMĚNOVÁ SMĚRNICE
• UCITS – pravidla obezřetnostního dohledu
• Solventnost II - požadavky v oblasti řízení a kontroly, zmocnění pro EK
• AIFMD – zásady řádné správy
• CRD – mechanismy správy a řízení, plány zachování provozu, rizika třetích stran
• BRRD – zachování provozu
• MIFID – obchodníci s CP, burza, algoritmické obchodování
• PSD2 – řízení operačních a bezpečnostních rizik, oznamování incidentů
66

66

ÚČINNOST

NAŘÍZENÍ I SMĚRNICE

17. LEDEN 2025

67

67

EK

- REGISTER OF DELEGATED ACTS
- Schválené verze (vzor ESAs final drafts)
- Q&A ESAs

68

68

ZÁKON O IMPLEMENTACI PŘEDPISŮ EVROPSKÉ UNIE V OBLASTI DIGITÁLNÍCH FINANCÍ (ZÁKON O DIGITALIZACI FINANČNÍHO TRHU)

- Z. č. 31/2025; účinnost 15. 2. 2025
- Dohled vykonává ČNB, trestá porušení povinností – DORA přestupky § 16 (10, 20 nebo 50 mil. Kč)
- Dohledová opatření (donucovací pokuty až do výše 20 mil. Kč)

69

69

DĚKUJI ZA POZORNOST!

TOMÁŠ NÝDRLE

70

70