01

DORA - stručné vysvětlení

Setkání interních auditorů z finančního sektoru

1.6.2023

Tomáš Kudělka, KPMG

DORA - stručně vysvětleno

Iniciativu "Digitální operační odolnost" zveřejnila Evropská komise na konci září 2020 jako návrh balíčku opatření k další digitalizaci finančního sektoru. Cílem je posílit konkurenceschopnost a inovace finančního trhu.

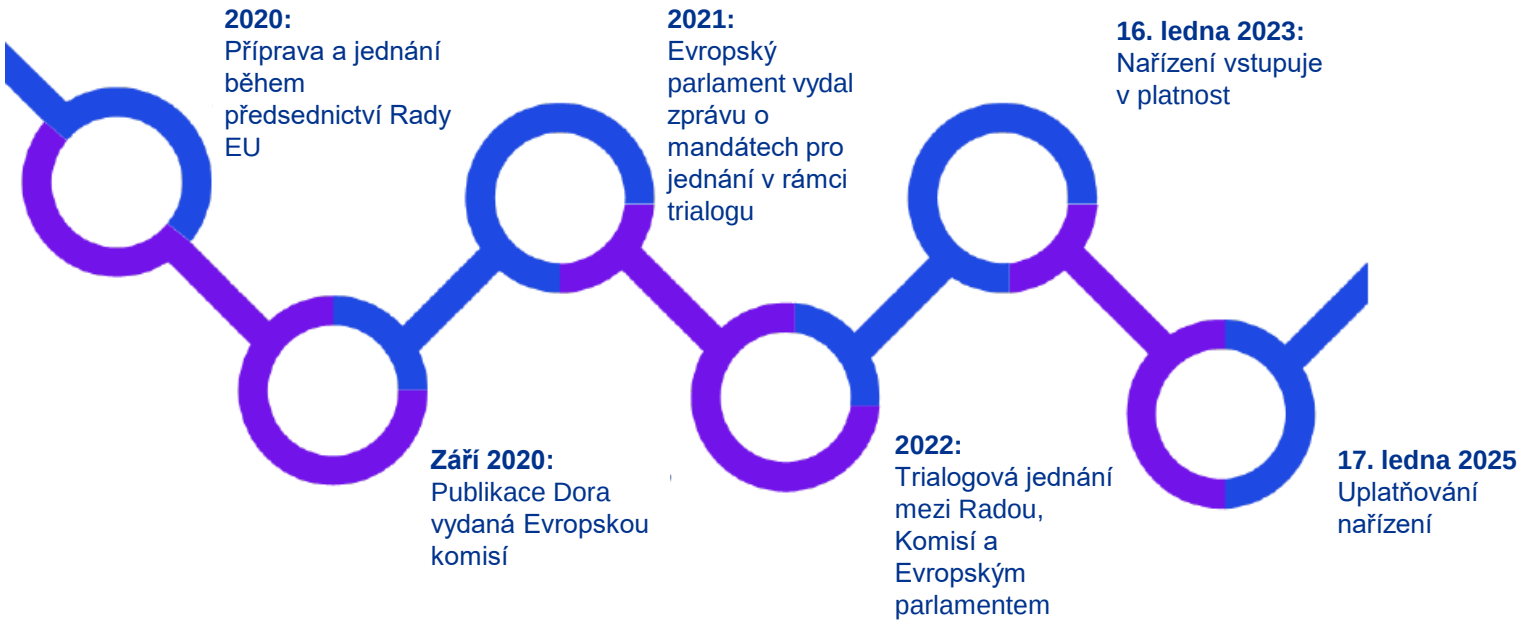
Návrh rozšiřuje stávající předpisy (MaGo, VAIT atd.) a řeší požadavky týkající se digitálních rizik.

Důležitými prvky jsou harmonizace předpisů pro řízení rizik informačních a komunikačních technologií (IKT), podávání zpráv, audity a hodnocení rizik externích poskytovatelů IKT.

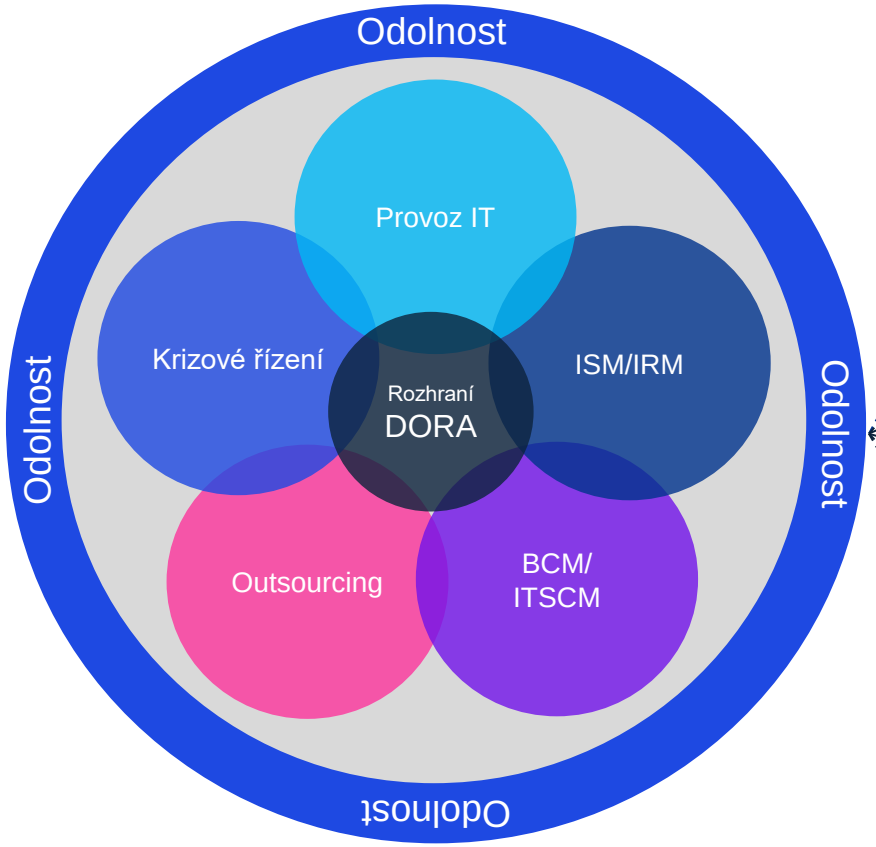
Záměr DORA

Cílem DORA je sjednotit stávající evropské i vnitrostátní normy a požadavky a vytvořit podrobný a komplexní rámec pro digitální provozní stabilitu finančních podniků v EU.

Důraz je kladen na zachování (digitálních) obchodních operací a souvisejících procesů a služeb v případě incidentu souvisejícího s IKT, zejména pokud by jejich trvalé selhání mohlo vést k nestabilitě celého evropského finančního systému.



Vaše šance díky efektivní implementaci požadavků DORA



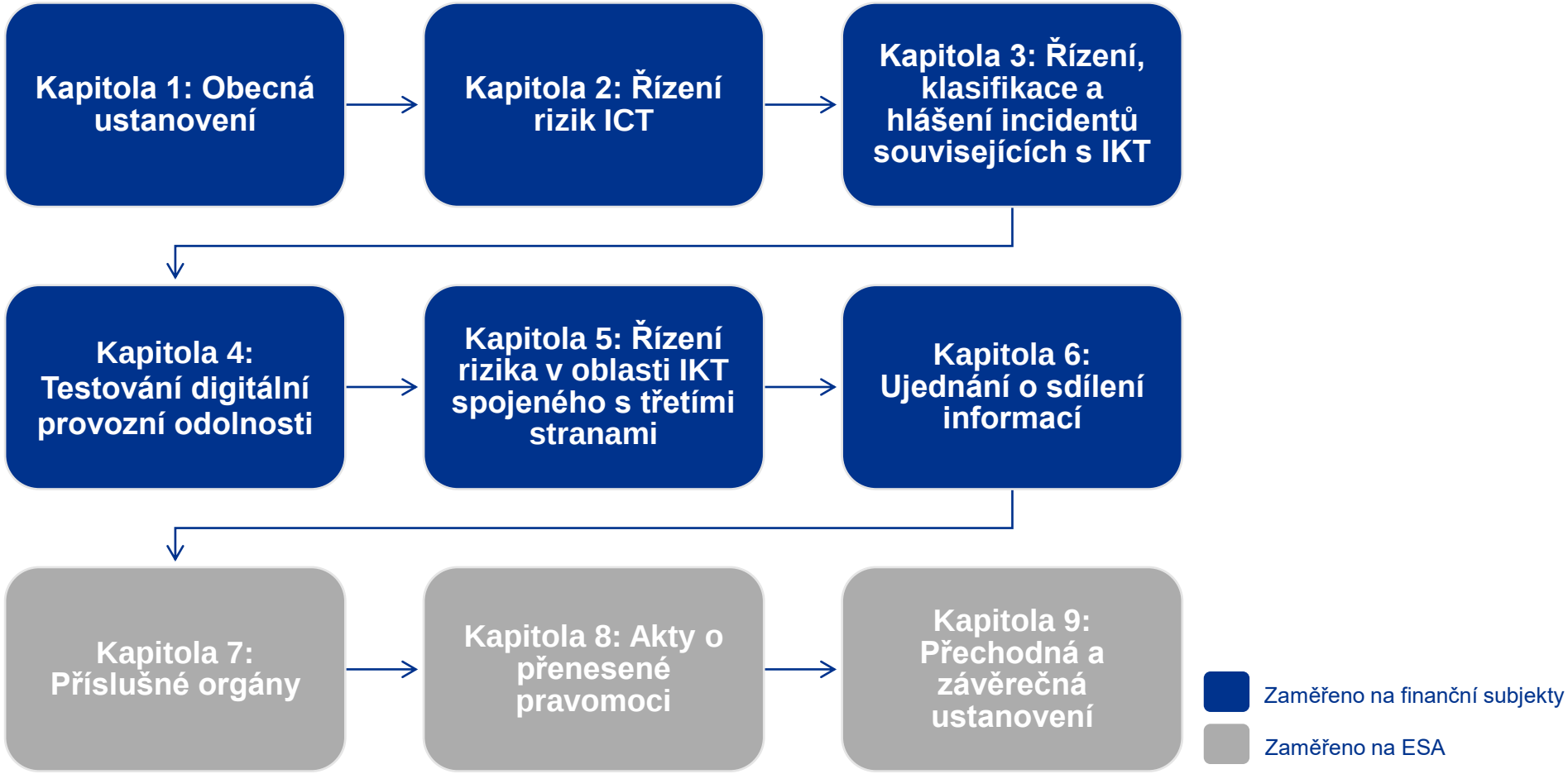
Přehled holistické perspektivy

- Podpora **prolomení klasického "silového myšlení"** v rámci funkcí druhé linie obrany (ISMS/BCMS).
- Příležitost k **synergickému potenciálu** díky užšímu propojení oborů ISM/IRM, krizového řízení, outsourcingu a BCM/ITSCM.
- Možné **úspory nákladů a úsilí** díky cílenější koordinaci oborů a mezi nimi.
- Jasné **vymezení rolí a odpovědností**, jednotné koncepty komunikace a efektivnější činnost.
- Lepší sladění oblastí zajišťuje **větší odolnost a schopnost reagovat v** případě vnějších vlivů (kybernetické útoky, narušení, mimořádné události/krize atd.).
- **Efektivnější výběr** opatření zapojením příslušných a mezioborových zúčastněných stran.

02

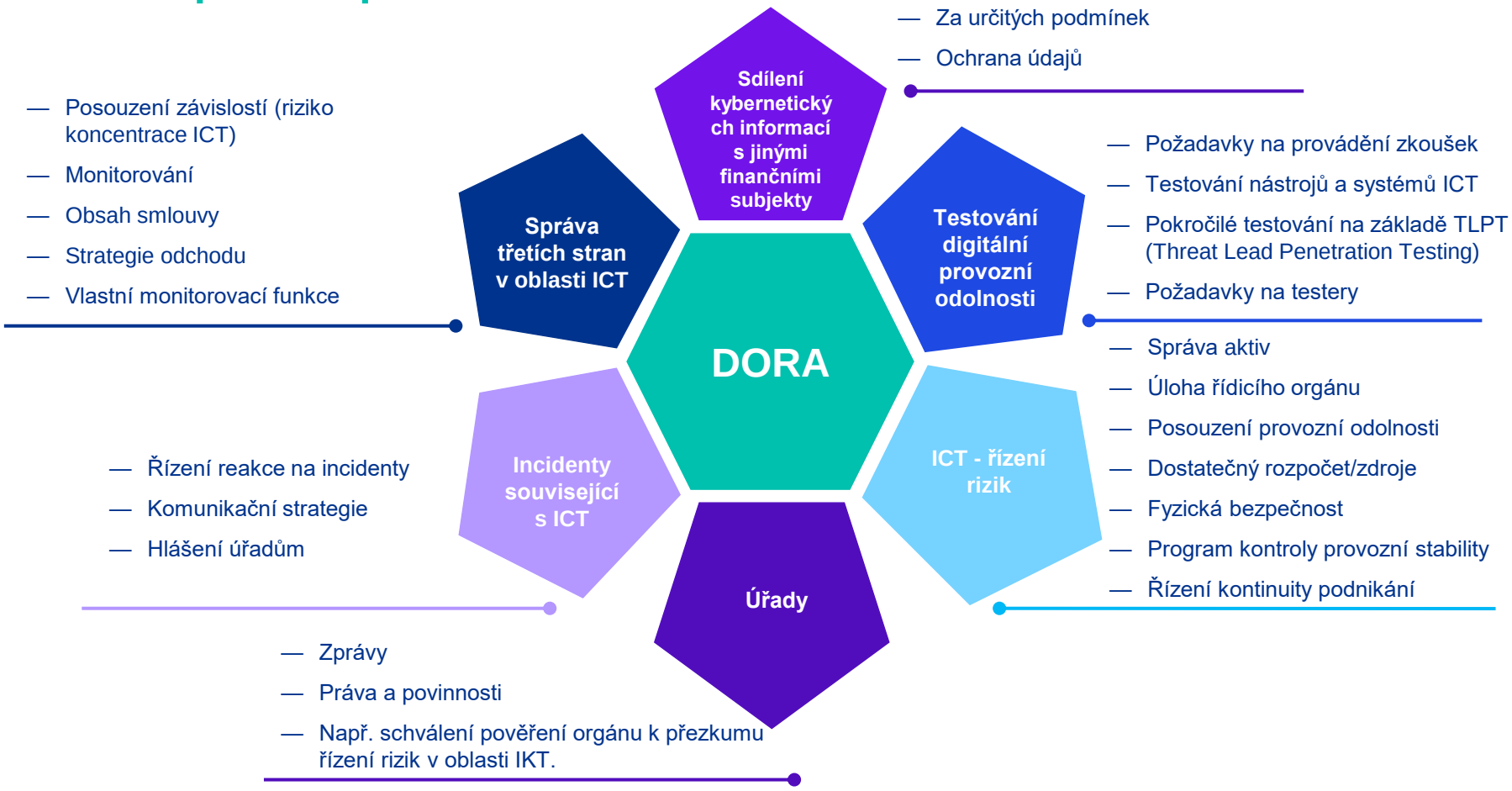
DORA - hluboký ponor

DORA | Přehled kapitol



Kapitola 1 - obecná ustanovení - hlavní části zákona DORA

Obecná ustanovení - přehled kapitola 1



Vybrané články zobrazené v mezinárodním cyklu řízení rizik

Přehledový článek 5- 45

Rámec řízení rizik ICT

Článek 5: Řízení a organizace	**Článek 6:** Rámec pro řízení rizika v oblasti IKT	**Článek 7:** Systémy, protokoly a nástroje IKT

6. Učte se
— **Článek 13:** Učení a vývoj

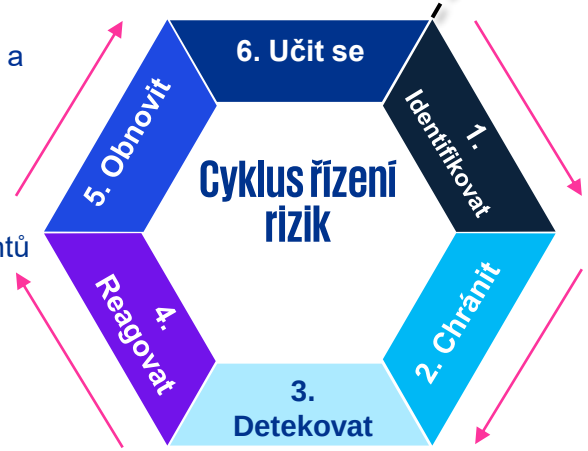
Start

— **Článek 14:** Komunikace
— **Článek 45:** Ujednání o sdílení informací

5. Obnovovat
— **Článek 12:** Strategie zálohování a obnovy dat

— **Článek 11:** Reakce a zotavení

4. Reagovat na
— **Článek 17:** Proces řízení incidentů souvisejících s IKT
— **Článek 19:** Hlášení závažných incidentů souvisejících s IKT
— **Článek 22:** Zpětná vazba od dohledu



1. Identifikovat
— **Článek 8:** Identifikace
— **Článek 29:** Předběžné posouzení rizika koncentrace ICT na úrovni subjektu

2. Chránit
— **Článek 9:** Ochrana a prevence
— **Článek 24-27:** Testování digitální provozní odolnosti
— **Článek 28/30** Obecné zásady/ klíčová smluvní ustanovení [s poskytovateli ICT - třetími stranami]

3. Detekovat
— **Článek 10:** Detekce
— **Článek 18:** Klasifikace incidentů v oblasti IKT a kybernetických hrozeb

DORA nezahrnuje pouze finanční subjekty, ale týká se více než 15 různých typů institucí.

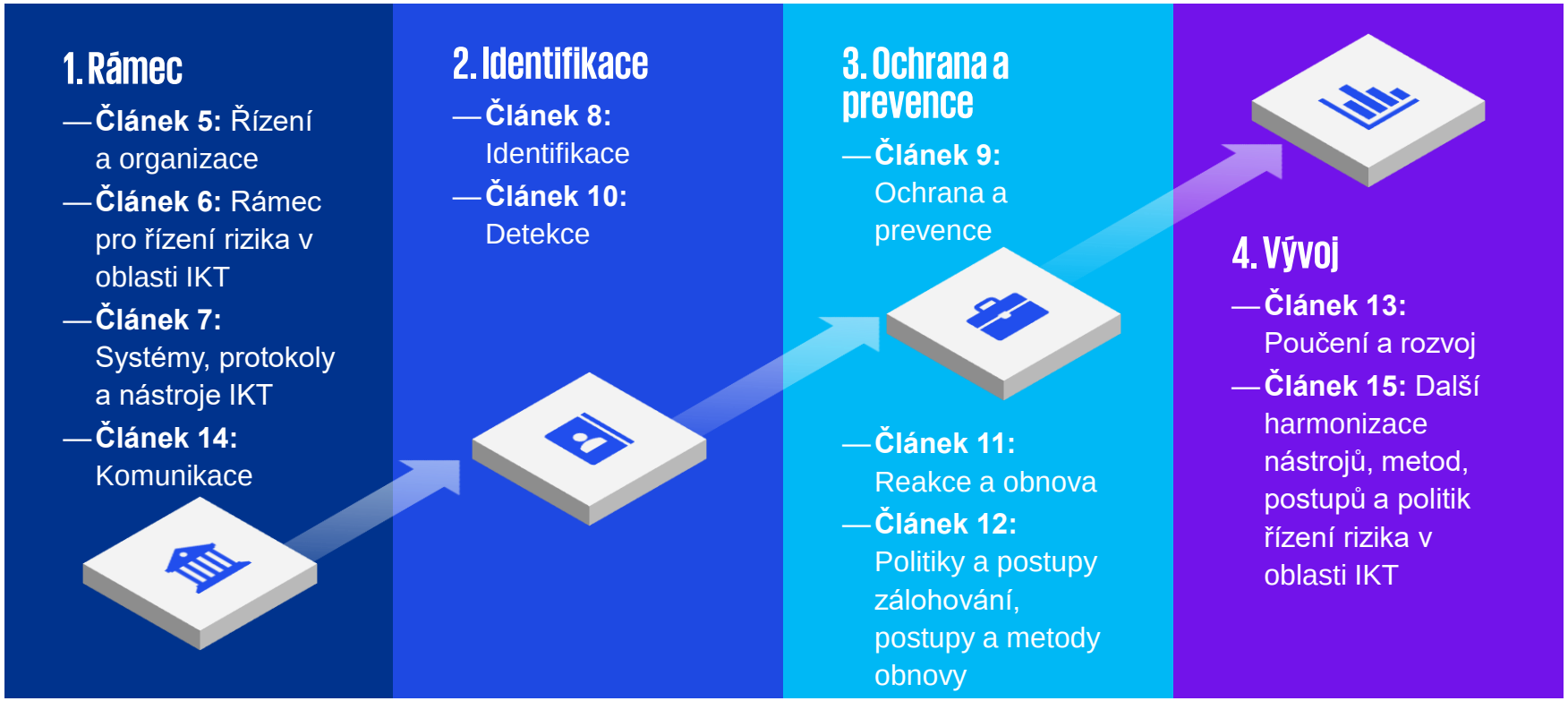
Obecná ustanovení - přehled kapitola 1

Platnost zákona se vztahuje i na finanční společnosti a poskytovatele informačních a komunikačních technologií třetích stran.

Úvěrové instituce	Platební instituce	Poskytovatelé účetních informačních služeb	Instituce elektronických peněz
Investiční společnosti	Poskytovatelé kryptoaktivních služeb a emitenti tokenů odkazujících na aktiva	Centrální depozitáře cenných papírů	Ústřední protistrany
Obchodní místa	Obchodní úložiště	Správci alternativních investičních fondů	Správcovské společnosti
Poskytovatelé služeb vykazování dat	Pojišťovací a zajišťovací subjekty	Zprostředkovatelé pojištění, zprostředkovatelé zajištění	Instituce zaměstnaneckého penzijního pojištění
Ratingové agentury	Správci kritických referenčních úrovní	Poskytovatelé služeb crowdfundingu	Poskytovatelé služeb třetích stran v oblasti ICT

Druhá kapitola představuje čtyři obecné zásady pro řízení rizik v oblasti ICT.

Řízení rizik ICT - přehled kapitola 2 (články 5-15)



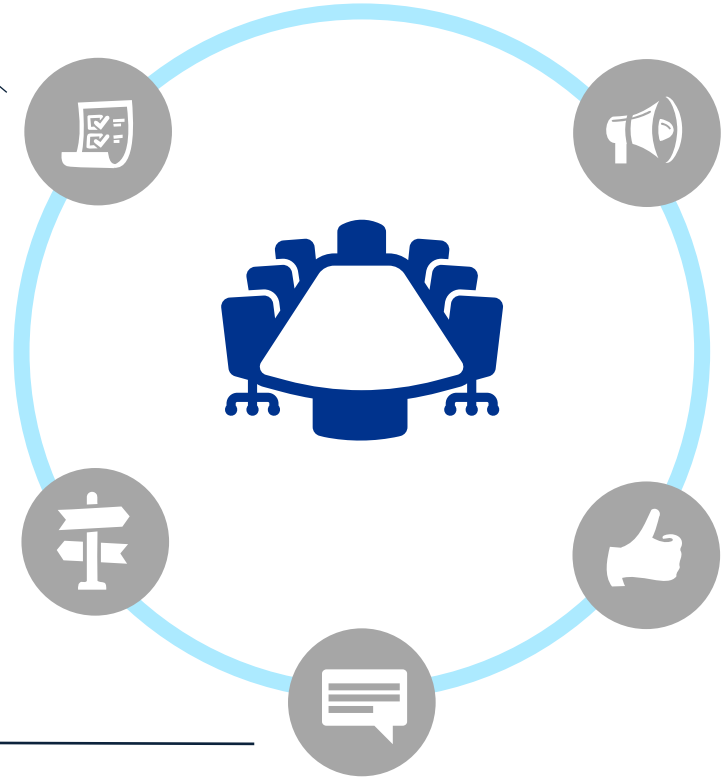
Článek 5 popisuje všechny příslušné povinnosti řídícího orgánu.

Podrobně kapitola 2 (článek 5)

Zavedení zásad

Vysoké standardy

- Dostupnost
- Autentičnost
- Integrita
- Důvěrnost údajů



Uspořádání kanálů pro podávání zpráv, které je informují o

- Ujednání uzavřená se službou ICT třetí strany
- Příslušné plánované změny materiálu
- Potenciální dopad na kritické nebo důležité funkce

Stanovení jasných rolí

Pro všechny funkce související s ICT

- Zavedení vhodných mechanismů řízení

Schválení a přezkoumání

- Politika kontinuity provozu ICT finančního subjektu
- Plány interního auditu ICT
- Rozpočet
- Politika finančního subjektu týkající se ujednání (poskytovatel ICT jako třetí strana)

Nést odpovědnost

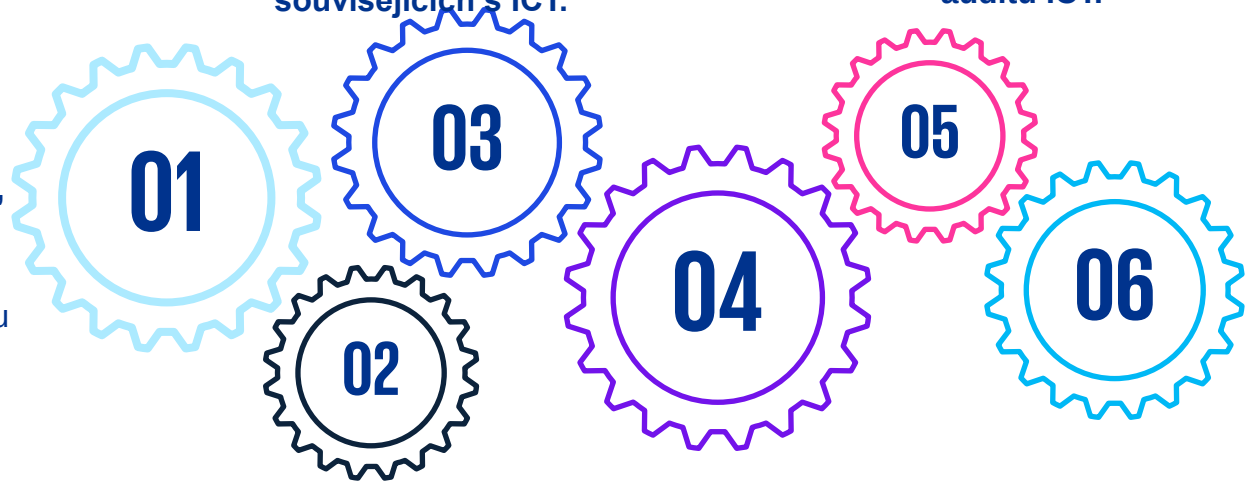
Pro strategii digitální provozní odolnosti

DORA vyžaduje rámec pro řízení rizik ICT, který umožňuje efektivní řešení rizik ICT.

Podrobně kapitola 2 (článek 6)

Součásti rámce řízení rizik ICT

Strategie, postupy, protokoly a nástroje ICT pro minimalizaci dopadu rizik ICT.



Přezkoumání a zdokumentování alespoň jednou ročně a v případě výskytu **závažných incidentů souvisejících s ICT.**

Zavedení **následného postupu,** včetně pravidel pro včasné ověření a nápravu **kritických zjištění auditu ICT.**

Strategie digitální odolnosti, která definuje **způsob provádění rámce (čl. 6 odst. 8 písm. a) až h)).**

Úplné a aktuální **informace o** rizicích v oblasti informačních a komunikačních technologií.

Pravidelné přezkoumávání rámce řízení rizik ICT **auditory ICT.**

Aby bylo možné řešit a řídit rizika ICT, měly by systémy, protokoly a nástroje používané finančními subjekty splňovat následující předpoklady

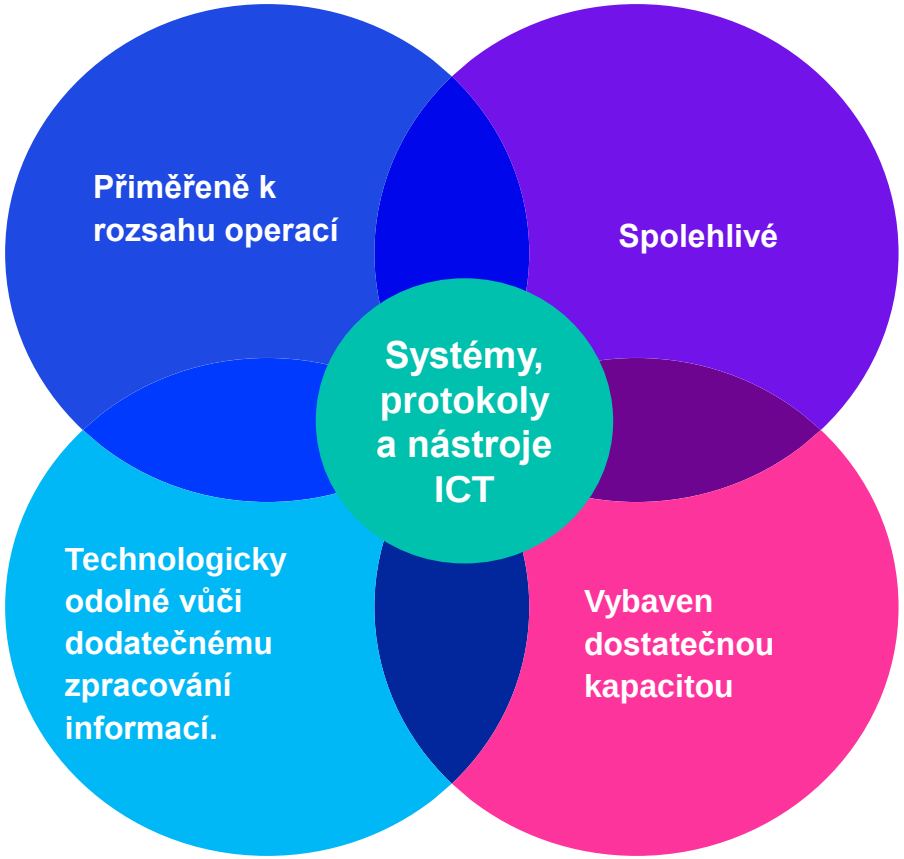
Podrobně kapitola 2 (článek 7)

Systém ICT:

— počítače, komunikace, zpracování dat, elektronické řídicí systémy (digitální nebo analogové)

— Včetně webových stránek, intranetu, extranetu, souborů a připojení

— počítačem podporovaný design, výrobní zařízení, hardwarové a softwarové součásti všech těchto systémů.



Např. pomocí nástrojů SIEM (SIEM = SIM +SEM).

— Správa bezpečnostních informací (SIM) a správa bezpečnostních událostí (SEM)

— Poskytování analýz v reálném čase pomocí výstrah

— Shromažďování událostí zabezpečení a dat protokolů z různých zdrojů

— 360stupňový pohled na všechny systémy

Protokoly ICT

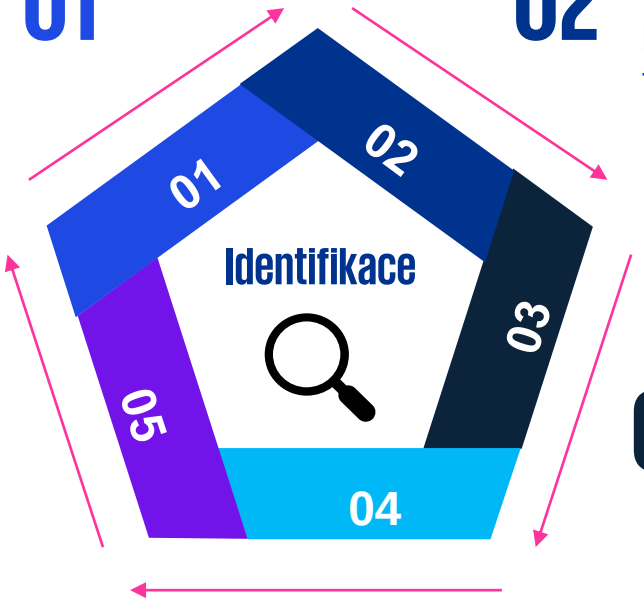
— zavedený soubor pravidel, která určují, jak se data přenášejí mezi různými zařízeními v téže síti.

Identifikace všech podnikových funkcí podporovaných ICT je zásadní pro účinné řízení rizik ICT.

Podrobně kapitola 2 (článek 8)

01 Podnikání, funkce, role atd. podporované ICT.

02 Informační prostředky a prostředky ICT podporující tyto funkce



03 Všechny procesy závislé na poskytovatelích služeb ICT třetích stran; identifikace propojení s poskytovateli, kteří podporují kritické nebo důležité funkce.

04 Provedení hodnocení rizik

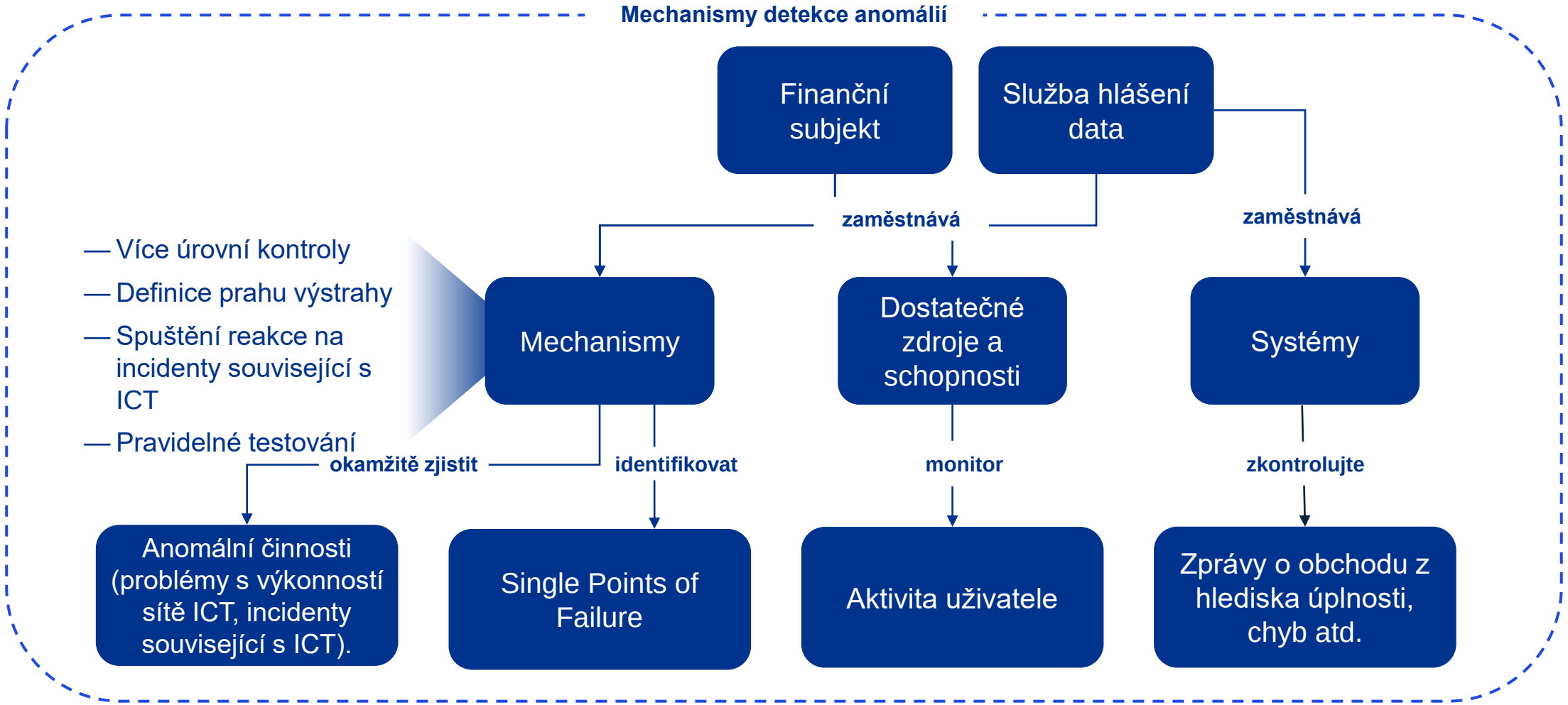
05 Přezkoumání alespoň jednou ročně nebo při významných změnách.

Ochrana a prevence jsou nedílnou součástí účinného řízení rizik v oblasti IKT.

Podrobně kapitola 2 (článek 9)

Za účelem rychlého odhalení anomálních činností musí mít finanční subjekty zavedeny mechanismy, které umožňují

Podrobně kapitola 2 (článek 10)



Je nutné vhodně řídit plány kontinuity provozu.

Podrobně kapitola 2 (článek 11)

Cíle

Politika kontinuity provozu ICT, jejímž cílem je:

— Zajištění funkcí **kontinuity**

— **Reagovat na** všechny incidenty související s ICT a řešit je.

— Neprodleně aktivujte **opatření pro omezení šíření**

— Odhad **škod** a **ztrát**

— Stanovení opatření v oblasti komunikace a **krizového řízení**

Recenze/ testování

— **Plány odezvy** a **obnovy** ICT podléhají nezávislému internímu auditu.

— pravidelně (alespoň jednou ročně) **testovat plány kontinuity,** zejména s ohledem na kritické funkce zadané externím poskytovatelům služeb ICT.

— Provedení **analýzy dopadů na podnikání** (BIA)

Během incidentů

— **Záznamy o činnostech** před událostmi narušení a během nich, kdy jsou aktivovány plány kontinuity provozu ICT a plány reakce a obnovy ICT.

Opatření k vhodnému řízení plánů kontinuity provozu

Prostřednictvím řízených zásad zálohování lze dosáhnout vysoké úrovně integrity.

Podrobně kapitola 2 (článek 12)

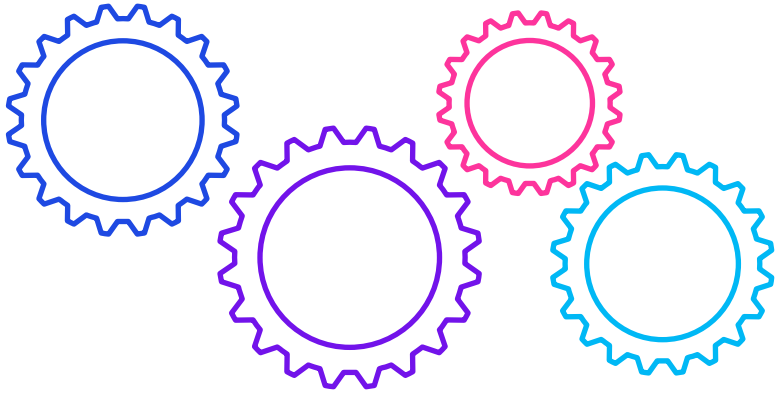
Cíle

- **Obnova** s minimálními prostoji, omezeným narušením a ztrátami (služby hlášení dat po celou dobu).
- Definujte **rozsah** údajů a minimální **četnost na** základě kritických údajů.
- Aktivace záložních systémů **nesmí ohrozit** bezpečnost systému.
- Ústřední protistrany: **vymáhání všech transakcí v** době narušení.

Požadavky

Nadbytečné kapacity ICT

Fyzicky a logicky oddělené



Testování se provádí **pravidelně**

Centrální depozitáři udržuje alespoň jedno **sekundární zpracovatelské místo.**

Při obnově po incidentu proveďte nezbytné **kontroly,** aby byla zachována **nejvyšší úroveň integrity dat.**

Finanční subjekty se poučí z incidentů souvisejících s IKT a odpovídajícím způsobem vyvinou své strategie.

Podrobně kapitola 2 (článek 13)

Operativní učení

— Řádné průběžné **zapracovávání poznatků** získaných z **testování provozní odolnosti do** procesu hodnocení rizik v oblasti ICT.

— Sledování **účinnosti strategie digitální provozní odolnosti.**

  — vývoj rizika ICT v čase

  — četnost, typy, rozsah a vývoj incidentů souvisejících s IKT.

— **Školení** zaměstnanců/programy zvyšování povědomí o bezpečnosti

— průběžně **sledovat** příslušný **technologický vývoj**

Komunikační plány jsou nezbytné pro všechny zúčastněné strany

Podrobně kapitola 2 (článek 14)

Zásady komunikace pro **interní** zaměstnance a **externí** zúčastněné strany

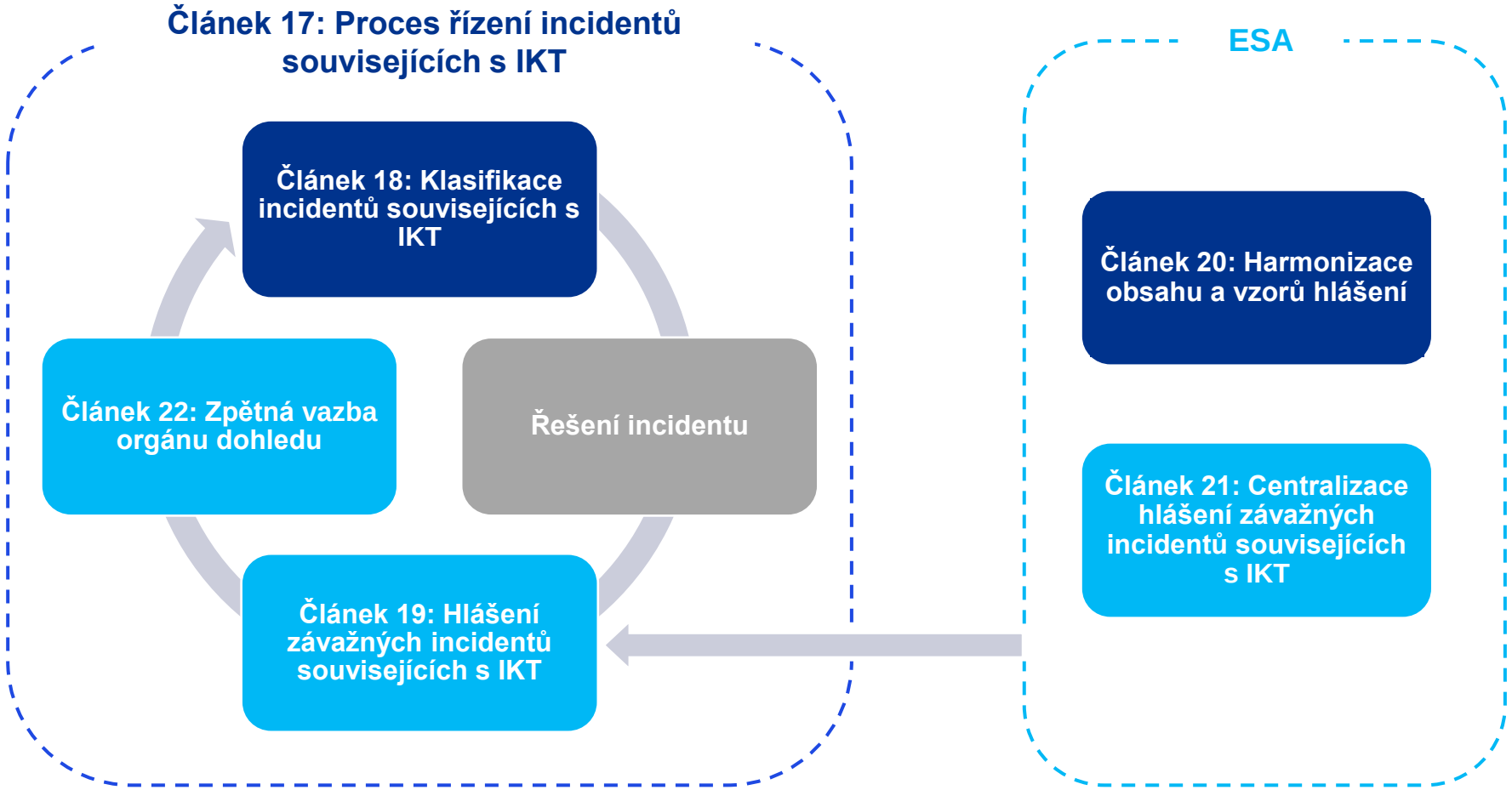
informování (minimálně) klientů a partnerů, případně i veřejnosti, o závažných incidentech nebo zranitelnostech souvisejících s IKT.

Alespoň jedna osoba ve finančním subjektu je pověřena **prováděním komunikační strategie pro případy související s IKT** a za tímto účelem plní **funkci pro veřejnost** a **média.**

Rozlišujte mezi **zaměstnanci zapojenými do** řízení rizik ICT a **zaměstnanci, které** je třeba informovat.

Řízení, klasifikace a hlášení incidentů souvisejících s ICT

Přehled kapitola 3 (články 17-23)



Proces řízení incidentů souvisejících s ICT se skládá ze šesti hlavních úkolů

Podrobně kapitola 3 (článek 17)

Zavedení a provádění procesu řízení incidentů souvisejících s IKT za účelem **odhalování**, **řízení** a **oznamování** incidentů souvisejících s IKT.

01

Zavedení ukazatelů včasného varování

02

Zavedení postupů pro identifikaci, sledování, zaznamenávání, kategorizaci a klasifikaci incidentů souvisejících ICT podle jejich priority.

03

Přiřazení rolí a odpovědností, které je třeba aktivovat pro různé typy incidentů a scénářů souvisejících s ICT.

04

Plány komunikace se zaměstnanci, externími zúčastněnými stranami a médii

05

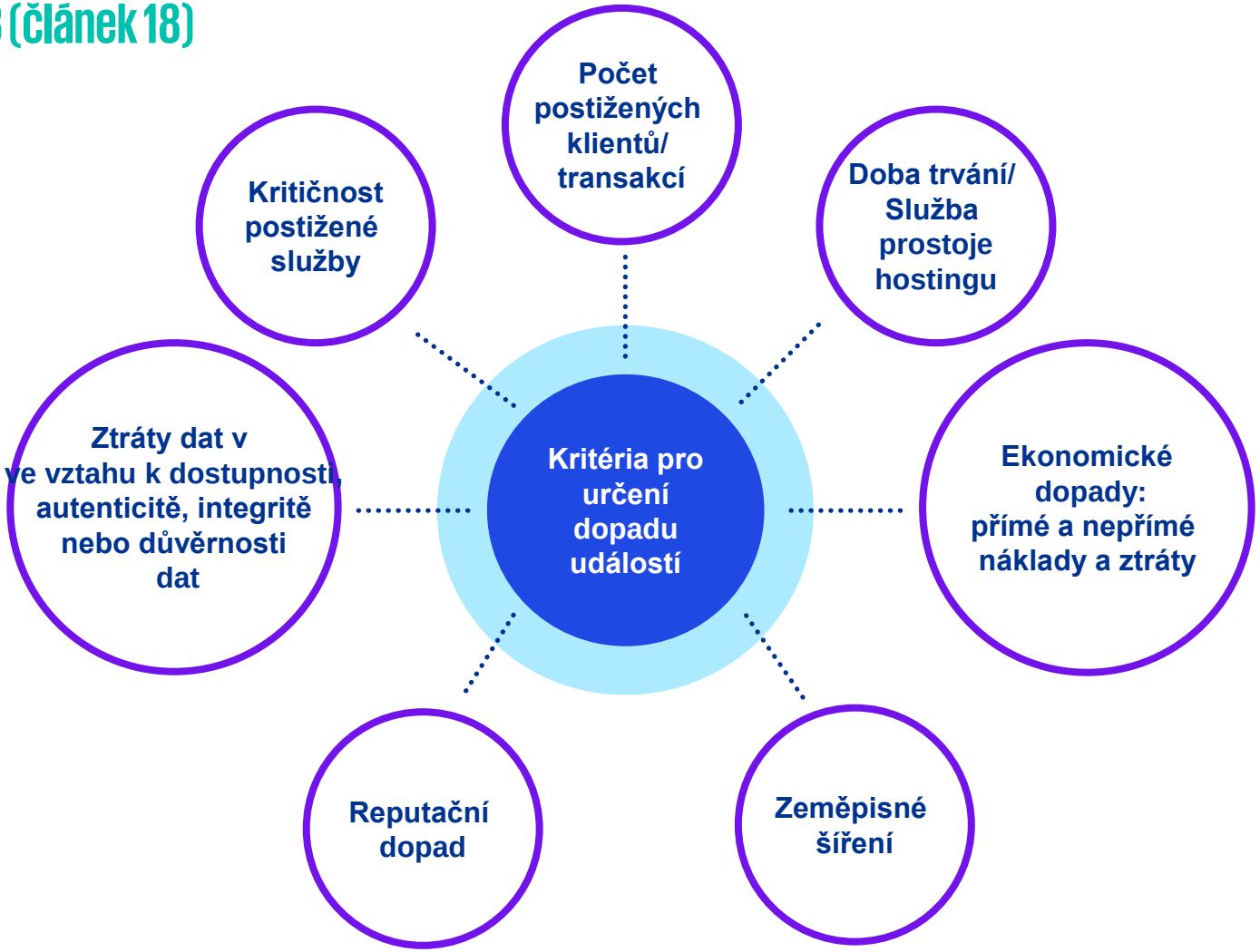
Hlášení závažných incidentů souvisejících s ICT řídicímu orgánu.

06

Zavedení postupů pro reakci na incidenty související s ICT s cílem zmírnit dopady.

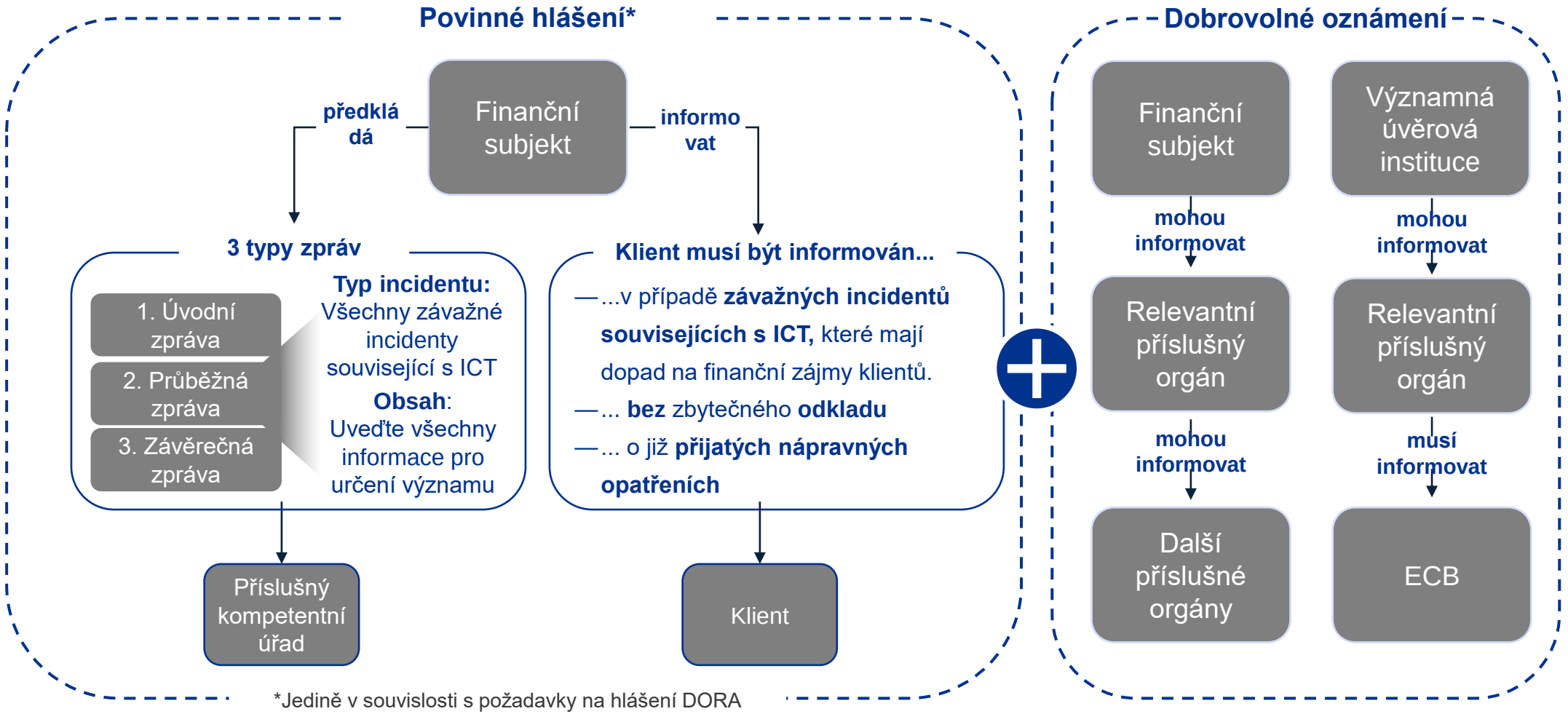
Incidenty související s ICT lze klasifikovat podle následujících kritérií

Podrobně kapitola 3 (článek 18)



Článek 19 objasňuje, jak a kdy se zprávy musí předkládat povinně a kdy jsou zprávy dobrovolné.

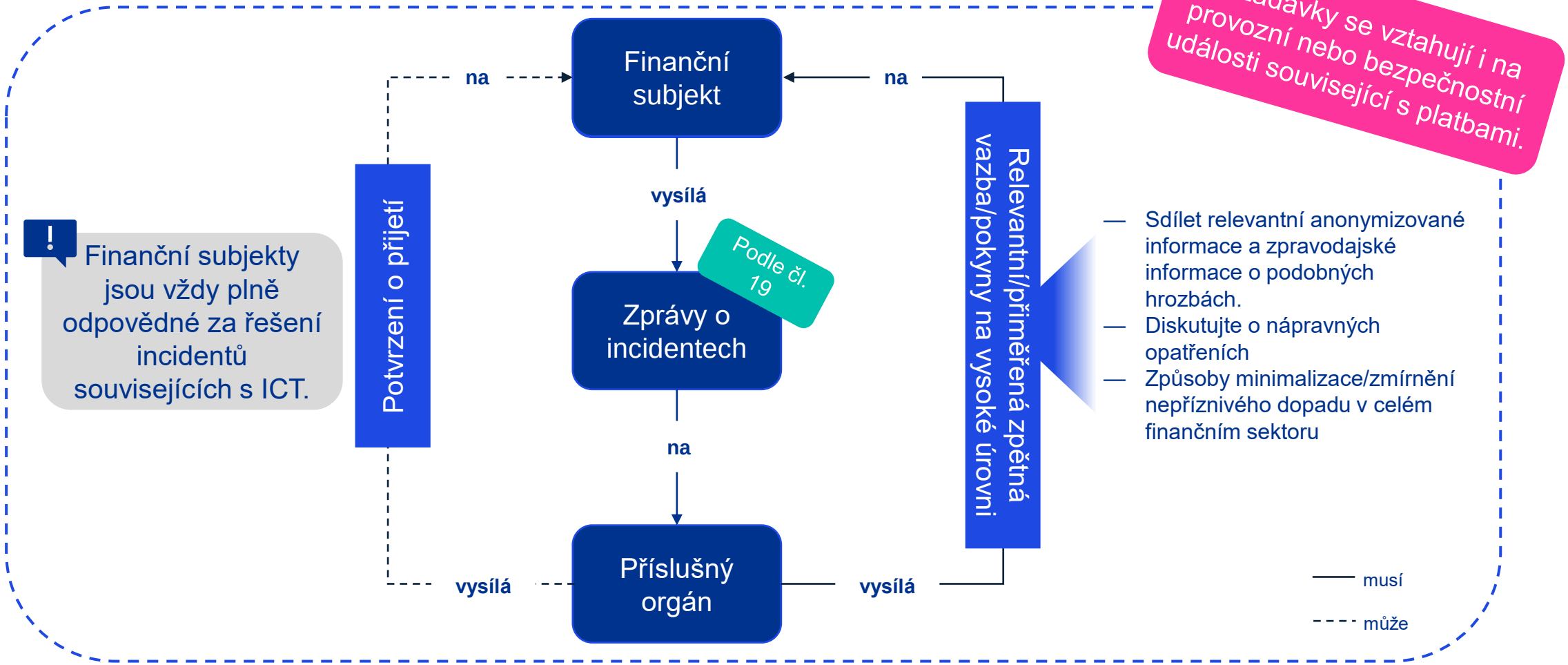
Podrobně kapitola 3 (článek 19)



*Jedině v souvislosti s požadavky na hlášení DORA

Po obdržení hlášení o incidentu souvisejícím s IKT poskytnou orgány finančním subjektům zpětnou vazbu a pokyny.

Podrobně kapitola 3 (článek 22 a 23)



Kapitola 4 obsahuje požadavky, nástroje a postupy, jak by mělo být prováděno testování provozní odolnosti digitálních technologií.

Testování digitální provozní odolnosti - přehled kapitola 4 (články 24-27)

Článek 24: Obecné požadavky na provádění testování digitální provozní odolnosti

Článek 25: Testování nástrojů a systémů IKT

Čl. 26: Pokročilé testování nástrojů, systémů a procesů IKT s využitím penetračního testování na základě hrozeb

Článek 27: Požadavky na subjekty provádějící penetrační testování na základě hrozeb

Požadavky na testování - nedílná součást rámce řízení rizik ICT

Podrobně kapitola 4 (článek 24 a 25)

Článek 24 - Obecné požadavky

- **Přiměřenost**: program musí odpovídat velikosti, profilu a rizikovosti společnosti (přístup založený na riziku).
- **Testování** všech kritických systémů a aplikací ICT alespoň jednou ročně.
- **Nezávislost:** finanční společnosti zajišťují, aby všechny testy prováděly nezávislé interní nebo externí strany.

Kapitola 4 se zabývá tím, jak se provádí pokročilé testování a jaké jsou požadavky na testery.

Podrobně kapitola 4 (článek 26 a 27)

Pokročilé testování nástrojů, systémů a procesů IKT na základě TLPT (článek 26)

Vztahuje se pouze na některé společnosti, které byly určeny příslušnými orgány.

Četnost rozšířených testů:
— Nejméně jednou za tři roky

Příslušné orgány:
— Identifikovat finanční subjekty, které jsou povinny provádět TLTP.

Po dokončení testování:
— Předkládají se zprávy a plány s nápravnými opatřeními

Testování:
— Příslušné procesy, systémy a technologie ICT na podporu kritických funkcí a služeb.
— V živých produkčních systémech
— Rozsah schválený orgánem

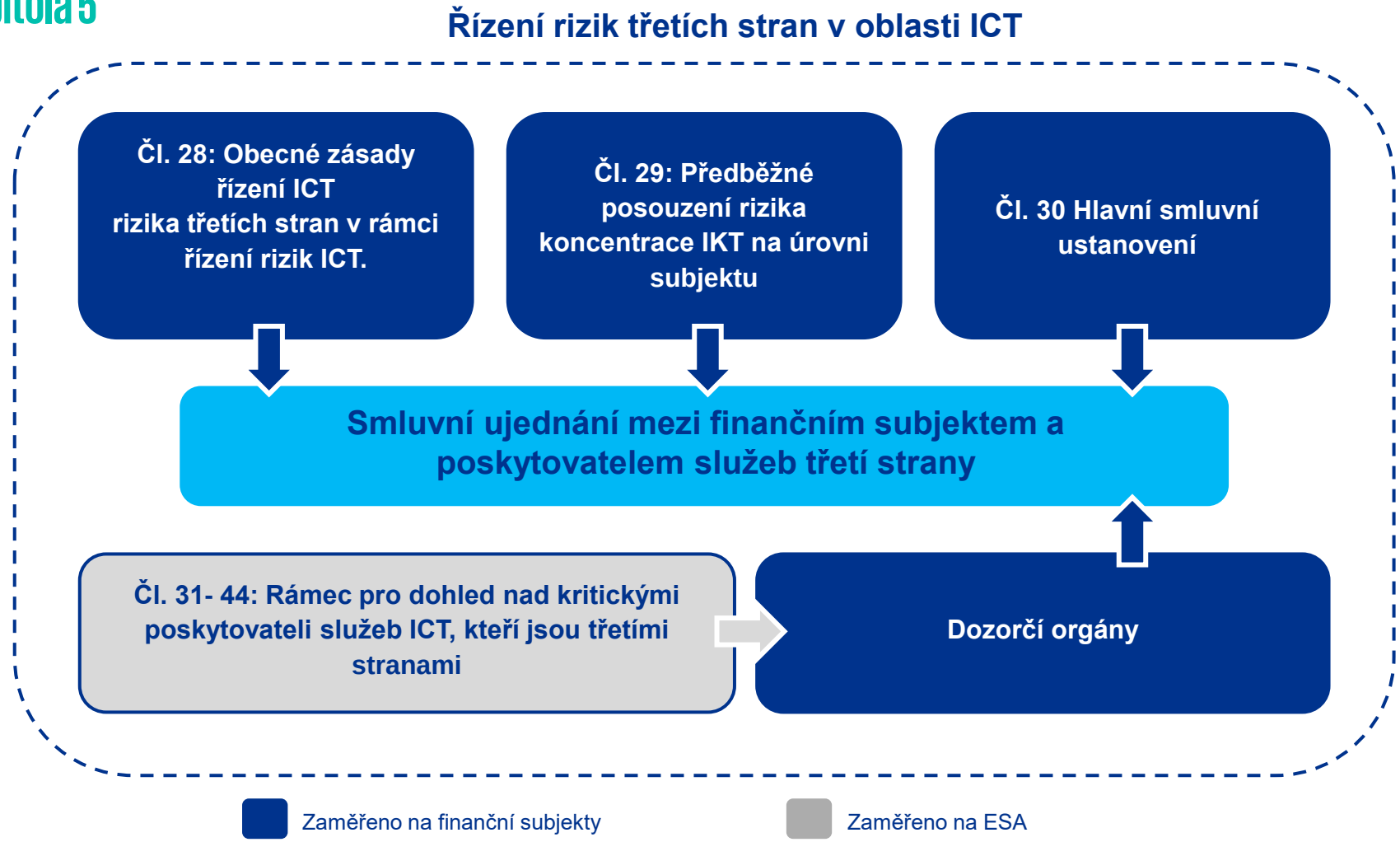
Požadavky na testery (článek 27):
— Vysoká vhodnost a pověst
— Krytí příslušným pojištěním odpovědnosti za škodu způsobenou při výkonu povolání
— Poskytnout nezávislé ujištění nebo auditní zprávu.

Při použití **interních testerů**:
— Použití bylo schváleno příslušným orgánem
— Poskytovatel zpravodajských informací o hrozbách je vůči finančnímu subjektu externí.

Základní funkce nebo služby delegované na třetí strany:
— U služeb třetích stran musí být provedeno pokročilé testování.

Kapitola 5 obsahuje nástroje a pokyny, jak řídit rizika ICT třetích stran.

Přehled kapitola 5



Článek 28 se týká obecných zásad, jak řídit rizika ICT třetích stran.

Podrobně kapitola 5 (článek 28)

— **Zajištění** komplexního **řízení rizik ICT ve vztahu k** poskytovatelům třetích stran.
— **kompletní sledování** rizik spojených s ICT třetích stran ve všech fázích vztahu.

Odpovědnost a ručení zůstává na finančním subjektu

Jaké jsou nejdůležitější aspekty procesu ICT pro třetí strany?

Klasifikace a analýza poskytovatele:
— Poskytované služby
— Podmínky monitorování
— posouzení vhodnosti
— Možné střety zájmů.

Včetně řídicího orgánu:
— Pravidelné podávání zpráv o rizicích

Záznam informací:
— Registr informací o smluvních ujednáních poskytovatelů služeb ICT

Proporcionalita: na základě
— Závislosti složitosti
— Typ a rozsah služby

Dodržování předpisů:
— Poskytovatel služeb třetí strany dodržuje standardy bezpečnosti informací

Riziková strategie:
— Přijmout a pravidelně revidovat strategii týkající se rizik třetích stran v oblasti ICT.

Aspekty, které je třeba mít na paměti před uzavřením smluvního ujednání o využívání služeb ICT

Podrobně kapitola 5 (článek 28)

Fáze spolupráce s externím poskytovatelem ICT služeb jsou rozděleny do tří fází. 1. Před uzavřením smlouvy 2. Aktivní smlouva 3. Po uzavření smlouvy

Aktivity

— Podpůrná funkce
— Podmínky dohledu
— Hodnocení rizik
— Náležitá péče
— Střety zájmů
— Určení četnosti auditů/oblastí

Smlouva Start

Ukončeno, pokud:

— Významné porušení zákonů
— Určité měnící se okolnosti (např. podstatná změna)
— Nedostatky v integritě, důvěrnosti
— Nespolehlivé a neefektivní služby

Smlouva Konec

Předpoklady, které musí poskytovatel ICT splnit

— Dodržování příslušného standardu zabezpečení informací
— Používání nejnovějších a nejkvalitnějších informačních standardů

Strategie odchodu musí být provedena bez

— Narušení obchodních činností
— Omezení dodržování právních předpisů
— Poškození kontinuity a kvality služeb poskytovaných klientům.

Důležité aspekty, které je třeba zahrnout do smlouvy při najímání služby ICT třetí strany

Podrobně kapitola 5 (článek 29 a 30)

Článek 29: Předběžné posouzení rizika koncentrace IKT na úrovni subjektu

Pokud jde o identifikaci rizik u služeb ICT podporujících **kritické nebo důležité funkce,** zvažte:

- Uzavření smlouvy s externím poskytovatelem služeb ICT, který **není snadno nahraditelný.**
- **více smluvních ujednání se** stejným externím poskytovatelem služeb ICT nebo s úzce propojenými externími poskytovateli služeb ICT.

Článek 30: Klíčová smluvní ustanovení

- Místa, kde mají být poskytovány funkce a služby ICT, kde mají být zpracovávány údaje, místo uložení.
- ustanovení o zajištění přístupu k datům, jejich obnovení a vrácení v případě ukončení smlouvy
- Úplný popis úrovně služeb včetně aktualizací a revizí
- Povinnost poskytnout pomoc v případě mimořádné události v oblasti IKT
- Účast externích poskytovatelů služeb ICT na programech zvyšování povědomí finančních subjektů o bezpečnosti ICT a na školeních o odolnosti digitálního provozu.
- Povinnost spolupracovat s orgány

služby ICT podporující kritické nebo důležité funkce:

- Právo sledovat poskytovatele, který je třetí stranou, a povinnost podávat zprávy a oznamovat.
- Strategie odchodu
- Kvantitativní a kvalitativní výkonnostní cíle
- Zavedení a testování pohotovostních plánů a zavedení bezpečnostních opatření ICT.
- Účastnit se penetračního testování finančního subjektu a plně s ním spolupracovat.

Sdílení informací je klíčem k minimalizaci šíření rizik

Podrobně kapitola 6 (článek 45)

Finanční subjekty jsou vyzývány k výměně informací s cílem zvýšit celkovou kybernetickou bezpečnost společností.

01 CÍL VÝMĚNY

Cíle výměny informací jsou:

— Zvyšování povědomí o rizicích v oblasti informačních a komunikačních technologií a minimalizace jejich šíření.
— Podpora obranných schopností a technik odhalování hrozeb

02 OHLAŠOVACÍ ORGÁNY

Oznámení příslušným orgánům:

— Potvrzení účasti na dohodách
— Začátek ukončení účasti

03 SMLOUVY

— Posílení digitální provozní odolnosti
— V rámci důvěryhodné komunity
— Zachování obchodního tajemství
— Ochrana osobních údajů
— Dodržování pokynů politiky hospodářské soutěže

04 TYP INFORMACÍ

— Informace o kybernetických hrozbách
— Ukazatele ohrožení
— Taktika, techniky a postupy
— Výstrahy a konfigurační nástroje kybernetické bezpečnosti

Zpráva o výkonu dohledu nad finančním trhem 2022 (cnb.cz)

Nařízení o digitální provozní odolnosti finančního sektoru (DORA) V prosinci 2022 bylo v Úředním věstníku uveřejněno nařízení (EU) 2022/2554 o digitální provozní odolnosti finančního sektoru (DORA). Nařízení přináší harmonizaci klíčových požadavků na provozní digitální odolnost pro většinu regulovaných subjektů finančního trhu. Jeho cílem je zvýšit výkonnost a stabilitu finančního systému a přispět k zajištění vysoké úrovně ochrany investorů a spotřebitelů v EU. Dohled nad dodržováním povinností stanovených tímto nařízením bude v českých podmínkách zajišťovat ČNB. Nařízení však zavádí i nový rámec dohledu, a to nad poskytovateli IKT služeb z řad třetích stran, které jsou pro subjekty finančního trhu kritickými poskytovateli IKT služeb. Vůči těmto poskytovatelům zakládá nařízení dohledové pravomoci evropských orgánů dohledu (EBA, EIOPA, ESMA). Spolu s nařízením DORA byla uveřejněna i směrnice (EU) 2022/2556, kterou se mění vybrané sektorové směrnice, pokud jde o digitální provozní odolnost finančního sektoru. Cílem této změnové směrnice je sjednotit a sladit současné požadavky na řízení rizik v oblasti IKT pro finanční sektor s nařízením DORA.

2022 Současně byly uveřejněny i směrnice (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS2) a směrnice (EU) 2022/2557 o odolnosti kritických subjektů (CER). Pokud jde o finanční subjekty, je nařízení DORA ve vztahu k oběma směrnicím považováno za odvětvový právní akt EU, přičemž ta ustanovení uvedených směrnic, která budou členskými státy uznána za rovnocenná ustanovením nařízení DORA, by se na finanční subjekty neměla uplatnit, aby se zabránilo zdvojování povinností a zbytečné zátěži subjektů.

ČNB a NÚKIB spojují síly při zvyšování kybernetické odolnosti finančního trhu - Česká národní banka (cnb.cz)

ČNB a NÚKIB spojují síly při zvyšování kybernetické odolnosti finančního trhu

Česká národní banka (ČNB) a Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) uzavřeli 31. května 2022 Memorandum o vzájemné spolupráci. Jde o vyústění dosavadní spolupráce obou dohledových orgánů a odraz dynamického rozvoje využívání informačních technologií, urychleného mimo jiné pandemií covid-19.
V současném světě roste bezprecedentním způsobem závislost na digitálních službách, které často nemají svou původní alternativu. Kromě řady příležitostí a přínosů pro uživatele těchto služeb to však zároveň představuje obrovskou výzvu v podobě zvládání pokračujícího transferu rizik do kybernetického prostoru. Dnes jsou tato rizika navíc významně posilována v důsledku eskalace napětí na Ukrajině i v dalších částech světa a hrají tak významnou roli rovněž z hlediska tak zvaných hybridních hrozeb. Odolnost proti těmto rizikům je klíčová zejména pro kritická odvětví jako doprava, energetika či zdravotnictví a v neposlední řadě pro sektor finančních služeb. Zajištění kybernetické odolnosti finančního (zejména bankovního) sektoru je přitom pro společnost nezbytným předpokladem pro zvládání všech těchto hrozeb.

ČNB, která vykonává dohled v oblasti řízení rizik IS/IT v bankách již od roku 2002, proto velmi uvítala vznik národní instituce zaměřené na kybernetickou a informační bezpečnost. Spolupráce obou institucí začala již v době vzniku NÚKIB, tedy v roce 2017. Uzavřené Memorandum je tedy potvrzením přínosné dosavadní spolupráce a kvalitním formálním rámcem pro další pokračování společného působení na podporu **kybernetické odolnosti finančního sektoru ČR**.

ČNB i NÚKIB spojuje společná oblast působnosti. Jedná se o **kybernetickou bezpečnost v nejdůležitější části finančního sektoru**. V první etapě se spolupráce zaměřila na koordinaci regulatorních požadavků a na metodické sladění přístupů, očekávání a požadavků kladených na společně dohlížené finanční instituce. Od počátku se odborníci na kybernetickou bezpečnost z obou dohledových orgánů setkávali na pracovních diskusích, jejichž smyslem bylo nalézt co nejefektivnější cestu společného působení směřujícího k podpoře kybernetické odolnosti bank.
Vyústěním této spolupráce je například **zavedení testů kybernetické odolnosti do dohledové praxe ČNB,** ke kterému došlo v roce 2020. Na rozdíl od penetračních testů je jejich cílem prověřit schopnost a úroveň komplexní reakce banky na kybernetický útok. Nezaměřují se „pouze“ na klíčové IT činnosti k odražení útočníka, ale také na další aktivity nezbytné ke zmírňování dopadů, včetně těch reputačních. Při tvorbě metodiky testů kybernetické odolnosti ČNB využila zkušenosti odborníků z NÚKIB s organizací podobných cvičení simulujících různé vektory útoků a jejich důsledky.
V roce 2021 se spolupráce obou dohledových autorit prohloubila **uskutečněním první společné kontroly,** která prakticky ověřila jednotnost přístupů obou institucí k jednotlivým detailům kybernetické bezpečnosti přímo v konkrétních posuzovaných případech.

Výše uvedené společné aktivity se staly důležitým východiskem nového Memoranda a daly mu věcný základ. Memorandum však nezohledňuje pouze dosavadní spolupráci, ale je zároveň koncipováno jako účelný rámec pro zvládnutí výzev plynoucích mimo jiné z připravované nové evropské regulace v oblasti kybernetické bezpečnosti a odolnosti. Konkrétně půjde o implementaci **směrnice NIS2 (Network and Information Security) a nařízení DORA (Digital Operational Resilience Act).** Tato nová evropská legislativa klade především důraz na řešení kybernetických rizik u nejdůležitějších IT dodavatelů finančního sektoru v EU nebo na zavedení rámce pro testování kybernetické odolnosti napříč EU.
Kromě těchto koncepčních témat však bude třeba i nadále reagovat na hrozby související s pokračujícím trendem útoků cílených na uživatele elektronických kanálů bank. Proto budou ČNB a NÚKIB pokračovat ve spolupráci na **zvyšování povědomí veřejnosti o kybernetických rizicích**. Hlavním smyslem těchto aktivit je podpora úsilí samotných bank při zvyšování znalostí klientů o rizicích souvisejících s využíváním distribučních elektronických kanálů. Bez dostatečné obezřetnosti klientů totiž není možné zajistit účinnou obranu před případy digitálních krádeží finančních prostředků nebo dat.

Spolupráce přináší výhody pro obě instituce zejména ve zrychlení toku informací. V oblasti kybernetické bezpečnosti je klíčové mít aktuální znalosti o hrozbách a ještě lépe o konkrétních aktivitách útočníků v kybernetickém prostoru. Pokud se v nějaké organizaci podaří pachatelům prolomit do informačních systémů, je nutné zavedení okamžitých opatření také ve zbývajících institucích k zamezení dalšího potenciálního napadení. **Sdílení důležitých informací je proto považováno za jeden ze základních pilířů obrany proti kybernetickým útokům**.
Zajišťování odolnosti proti kybernetickým hrozbám je nikdy nekončící proces. V dalším období tak ČNB i NÚKIB čekají náročné výzvy jak v oblasti implementace nové regulace, tak v dohledu. **Spojenectví** je výhodou, jak tyto úkoly lépe naplnit, ale také **hodnotou, kterou je třeba dále pěstovat**. ČNB si velmi cení úzké funkční spolupráce s NÚKIB a hodlá ji do budoucna dále rozvíjet.

Tomáš Kudělka – KPMG NIS 2 a DORA garant

Tomáš Kudělka

Director

Tel.: +420 724 244 944

Email: tkudelka@kpmg.cz

Tomáš pracuje již 25 let v IT a IT bezpečnosti. Svou kariéru zahájil v KPMG v oddělení Risk Managementu. Zaměřoval se především na informační bezpečnost – procesní i řídící frameworky (ISO 27001, COBIT, ITIL, PCI DSS) a technické zabezpečení (penetrační testy, configuration review, apod.). Později byl také zodpovědný za projekty v oblasti řízení IT a projekty v oblasti návrhu IT architektur. Po prvních 10-ti letech práce v oblasti poradenství pro KPMG přešel do IT provozu. Nejdříve vystavěl a jako výkonný ředitel řídil globální provozní centrum pro mezinárodní IT společnost Diebold Nixdorf. Následně 3 roky pracoval jako CTO pro mezinárodního systémového integrátora, společnost Simac Technik.
V roce 2019 se do KPMG vrátil a v současné době pracuje jako Director v Technology týmu.

Oblasti NIS 2 se v odborných kruzích aktivně věnuje. Vystupuje často na konferencích a v odborných diskusích, například:

- Kulatý stůl na téma NIS 2 se zástupci NÚKIB: Cyberblog kulatý stůl: NIS 2 – co přináší nová evropská směrnice zaměřená na standardizaci v oblasti kybernetické bezpečnosti? – Cyberblog
- O2 CyberCast: O2 CyberCast #5 s Tomášem Kudělkou z KPMG: Nová bezpečnostní směrnice NIS 2 se bude týkat mnohem více společností než jednička. - O2
- Konference IT governance 2022: Program XVIII. konference IT Governance 2022 | ISACA CRC
- Konference Směrnice NIS 2: Procesy a technologie: Virtuální konference "Směrnice NIS 2: Procesy a technologie" - NIS2.tech

A publikoval řadu článků na téma NIS 2 v oborných periodikách, například:

- NIS2 bude srovnatelná s GDPR – Týdeník Euro (tydenikeuro.cz)
- Na tisíce firem dopadne nová administrativa. Některé může přijít až na stovky milionů | Hospodářské noviny (HN.cz)
- Evropa proti kyberzločinu. Nová direktiva o IT bezpečnosti ovlivní tisíce firem | Týdeník pro ekonomiku, politiku a byznys (tydenikhrot.cz)
- NIS2 zpřísní nároky na kyberbezpečnost firem i státu (systemonline.cz)