Čo očakávať od regulácie digitálnej prevádzkovej odolnosti DORA?

NÁRODNÁ BANKA SLOVENSKA
EUROSYSTÉM

Alexandra Urbánová Csajková

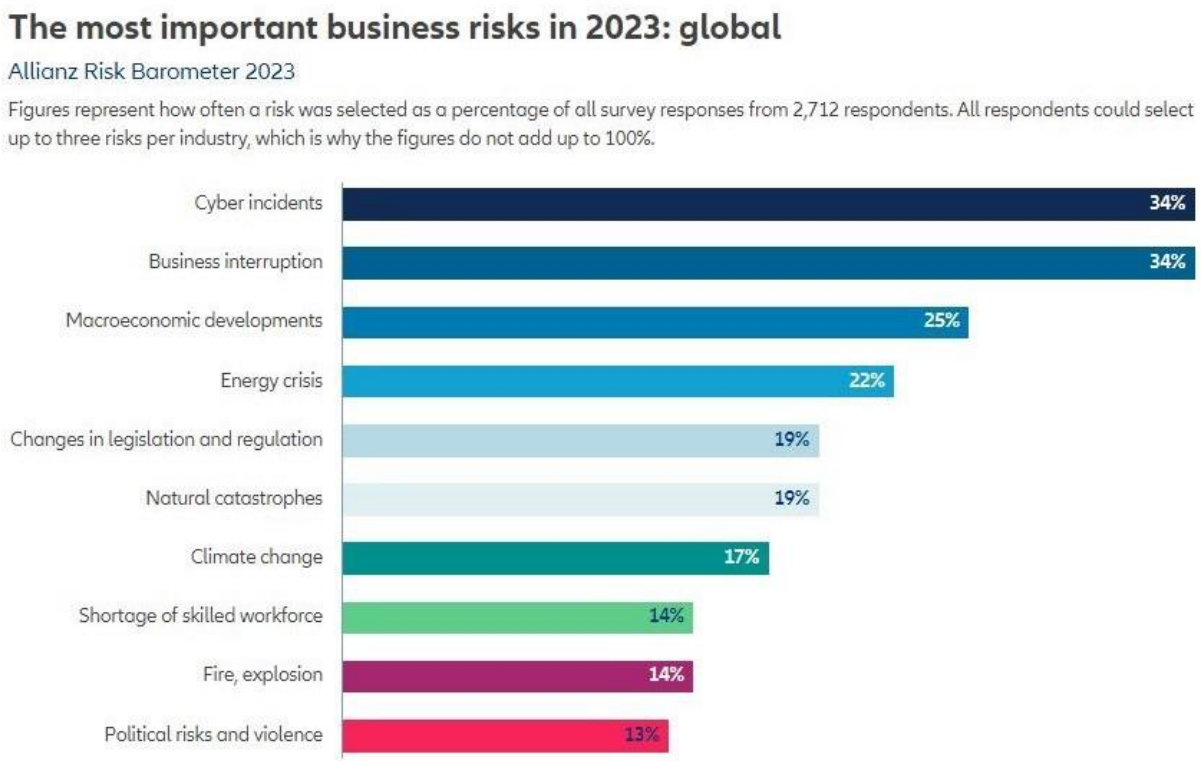
03.10.2023

Agenda

- Motivácia
- Nariadenie DORA
- Prehľad RTS/ITS
- Pripravenosť slovenského finančného sektora
- Ďalšie kroky

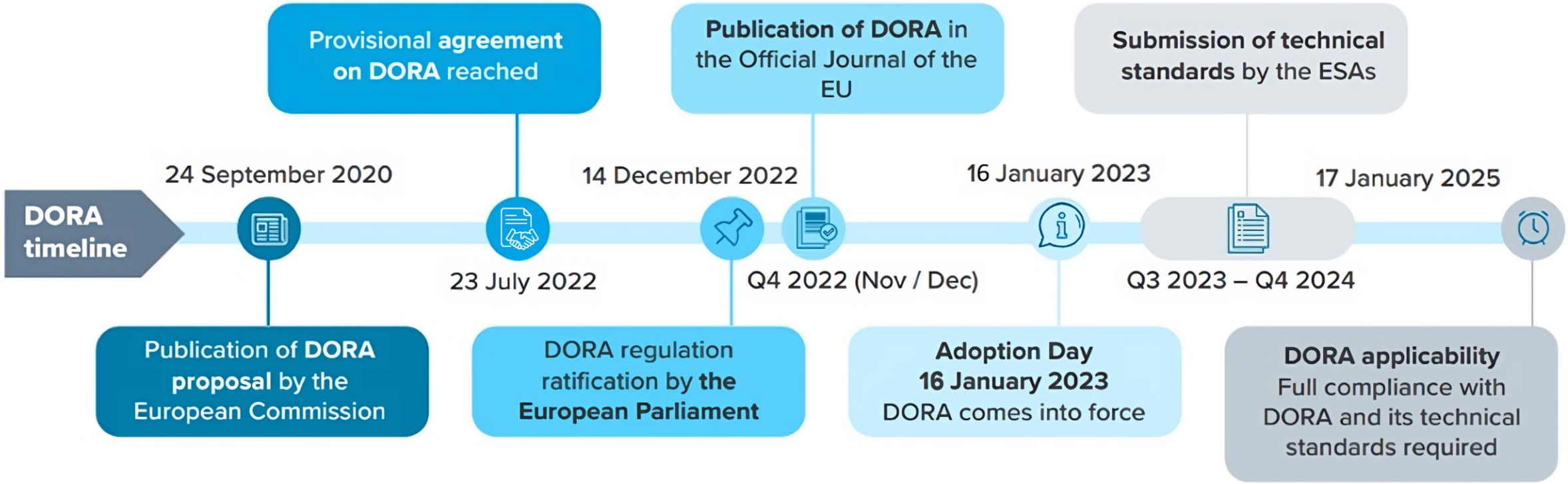
Motivácia

Kybernetické incidenty, ako sú úniky dát, ransomvérové a malvérové útoky alebo narušenia v oblasti IKT, sa stali už druhý rok po sebe celosvetovo **najvýznamnejším rizikom**.



Nariadenie DORA

Kde sa nachádzame?



Všeobecný prehľad

- **nariadenie** Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora
- uplatňuje sa od **17.1.2025**
- harmonizácia pravidiel pre riadenie IKT rizík
- **presun pozornosti od finančného zdravia subjektov na ich udržateľnú prevádzku aj v prípade, ak dôjde ku kritickému narušeniu fungovania IKT**
- oblasti DORA: (i) riadenie IKT rizika
  (ii) riadenie, klasifikácia a nahlasovanie incidentov súvisiacich s IKT
  (iii) testovanie digitálnej prevádzkovej odolnosti
  (iv) riadenie rizika IKT tretích strán
  (v) zdieľanie informácií

Pôsobnosť

- uplatňuje sa na **takmer všetky typy dohliadaných subjektov a tretie strany**

ALE

Výnimky:

- princíp proporcionality: veľkosť a celkový rizikový profil, ako aj povaha, rozsah a zložitosť služieb, činností a operácií.
- finančné subjekty iné než mikropodniky ...
- ... alebo „inak" v prípade mikropodnikov
- zjednodušený rámec riadenia IKT rizika
- testovanie vs. mikropodniky
- nie mikro, nie zjednodušený rámec: pokročilé testovanie, stratégia riadenia rizika IKT tretích strán

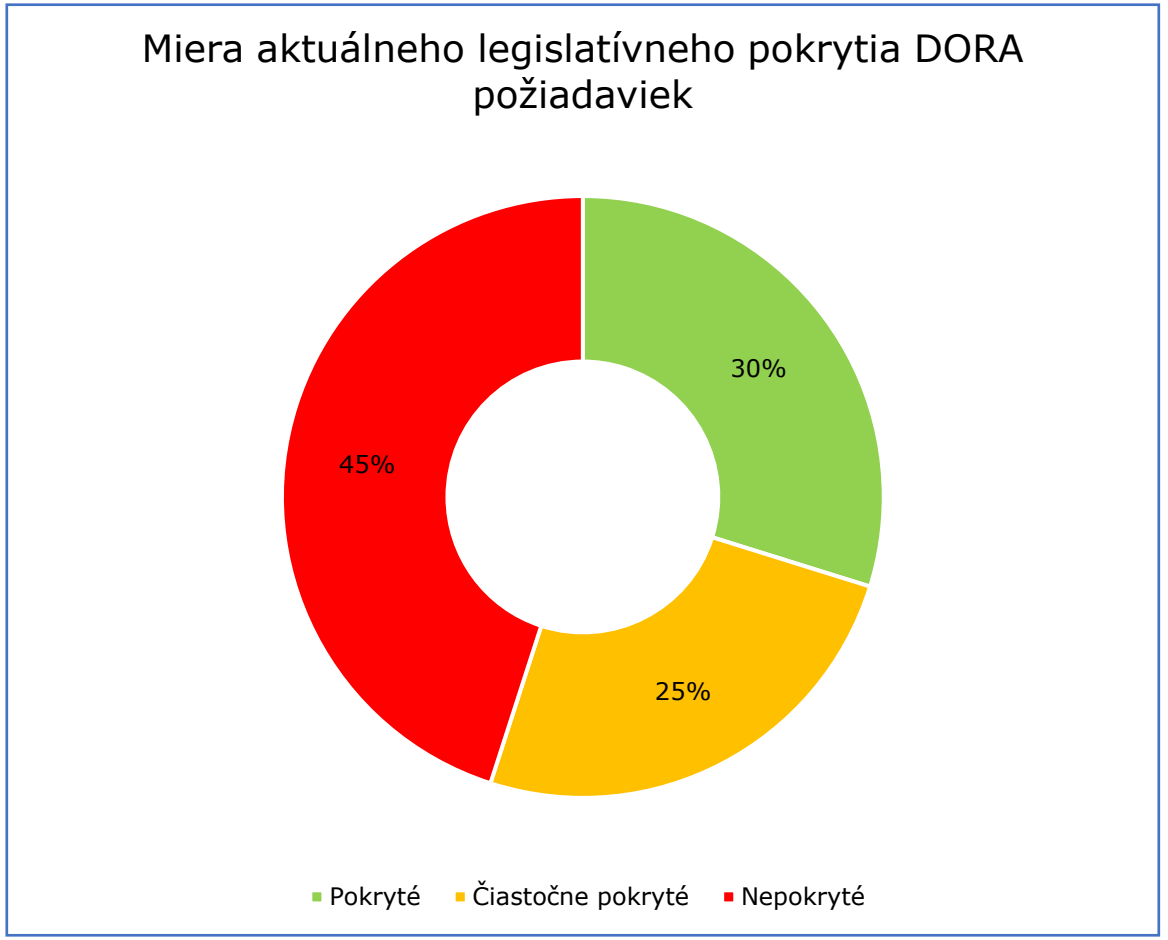
DORA scope	NOT	chapter II, chapter III, IV, V Section 1 proporcionalita	financial entities other than microenterprises	or ... microenterprises	Simplified ICT risk management	microenterprise testing	advanced testing	strategy on ICT third party risk	oversight
a) úverové inštitúcie;	post office giro Art. 2(5) point.3 2013/36/EU	size, risk profile, nature, scale, complexity, services, acitivites, operations	Art. 5(3) Art. 6(4) Art. 6(6) Art. 8(3) Art. 8(7) Art. 11(3) Art. 11 (6-7) Art. 11(10) Art. 12(4) Art. 13(2) Art. 13(7) Art. 24(1) Art. 24(3-6) Art. 26(1)	Art. 6(5)	small non-interconnected exempted 2013/36/EU	Art. 25(3)	Art. 26(1) non micro non simplified	Art. 28(2) non micro non simplified	critical for financial entities not a financial entity not an intra-group service
b) platobné inštitúcie vrátane platobných inštitúcií vyňatých podľa smernice (EÚ) 2015/2366;					small non-interconnected payment institutions exempted				
c) poskytovatelia služieb informovania o účte;									
d) inštitúcie elektronických peňazí vrátane inštitúcií elektronických peňazí vyňatých podľa článku 9 ods. 1 smernice 2009/110/ES;					small non-interconnected electronic money institutions exempted				
e) investičné spoločnosti;	natural or legal person Art. 2, 3 2014/65/EU post office giro Art. 2(5) point.3 2013/36/EU				small non-interconnected investment firms				
f) poskytovatelia služieb kryptoaktív, ktorým bolo udelené povolenie podľa nariadenia Európskeho parlamentu a Rady (EÚ) .../... a emitenti tokenov krytých aktívami;									
g) centrálne depozitáre cenných papierov									
h) centrálne protistrany;									
i) obchodné miesta;	natural or legal person Art. 2, 3 2014/65/EU								
j) archívy obchodných údajov;									
k) správcovia alternatívnych investičných fondov;	Art. 3(2) 2011/61/EU								
l) správcovské spoločnosti;									
m) poskytovatelia služieb vykazovania údajov;									
n) poisťovne a zaisťovne;	Art. 4 2009/138/EC								
o) sprostredkovatelia poistenia, sprostredkovatelia zaistenia a sprostredkovatelia doplnkového poistenia;	micro, small or medium size								
p) inštitúcie zamestnaneckého dôchodkového zabezpečenia;	do not have more than 15 members				small occupational retirement				
q) ratingové agentúry;									
r) správcovia kritických referenčných hodnôt;									
s) poskytovatelia služieb hromadného financovania;									
t) archívy sekuritizačných údajov;									
u) externí poskytovatelia služieb IKT									

Zdroj: NBS

Každý finančný subjekt by mal byť primerane odolný v digitálnom svete.

Ďalšie legislatívne aspekty

- DORA je nariadenie
- DORA rieši digitálnu prevádzkovú odolnosť
- DORA je lex specialis k NIS2 smernici
- DORA rieši aj PSD2 incidenty
- DORA požiadavky sú bohatšie ako existujúce ustanovenia o digitálnej prevádzkovej odolnosti L1, L2 a L3 regulácie v jednotlivých sektoroch
- AI act, FIDA, GDPR, CER, Data act, ...



Zdroj: NBS

Prehľad RTS/ITS

RTSs, ITSs a usmernenia

	DORA policy work	Article	Public consultation	Finalise
	Call for advice on criticality criteria and fees	31.8 | 43.2	26 May - 23 June 23	30 Sept 2023
FIRST BATCH	RTS on ICT risk management framework	15		
	RTS on simplified ICT risk management framework	16		
	RTS on criteria for the classification of ICT-related incidents	18.3	19 June - 11 Sept 23	17 Jan 2024
	ITS to establish the templates for the Register of information	28.9		
	RTS to specify the policy on ICT services performed by 3rd party	28.1		
SECOND BATCH	RTS on specifying the reporting of major ICT-related incidents	20.a		
	ITS to establish the reporting details for major ICT-related incidents	20.b		
	Guidelines on the estimation of aggregated costs/losses caused by major ICTrelated incidents	11.11		
	RTS to specify threat led penetration testing aspects	26.11	Nov/Dec 23 - TBC	17 July 2024
	RTS to specify elements when sub-contracting critical or important functions	30.5		
	GL on cooperation between ESAs and CAs regarding the structure of the oversight	32.7		
	RTS to specify information on oversight conduct	41		
	Feasibility report on single EU Hub for major ICT-related events	21	TBC	17 January 2025

Zdroj: Prezentácia Joint ESAs public hearing on the first batch of DORA policy products

Riadenie IKT rizika

Rámec riadenia IKT rizika 1/2

- spôsob **riadenia IKT rizika** a zvyšovania **digitálnej prevádzkovej odolnosti**
- sumarizácia riadenia IKT rizika sa premieta do **správy**, ktorá sa predkladá NBS na žiadosť
- jednotlivé časti tejto správy kopírujú požiadavky DORA a napĺňajú sa obsahom, čo finančný subjekt robí pre digitálnu prevádzkovú odolnosť
- prechádza celým **životným cyklom IKT aktív** (evidencia, testovanie, zabezpečenie nepretržitého fungovania, ...) a rieši aj ďalšie náležitosti (roly, zodpovednosti, reporting, informovanie, školenia, ...)
- RTS zavádza harmonizáciu nástrojov, metód, procesov a politík riadenia rizík IKT
  - technologicky neutrálne
  - cross sektorovo
  - proporcionálne

Rámec riadenia IKT rizika 2/2

- **bezpečnostné politiky, postupy, protokoly a nástroje IKT**
  - ustanovenia o riadení
  - správa IKT aktív
  - šifrovanie a kryptografia
  - bezpečnosť prevádzky IKT
  - zabezpečenie siete
  - projektové riadenie IKT a riadenie zmeny IKT
- politika **ľudských zdrojov a kontrola prístupu**
- **detekcia a reakcia na incidenty** súvisiace s IKT
- IKT **business continuity management**
- zjednodušený rámec riadenia IKT rizík
  - len pre vybrané subjekty (napr. malé inštitúcie dôchodkového zabezpečenia)
  - nižšia miera podrobnosti kladených požiadaviek vo všetkých oblastiach

Správa o rámci riadenia rizík IKT

- prehľad **hlavných zmien a vylepšení** rámca riadenia rizík IKT od posledného preskúmania
- zhrnutie **zistení** a sebahodnotenie závažnosti **slabých stránok, nedostatkov** a medzier v rámci riadenia rizík IKT počas sledovaného obdobia vrátane podrobnej analýzy
- **opatrenia** určené na riešenie všetkých zistení a nedostatkov
- **výhľad** a plánovaný ďalší vývoj
- informácie o **predchádzajúcej kontrole**
- **zdroje informácií** použité pri príprave správy a preskúmania (výsledky z interného auditu, výsledky compliance, výsledky testovania digitálnej prevádzkovej odolnosti a pokročilého testovania nástrojov, systémov a procesov IKT založených na TLPT, atď.)

Riadenie, klasifikácia a nahlasovanie incidentov súvisiacich s IKT

IKT incidenty – klasifikácia

- => konzistentný one-size-fits-all prístup pre všetky subjekty bez sektorových špecifík

Subjekt klasifikuje incident ako závažný, ak sú splnené aspoň 2 primárne klasifikačné kritériá alebo 1 primárne kritérium a 2 sekundárne klasifikačné kritériá

Primárne kritérium	Prahové hodnoty – platí ALEBO
Dotknutí klienti, finančné protistrany, transakcie	• 10% klientov alebo 50 000 klientov • 10% protistrán • 10% transakcií alebo objem transakcií 15 000 000 EUR • vplyv na relevantných klientov alebo protistrany
Straty údajov	• významný vplyv na kritické údaje v súvislosti s ich dostupnosťou, pravosťou, integritou alebo dôvernosťou
Dotknuté kritické služby	• vplyv na kritické služby eskalovaný riadiacemu orgánu

IKT incidenty – klasifikácia

Sekundárne kritérium	Prahové hodnoty – platí ALEBO
Vplyv na reputáciu	• pozornosť médií • sťažnosti od klientov alebo protistrán • neplnenie regulačných požiadaviek • strata klientov alebo protistrán
Trvanie incidentu a výpadok služby	• 24h trvanie incidentu • 2h výpadok služieb pre kritické funkcie
Geografické rozloženie	• vplyv na klientov, protistrany, pobočky, trhové infraštruktúry, tretie strany aspoň v 2 členských štátoch
Hospodársky vplyv	• priame a nepriame náklady a straty nad 100 000€

- **opakujúce sa incidenty** sa posudzujú kumulatívne za obdobie 3 mesiacov
- detaily závažného incidentu NBS reportuje ďalším relevantným autoritám bez anonymizácie
- **významná kybernetická hrozba** je taká, ktorá by mohla mať vplyv na kritické a dôležité funkcie, má vysokú pravdepodobnosť materializovať sa a mohla by splniť podmienky závažného incidentu

IKT incidenty – obsah, lehoty

- oznamovanie závažných IKT incidentov
- **počiatočné oznámenie** – do 4 hodín od klasifikácie ako závažný, najneskôr **24h** od detekcie
- **priebežná správa** – po obnovení činností, najneskôr **72h** od klasifikácie incidentu ako závažného alebo predloženia počiatočného oznámenia (podľa toho, čo nastane skôr)
- **záverečná správa** – najneskôr **1 mesiac** od klasifikácie incidentu ako závažného alebo predloženia počiatočného oznámenia (podľa toho, čo nastane skôr)
- obsah oznámení a správ
  - závažných IKT incidentov
    - o subjekte - typ subjektu, reportujúci a ovplyvnený subjekt, kontakt, typ správy, ...
    - o incidente – podľa typu správy
  - významných kybernetických hrozieb
- outsourcing oznamovania a zasielania správ na tretiu stranu – zodpovednosť zostáva na finančnom subjekte

Testovanie digitálnej prevádzkovej odolnosti

Threat-Led Penetration Testing

- **riadený pokus o narušenie kybernetickej odolnosti** subjektu simulovaním taktík, techník a postupov aktérov reálnych hrozieb
- frekvencia výkonu testov **jedenkrát za 3 roky**
- väčšinou vykonávaný **externými subjektami** špecializujúcimi sa na takúto činnosť
- výkon a rozsah testu pozná iba vedenie subjektu a TLPT autorita
- dĺžka testu najmenej 12 týždňov (nezahŕňa predprípravu a vypracovanie výsledkov)
- výkon testu **na produkčných systémoch** subjektu
- výsledok nie je vyhovel/nevyhovel, ale **zistiť slabé stránky a poučiť sa z nich**
- koho sa to napr. bude týkať:
  - globálne systémovo významné inštitúcie (G-SII) alebo iné systémovo významné inštitúcie (O-SII)
  - platobné inštitúcie a inštitúcie elektronických peňazí s hodnotou platobných transakcií nad 250 mld EUR
  - Centrálny depozitár cenných papierov, Burza cenných papierov
  - poisťovne a zaisťovne s viac ako 10% trhovým podielom na národnom trhu
  - **ale aj iné subjekty**
- subjekty mimo rozsahu vyššie budú mať povinnosť vykonávať klasické penetračné testovanie

Riadenie rizika IKT tretích strán

Politika pre zmluvné dojednania

- RTS určuje politiku pre zmluvné dojednania s tretími stranami o využívaní IKT služieb **podporujúcich kritické alebo dôležité funkcie** finančného subjektu
- stratégia pre riziko IKT tretích strán je súčasťou rámca riadenia IKT rizík
- zahŕňa **externých aj vnútroskupinových** poskytovateľov
- definuje základné súčasti nastavenia riadenia rizík a rámca internej kontroly, ktorého neoddeliteľnou súčasťou sú napr.:
  - ex-ante hodnotenie rizík
  - due dilligence
  - konflikt záujmov
  - monitoring zmluvných dojednaní
  - ukončenie zmluvných dojednaní
- revízia najmenej 1x ročne

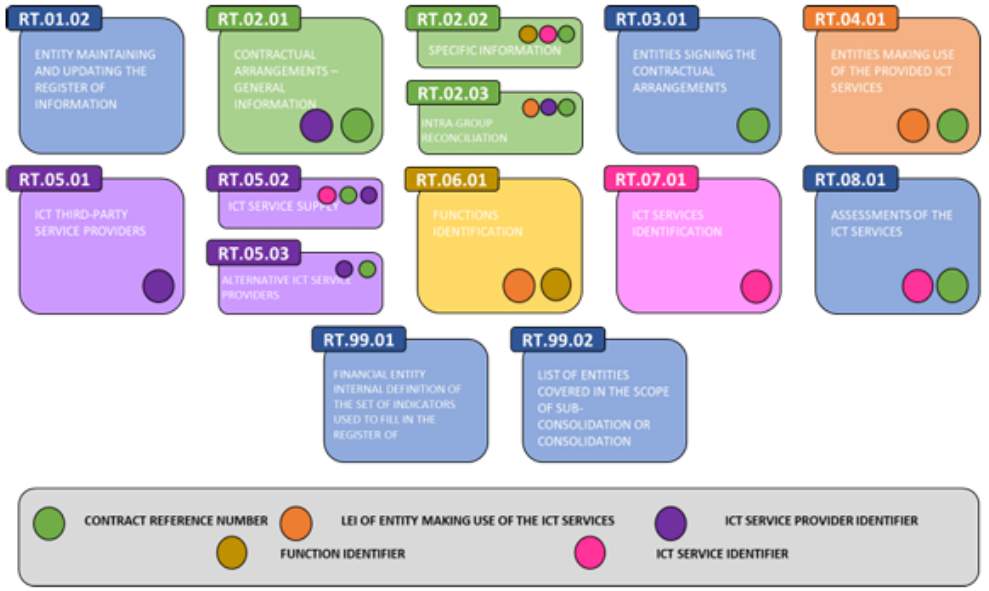
Politika pre zmluvné dojednania

- proporcionalita
- metodika určenia IKT služieb podporujúcich kritické alebo dôležité funkcie
- proces výberu a posúdenia budúcich poskytovateľov IKT služieb
- opatrenia na identifikáciu, prevenciu a riadenie vzniknutých alebo potenciálnych konfliktov záujmov
- požiadavky na písomné zmluvné dojednania
- opatrenia v prípade nedostatkov zo strany IKT tretích strán
- pravidelné revidovanie a testovanie exit plánu pre každú IKT tretiu stranu

Register informácií

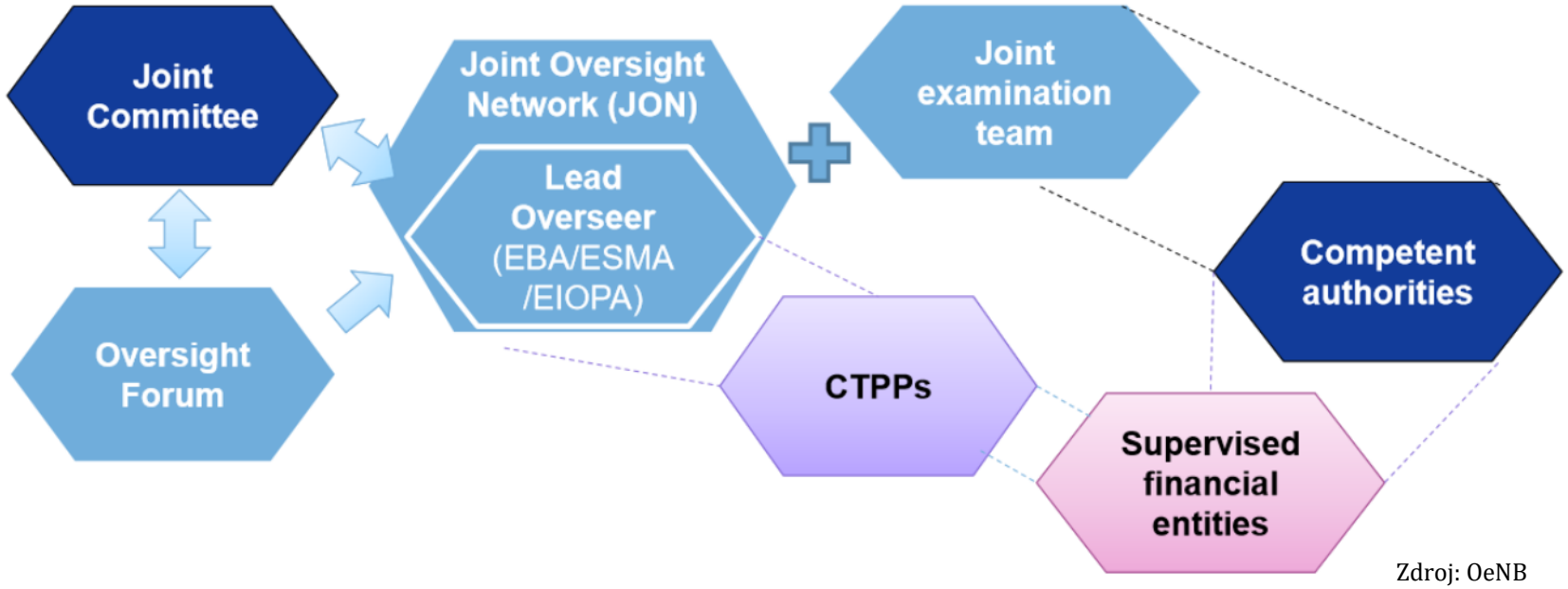
- register informácií má na priebežnej báze zachytávať informácie týkajúce sa **zmluvných dojednaní o využívaní IKT služieb** uzavretých s tretími stranami
- **dva súbory vzorov -** úroveň subjektu (10) a subkonsolidovaná a konsolidovaná úroveň (14) vzájomne previazaných tabuliek
- konkrétne atribúty a validácie
- LEI kód je primárny identifikátor subjektu
- priame zmluvy, plánované zmluvy, ukončené zmluvy
- podklad pre vyhodnotenie kritickosti IKT tretích strán za účelom oversight aktivít

Illustration 2: Structure of the register of information at (sub)consolidated level



Zdroj: Discussion paper k ITS

Štruktúra oversight



Zdroj: OeNB

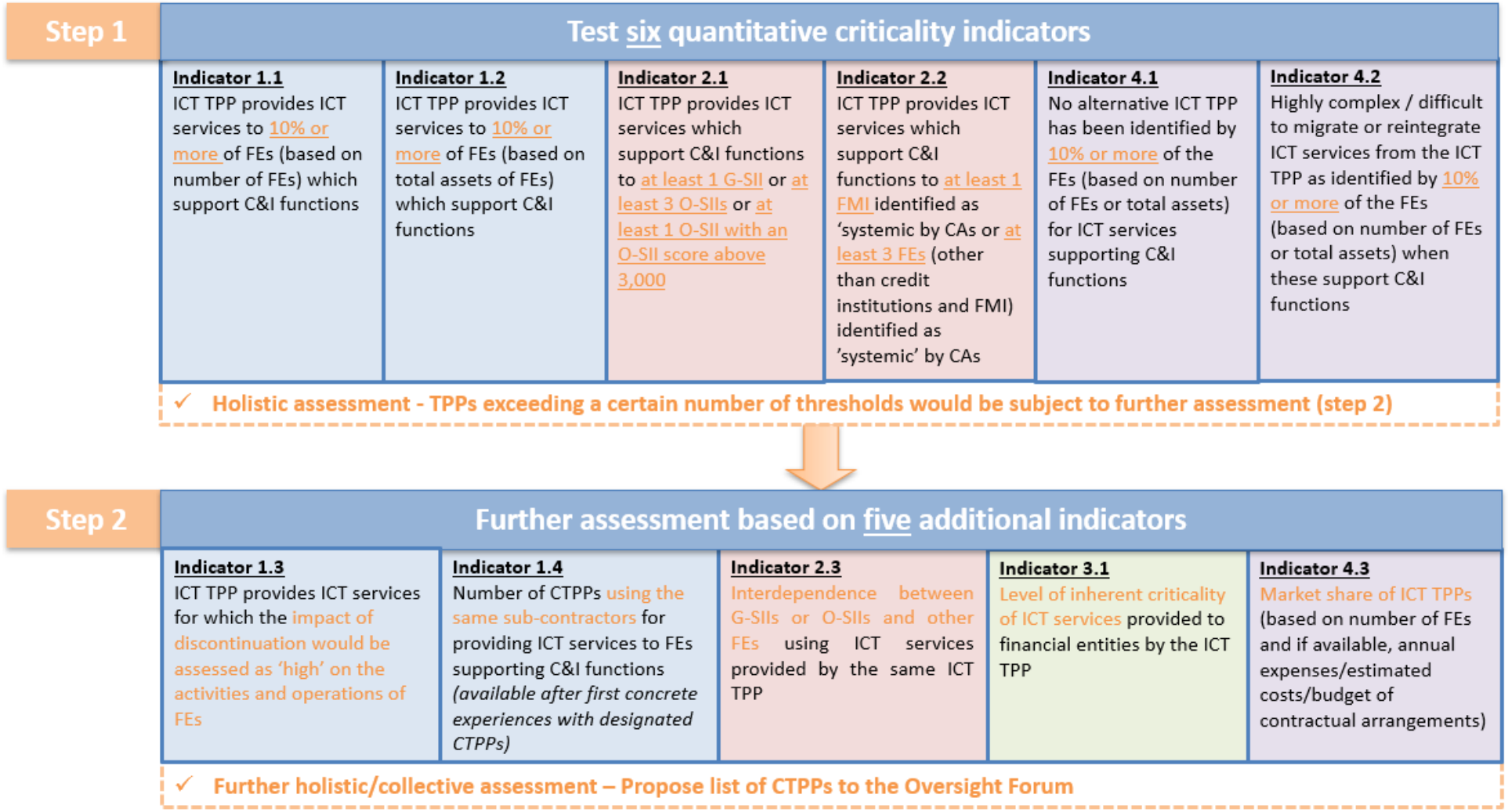
- ročný cyklus: určovanie kritických IKT tretích strán na základe kvalitatívnych a kvantitatívnych kritérií a posúdenie dobrovoľných žiadostí, menovanie Lead Overseera pre každú kritickú IKT tretiu stranu, individuálny oversight plán, priebežný oversight, odporúčania a follow-up
- na pokrytie priamych a nepriamych nákladov na oversight aktivity (ESAs aj CA) sa bude Lead Overseer od IKT tretích strán vyberať príspevky na základe ich rozhodujúceho obratu

Kritickosť IKT tretích strán

- dvojkrokové posudzovanie s ohľadom na:

1. **vplyv na poskytovanie finančných služieb** (stabilitu, kontinuitu, kvalitu) v prípade zlyhania IKT tretej strany
2. **systémový charakter alebo význam finančných subjektov** na základe:
   - i) počet G-SII alebo O-SII závislých od príslušnej IKT tretej strany
   - ii) závislosť medzi G-SII a O-SII a inými finančnými subjektmi
3. **kritické alebo dôležité funkcie**
4. **stupeň nahraditeľnosti** IKT tretej strany
   - i) neexistencia alternatív (obmedzený počet, technologická zložitosť, osobitosť)
   - ii) ťažkosti s presunom na iného dodávateľa (presun dát, nákladnosť presunu, prevádzkové riziko)

Kritickosť IKT tretích strán



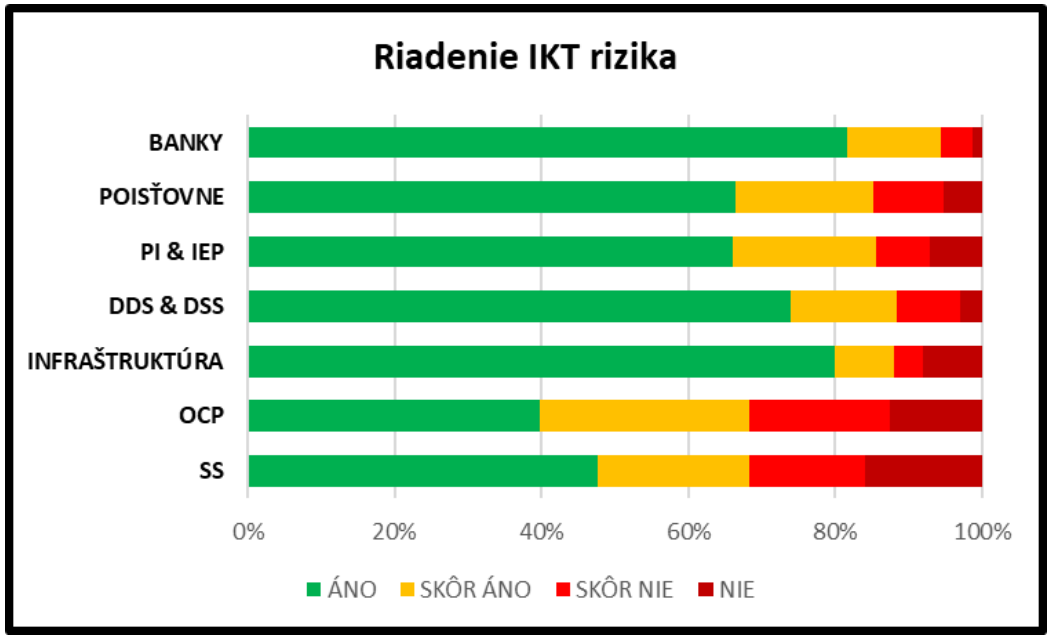
Pripravenosť slovenského finančného sektora

Dotazník

- samohodnotenie finančných subjektov
  - všeobecné informácie vrátane personálnych a finančných údajov
  - 95 otázok na základe 5 DORA oblastí
  - zatiaľ len všeobecná formulácia otázok z dôvodu absencie RTS/ITS v tej dobe
  - 4 úrovne súladu (áno/skôr áno/nie/skôr nie)
  - špecifické doplňujúce otázky zo všetkých oblastí nad rámec DORA (napr. typy incidentov, cloudové služby, ...)
- uskutočnené Q1/2023
- 79 subjektov (odpovedí) - výsledky je potrebné brať s určitou rezervou

Riadenie IKT rizika (25 otázok)

- subjekty deklarujú, že používajú a udržiavajú aktualizované systémy a nepretržite monitorujú a kontrolujú ich bezpečnosť a fungovanie
- tri štvrtiny subjektov dokumentujú politiky a postupy zálohovania, usilujú sa o zavádzanie mechanizmov na promptnú detekciu anomálnych aktivít
- viac ako 80% subjektov uvádza, že má zamestnancov dostatočne skúsených v oblasti IKT bezpečnosti
- u tretiny subjektov nie je rámec riadenia IKT rizík predmetom interného auditu
- tretina subjektov nedisponuje stratégiou digitálnej prevádzkovej odolnosti
- polovica subjektov nemá vypracovaný program zvyšovania informovanosti o bezpečnosti v oblasti IKT



Graf 1: Samohodnotenie pripravenosti finančného trhu na DORA v oblasti riadenia IKT rizík

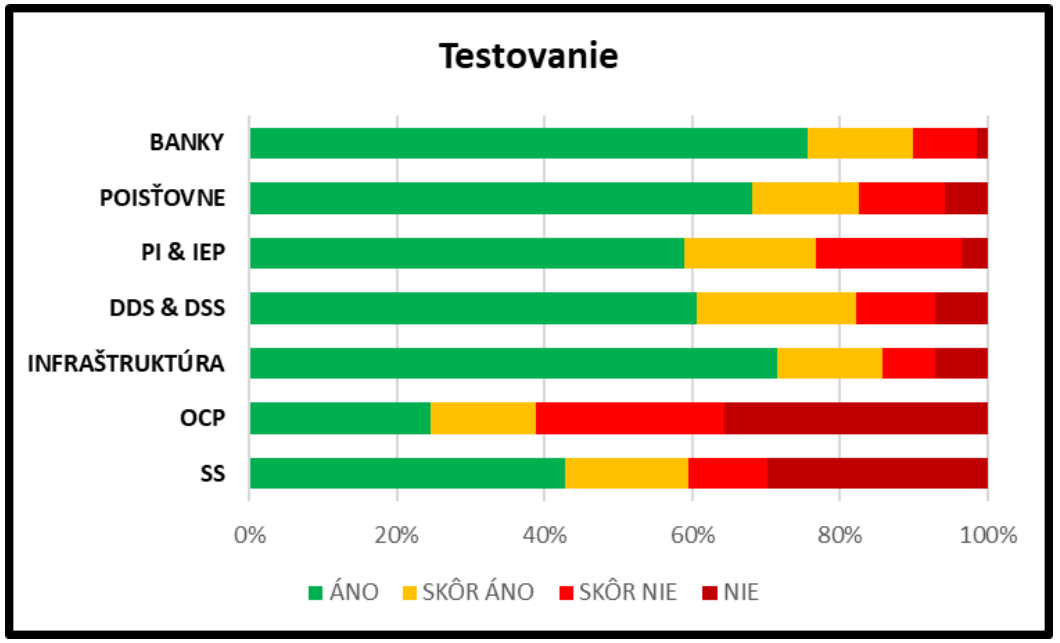
Incidenty (29 otázok)

- dve tretiny subjektov uvádzajú, že klasifikujú IKT incidenty a kybernetické hrozby a odlišujú ich od iných incidentov operačného rizika
- u 90% subjektov je riadiaci orgán subjektu o závažnom incidente informovaný
- takmer všetky subjekty deklarujú, že IKT incidenty nemali dopad na zahraničné subjekty v rámci konsolidovaného celku
- v tretine subjektov spôsobili IKT incidenty výpadok kritickej alebo dôležitej funkcie
- viac ako polovica subjektov nevyčísľuje súhrn ročných nákladov a strát spôsobených závažnými IKT incidentmi

Graf 2: Samohodnotenie pripravenosti finančného trhu na DORA v oblasti incidentov

Testovanie (18 otázok)

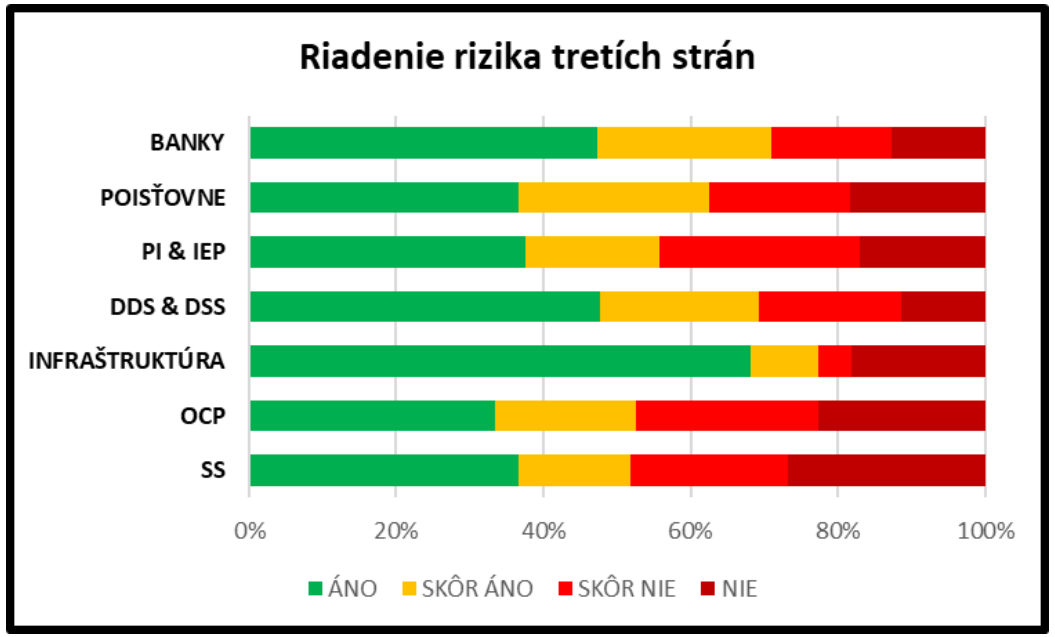
- viac ako tri štvrtiny subjektov uvádzajú, že vykonávajú základné funkčné testovanie na pravidelnej báze
- v polovici subjektov dochádza k uznávaniu testov v rámci konsolidovaného celku
- menej ako polovica subjektov má vypracovaný program testovania digitálnej prevádzkovej odolnosti
- dve tretiny subjektov nevykonávajú testovanie prostredníctvom červeného tímu (red team testing)
- polovica subjektov netestuje na produkčných systémoch



Graf 3: Samohodnotenie pripravenosti finančného trhu na DORA v oblasti testovania

Riadenie rizika tretích strán (18 otázok)

- viac ako dve tretiny subjektov požadujú od IKT tretích strán, aby spĺňali normy kvality v oblasti informačnej bezpečnosti
- takmer všetky subjekty identifikujú závislosti na IKT tretích stranách poskytujúcich služby podporujúce kritické alebo dôležité funkcie
- u 80% subjektov absentuje stratégia ukončenia angažovanosti voči IKT tretej strane
- iba tretina subjektov posudzuje riziko koncentrácie IKT tretích strán
- menej ako tretina subjektov by v plnom rozsahu dokázala nahradiť IKT tretie strany poskytujúce kritické a dôležité funkcie



Graf 4: Samohodnotenie pripravenosti finančného trhu na DORA v oblasti riadenia rizika tretích strán

Ďalšie kroky

Pilotné zbery

- incidenty
  - závažné IKT incidenty, významné kybernetické hrozby
  - počiatočné oznámenie 1x, priebežná správa nx, záverečná správa 1x
- register informácií
  - voľná príloha ŠZP
  - plný rozsah
  - priame zmluvy a subkontraktor 1. úrovne
  - nové/zmenené zmluvy
- testovanie
  - štruktúrovaný zber informácií vo forme dotazníka
- termín: Q4/23-Q2/24

Ďalšie informácie

- druhý balík RTS/ITS verejná konzultácia plánovaná na Q4/2023
- spolupráca so sektorovými asociáciami
- pravidelné informovanie na pripravovanej webstránke vrátane FAQ
- otázky: itdohlad@nbs.sk

Ďakujem za pozornosť

Otázky