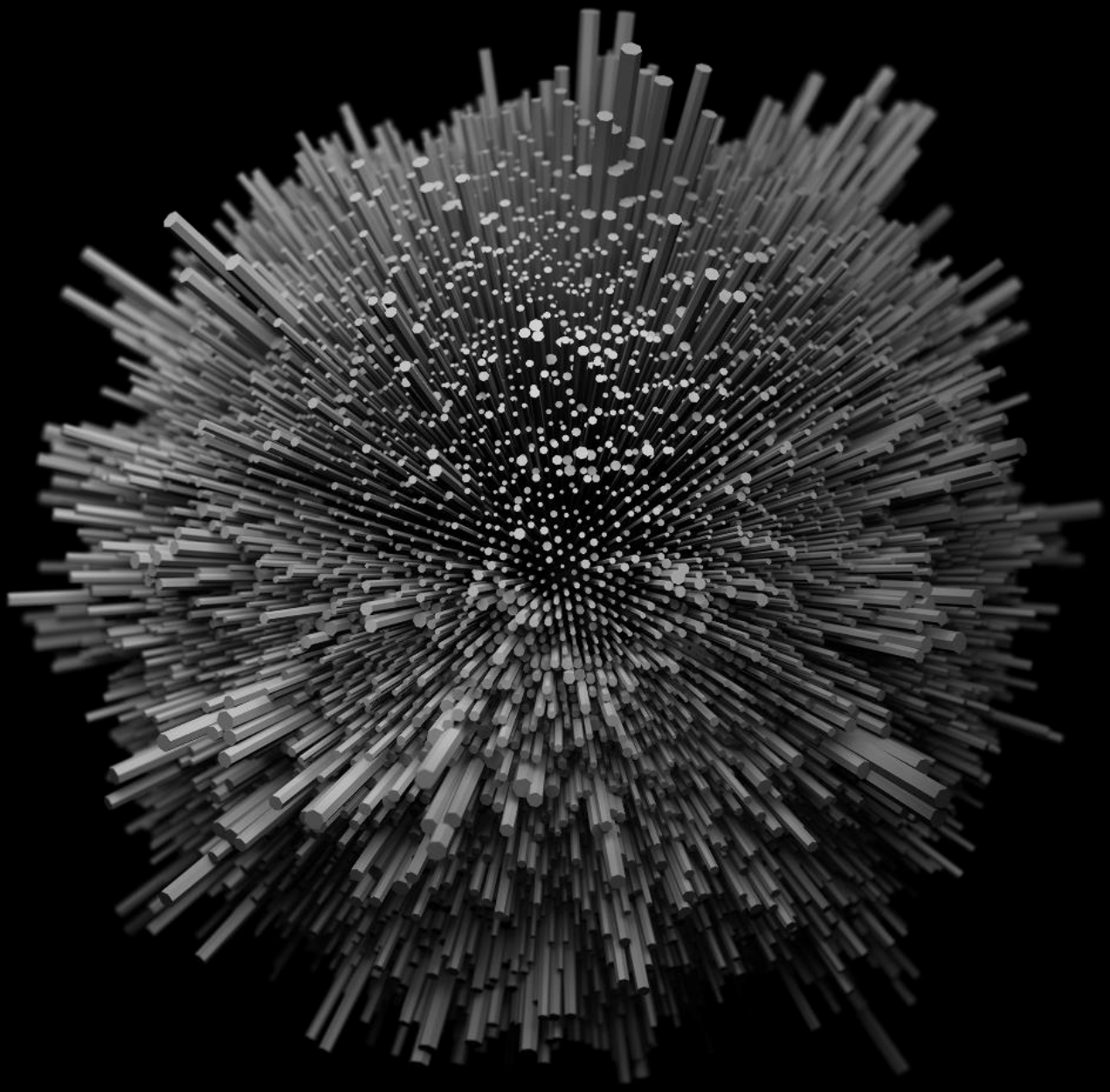
Deloitte.



DORA a NIS2

Dva legislativní nástroje EU.

V čem se liší? Jaké požadavky přinášejí? Jaké výzvy představují? Pro koho jsou relevantní? Buďte připraveni.

MAKING AN IMPACT THAT MATTERS since 1845

1 | Digital Operational Resilience Act (DORA)

DORA je **nařízení EU**, které přináší komplexní rámec pro **harmonizaci procesů a standardů v oblasti digitální odolnosti** s cílem **posílení odolnosti** digitálních operací ve **finančním sektoru** vůči digitálním a kybernetickým hrozbám. Jedná se o celosvětově první rámec, který umožňuje **dozorovým orgánům** v oblasti finančních služeb dohlížet na poskytovatele kritických ICT služeb, včetně poskytovatelů cloudových služeb.

NA KOHO SE DORA VZTAHUJE?

DORA se vztahuje na převážnou většinu firem působících v **oblasti finančních služeb**, včetně **bank, pojišťoven či investičních společností**.

CO DORA STANOVUJE?

DORA stanovuje závazná pravidla pro následující oblasti:

Řízení, klasifikace a hlášení incidentů souvisících s ICT

Testování digitální provozní odolnosti, včetně testování nástrojů, systémů a procesů ICT

Řízení rizik v oblasti ICT, včetně rámce a procesů pro řízení rizik

Řízení rizik v oblasti ICT spojených s třetími stranami, včetně rámce dohledu

Sdílení informací o kybernetických hrozbách

2 | Network and Information System 2 (NIS2)

NIS2 je **směrnice EU**, která stanovuje **obecné cíle pro národní zákony** členských států v oblasti **kybernetické bezpečnosti a ICT systémů a sítí** s cílem posílit bezpečnost napříč EU. Na rozdíl od nařízení, která jsou přímo použitelná v členských státech, je implementace NIS2 jako směrnice v kontextu ČR zajištěna **novelou zákona o kybernetické bezpečnosti (ZoKB**) z pera NÚKIB.

NA KOHO SE NIS2 VZTAHUJE?

NIS2 rozšiřuje počet subjektů, které spadají pod zákony regulující kybernetickou bezpečnost. Zjednodušeně řečeno se nová pravidla vztahují na jakékoli **provozovatele regulovaných služeb** – provozovatele ICT systémů, organizace z oboru bankovnictví a finančních služeb, energetiky, zdravotnictví, vodohospodářství nebo dopravy.

CO NIS2 STANOVUJE?

NIS2 stojí na třech základních pilířích:

Definice národních strategií pro kybernetickou bezpečnost

Podpora strategické spolupráce a výměny informací mezi členskými státy

Aplikace opatření na klíčová odvětví

Směrnice dopadne na veškeré subjekty poskytující služby v níže uvedených klíčových odvětvích a splňující podmínku „velkého podniku“ dle doporučení Evropské komise.

- **Energetika**
- **Doprava**
- **Bankovnictví a infrastruktura finančních trhů**
- **Zdravotnictví**
- **Veřejná správa**
- **Vesmír**
- **Vodovodní služby (pitná a odpadní voda)**
- **Digitální infrastruktura a poskytování řízených ICT služeb**

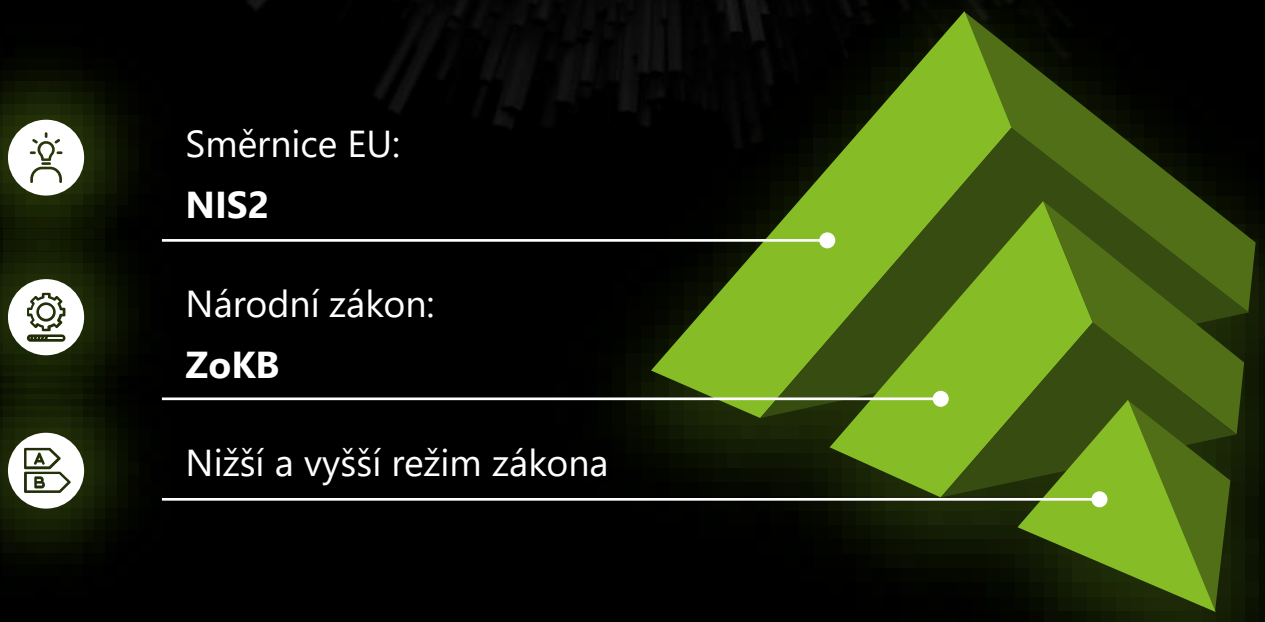
NIS2 nicméně dopadá i na další sektory, jako jsou **poštovní a kurýrní služby** nebo **odpadní hospodářství, chemický průmysl, potravinářství, výroba a výzkum**.

3 | NIS2 v ČR: Zákon o kybernetické bezpečnosti (ZoKB)

ZoKB představuje **aplikaci směrnice NIS2**, která mimo jiného stanovuje oblasti, jež musí zákon pokrývat, včetně:

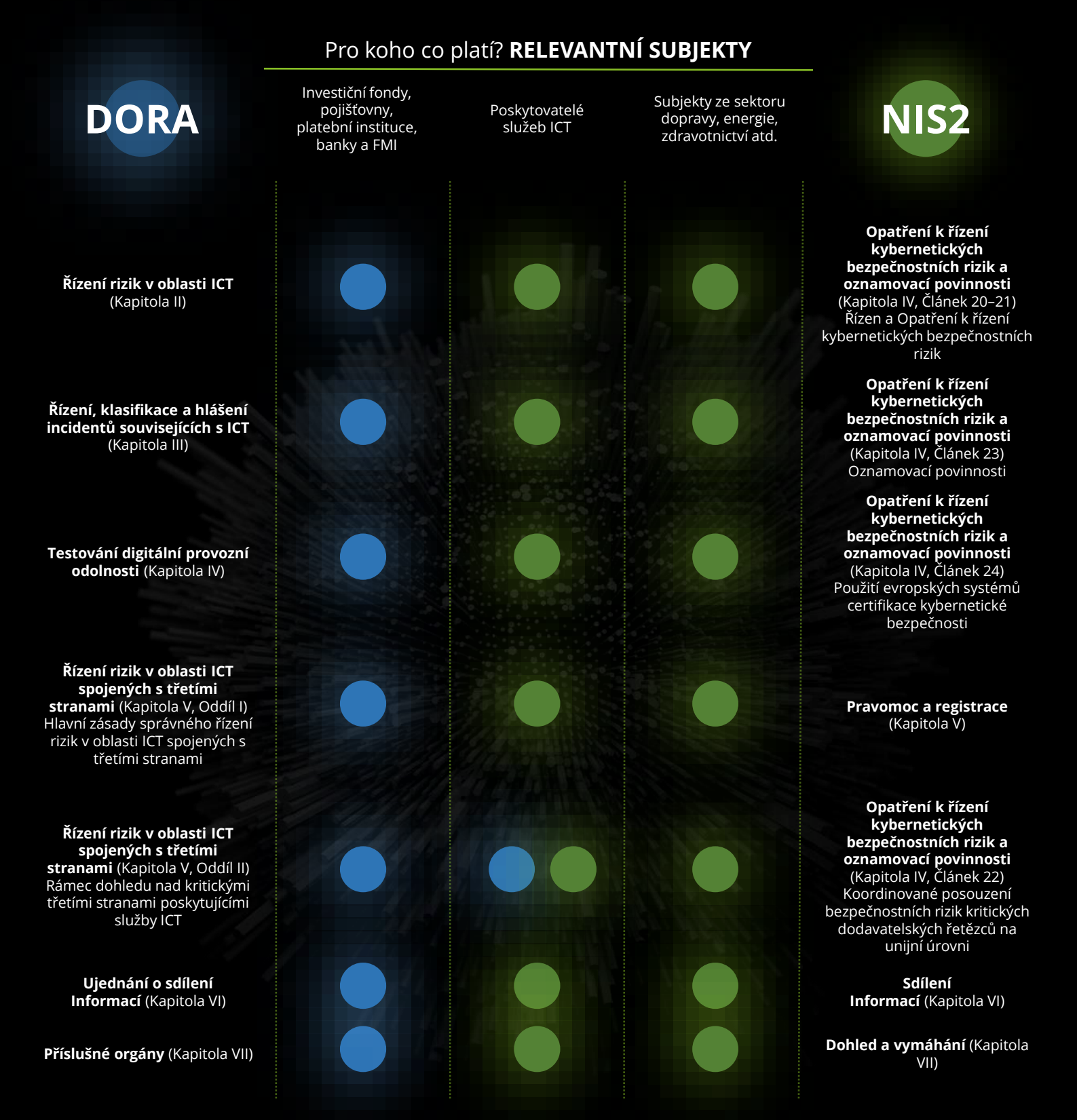
- Systému **řízení bezpečnosti** informací
- Řešení **kybernetických incidentů**
- **Řízení kontinuity provozu**
- Bezpečnosti **dodavatelského řetězce**
- Bezpečného **nákupu, vývoje a údržby**
- Bezpečnostního **auditu**
- Kybernetické **hygieny a školení**
- **Kryptografických** postupů a šifrování
- **Bezpečnosti lidských zdrojů**
- Kontroly **přístupu**
- Správy **aktiv**
- Bezpečné **komunikace**

Návrh ZoKB byl předložen v létě 2023 a stanovoval **dva režimy** – vyšší a nižší, jež odrážejí princip dvourychlostní kybernetické bezpečnosti s cílem ulehčit menším organizacím od přísných pravidel. Momentálně je však znovu v procesu příprav – členské státy mají čas do 17. října 2024, aby NIS2 zanesly do vnitrostátního práva.



4 | DORA jako Lex Specialis pro finanční instituce

Pokud jde o vymezení vazeb mezi nařízením DORA a směrnicí NIS2, dle Evropské komise pro subjekty finančního sektoru představuje DORA *lex specialis*, což znamená, že v praxi mají požadavky DORA přednost před jakýmikoli překrývajícími se regulačními texty, jako jsou směrnice NIS nebo ESA.



5 | Jak Vám můžeme pomoci?

V Deloitte nabízíme komplexní, holistické služby, které mohou být pro Vaši organizaci přínosem, a to od GAP analýzy až po samotnou implementaci kroků vedoucích k souladu s danými regulacemi.

GAP analýza a implementace

Provedeme analýzu existujících procesů, aplikací a personálního zabezpečení v kontextu relevantních pravidel, navrhneme implementační roadmapu zohledňující Vaši technologickou, procesní a organizační připravenost, navrhneme konkrétní změny na úrovni celku a jednotlivých domén a budeme Vám nápomocni při jejich implementaci.

Rámec řízení rizik

Abyste splnili relevantní požadavky, budete muset mít zavedeny spolehlivé procesy řízení rizik. Pomůžeme Vám sladit obchodní strategie a kybernetická rizika Vaší organizace a udržovat komplexní a účinný rámec řízení rizik.

Řízení rizik třetích stran (TPRM) a monitorování

Posouzení, zda Vaše strategie a plány reakce a obnovy odpovídajícím způsobem reagují na pravidla vztahující se na řízení rizik v oblasti ICT, můžete nechat na našich odbornících. TPRM rámec společnosti Deloitte je založen na špičkových postupech a vychází z globálních regulačních požadavků. Poskytujeme tak holistické řešení při řízení složitostí v rámci ekosystémů třetích stran.

Hlášení incidentů a sdílení analýzy hrozeb

Pomůžeme Vám přizpůsobit se novým pravidlům v oblasti podávání zpráv a sladit v tomto směru interní procesy s cílem optimalizovat přidělování zdrojů. Zároveň asistujeme při vývoji a integraci procesu sdílení informací o kybernetických hrozbách.

Testování odolnosti a penetrační testování na základě hrozeb (TLPT)

Provádíme skenování zranitelností, penetrační testy i robustní testování kontinuity podnikání a zotavení se po havárii. Naše kybernetická praxe poskytuje nejkvalitnější služby penetračního testování svého druhu, a to díky našim vysoce kvalifikovaným odborníkům a technologickému zázemí.

Neváhejte nás kontaktovat

Jakub Höll
Director
Cyber Strategy Lead
+420 734 353 815
jholl@deloittece.com

Martin Antoš
Manager
IT Regulatory Compliance Expert
+420 734 783 919
mantos@deloittece.com

Viktor Paggio
Manager
Cyber SME
+420 725 009 732
vpaggio@deloittece.com

Deloitte.