Směrnice NIS2
a hlavní plány její transpozice v České republice

Michaela Henzlová

Jan Hénik

NÚKIB

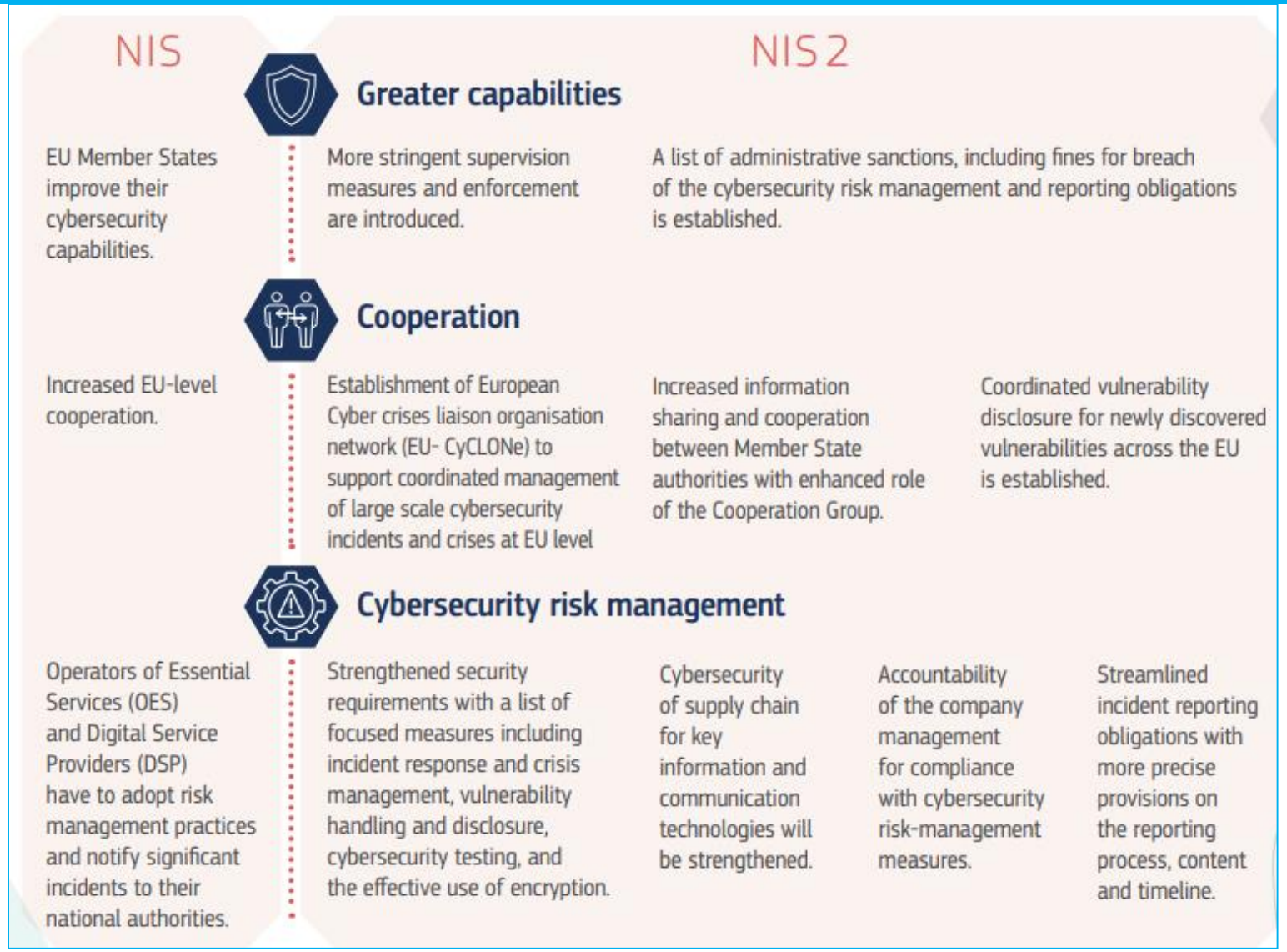
Národní úřad pro kybernetickou a informační bezpečnost

listopad 2022
TLP: CLEAR

Odbor regulace
NÚKIB

Období po roce 2024 (?)

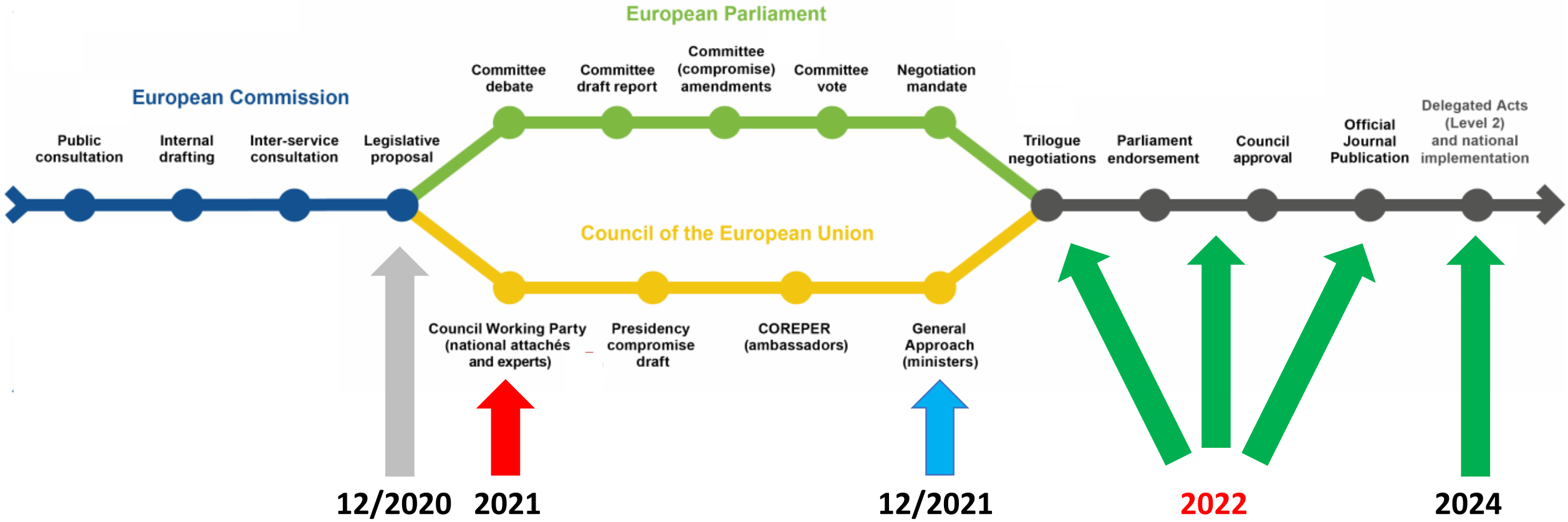
- Na konci roku 2020 zahájena z podnětu Evropské Komise revize směrnice NIS **– tzv. směrnice NIS2.**
  - prvotní návrh zveřejněn zde: [Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)]
- Aktuální návrh zachovává mnoho institutů z původní směrnice NIS, většinu z nich však prohlubuje



Zdroj schématu: [Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu)]

Vývoj vyjednávání NIS2

Aktuální stav a časový odhad legislativního procesu:



- Shoda s EP nalezena, finalizován text, **publikace plánována v 4Q 2022** (transpoziční lhůta 21 měsíců)
- **Implementace do národního práva se předpokládá v polovině roku 2024.**

Disclaimer

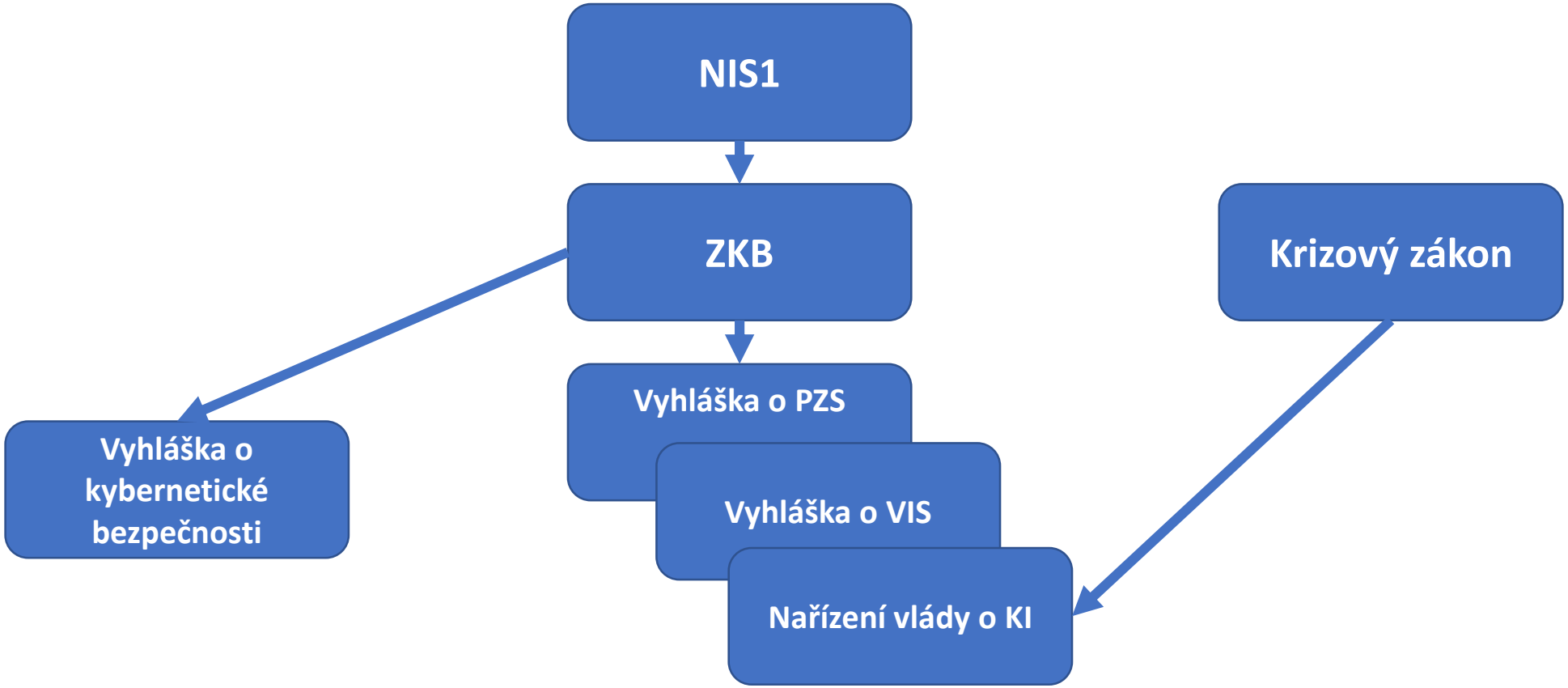
Ačkoli již byla v rámci unijního legislativního procesu nalezena předběžná shoda ohledně budoucí podoby směrnice NIS2, finální text směrnice dosud nebyl schválen a publikován v Úředním věstníku Evropské unie.

Výsledná podoba směrnice se tedy ještě může měnit.

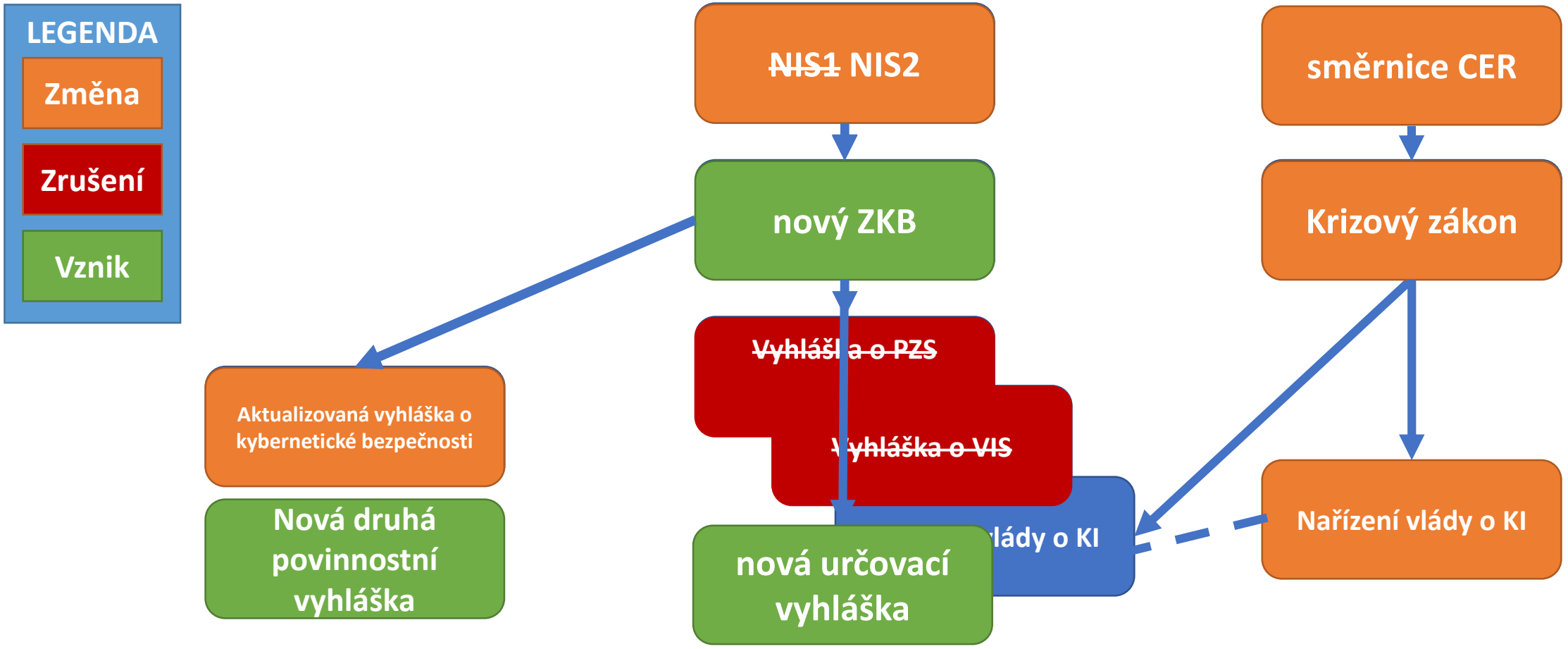
Informace publikované v této prezentaci vycházejí z posledních veřejně dostupných verzí směrnice a mohou být do budoucna upraveny v závislosti na finální podobě textu.

V rámci legislativního procesu mohou prezentované závěry projít změnami.

Návrh změny – současný stav



Návrh změny – budoucí chtěný stav



Konkrétní změny – povinné osoby

Aktuálně regulováno cca **400** povinných osob

Nově regulováno minimálně **6 000** povinných osob
(tzn. min 15x tolik)

Proč?

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud

systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

Koho se budou nové povinnosti týkat I.

- Okruh odvětví regulovaných NIS2 je uveden v přílohách I a II.
  - Směrnicí je regulováno cca 60 služeb v 18 odvětvích
- **Regulace se netýká každého v daném odvětví** – musí splnit kritéria:
  - organizace poskytuje **alespoň jednu službu uvedenou v přílohách směrnice, a zároveň**
  - **je středním nebo velkým podnikem**, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK).
- Speciální pozornost při posuzování velikosti podniku je potřeba věnovat přičítání velikosti dalších organizací k velikosti mé organizace v rámci kategorií tzv. partnerských nebo propojených podniků.
  - především v případě koncernového řízení to může v praxi znamenat, že dceřiná společnost, která by sama o sobě byla velikostí malým podnikem bude při připočtení velikosti mateřské společnosti např. středním nebo velkým podnikem

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Doporučení Komise 2003/361/ES z 6. května 2003

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

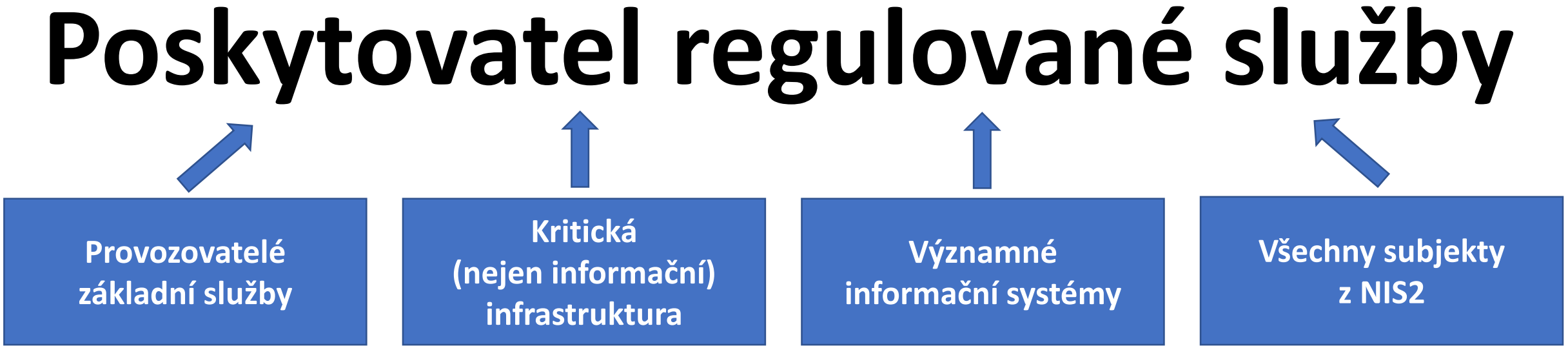
Evropská Komise, Uživatelská příručka k definici malých a středních podniků, PDF ISBN 978-92-79-69931-3 doi:10.2873/117802 ET-01-17-660-CS-

Koho se budou nové povinnosti týkat II.

- **Velikost organizace ve spojení se službou je sice primárním způsobem určení, ale není jediným.**
- U některých vyjmenovaných služeb je stanoveno, že pod regulaci směrnice NIS2 budou **spadat všechny organizace**, nehledě na jejich velikost.
- Členské státy mají také k zařazení do regulace využít dodatečných kritérií a vztáhnout regulaci i na takové organizace, které **poskytují služby uvedené v přílohách, a zároveň bez ohledu na velikost**
  - jsou **jedinými poskytovateli** služby, která je nezbytná v členském státě ze sociálního nebo ekonomického hlediska,
  - by narušení jejich služby mohlo mít **významný dopad** na veřejnou bezpečnost nebo zdraví osob,
  - by narušení jejich služby mohlo vyvolat **významné riziko, zejména s přeshraničním dopadem**.
- Posledním specifickým způsobem určení je **propojení směrnice NIS2 s tzv. směrnicí CER (směrnice týkající se budoucí kritické infrastruktury)** – kdo bude povinnou osobou podle CER (neznámá množina) – bude povinou osobou podle NIS2

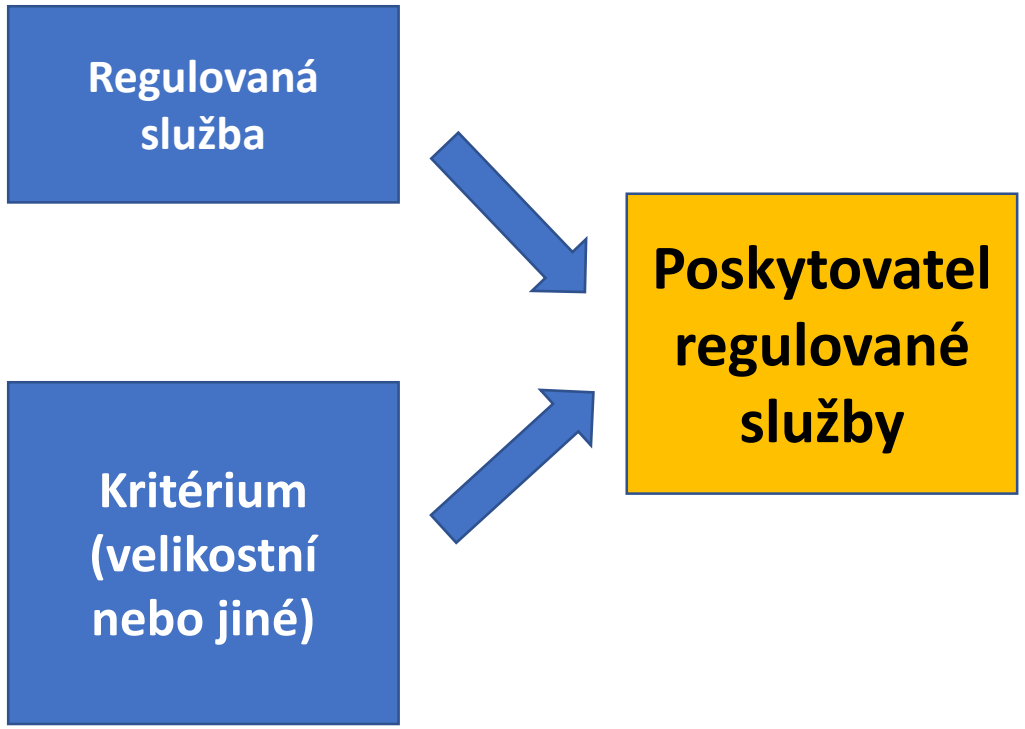
Nové znění zákona o kybernetické bezpečnosti

Jedna jediná povinná osoba*:



*Pro primární sadu některých povinností spojených s prevencí – zavádění bezpečnostních opatření, hlášení incidentů, apod.

Shrnutí stanovení povinných osob



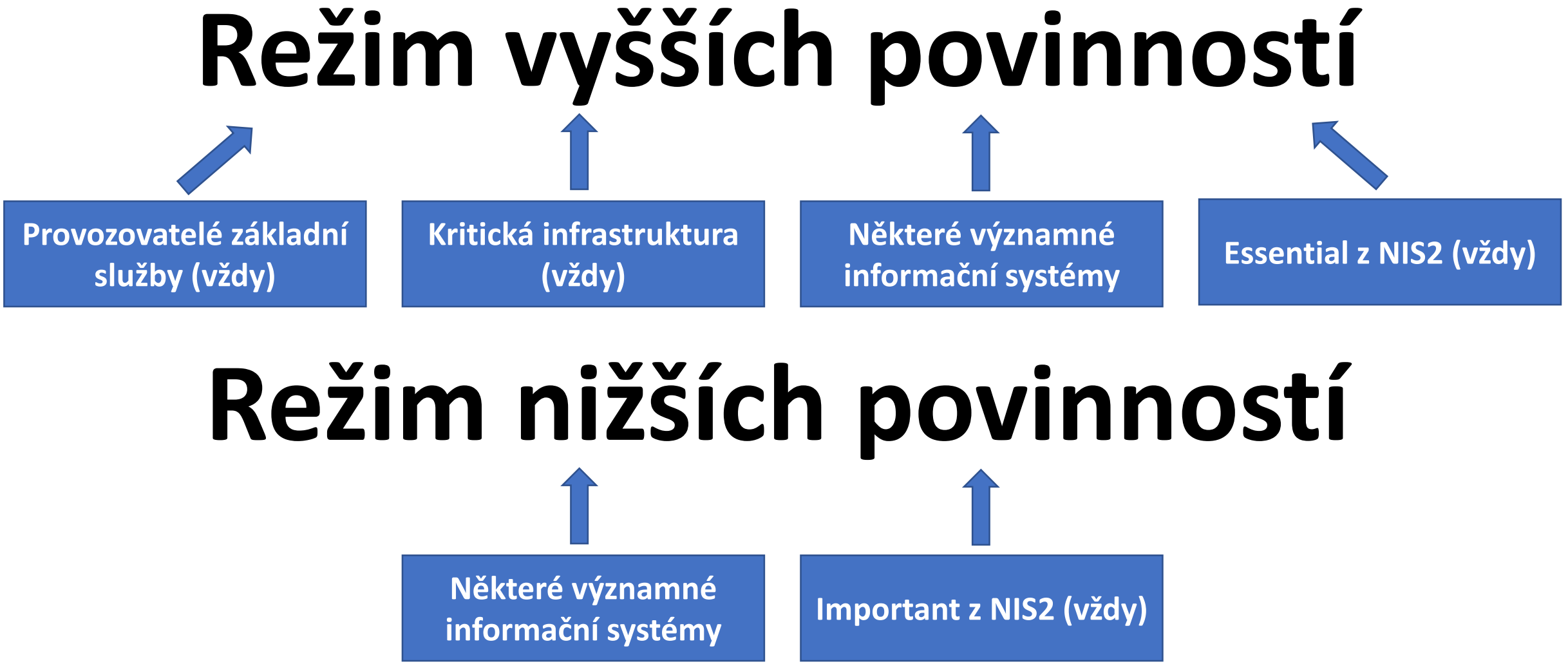
Režimy povinné osoby podle směrnice NIS2

*„Entities falling within the scope of this Directive should be **classified into two categories,** essential and important reflecting the level of criticality of the sector or of the type of services they provide, as well as their size.“*

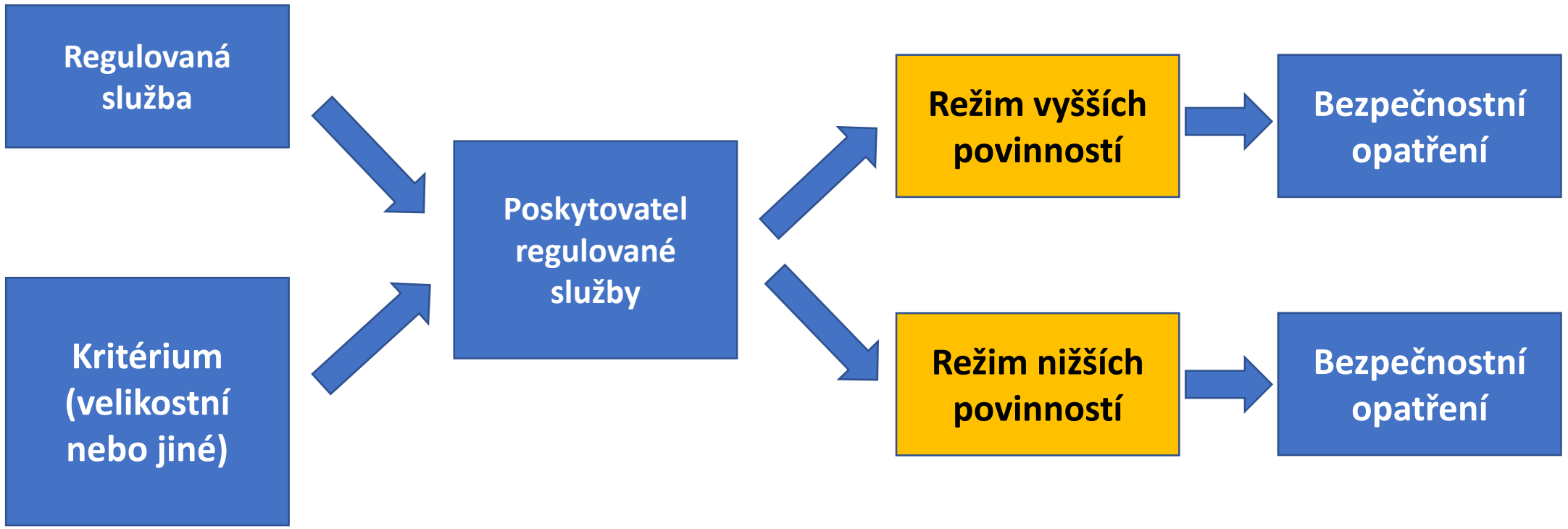
Essential entities (základní)

Important entities (významné)

Nové znění zákona o kybernetické bezpečnosti



Shrnutí stanovení povinných osob



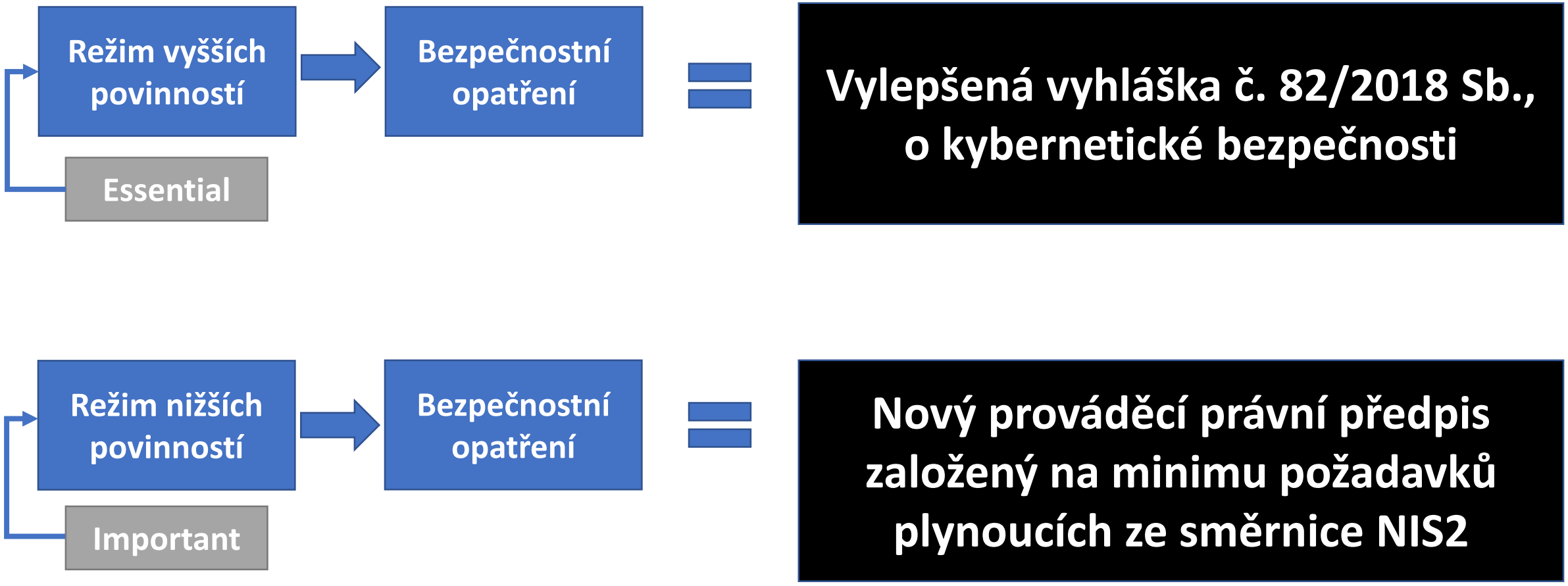
Bezpečnostní opatření

Směrnice stanovuje okruhy bezpečnostních opatření, které mají členské státy rozpracovat ve svých právních předpisech a uložit je budoucím povinným osobám (aktuální čl. 18 NIS2):

- **Analýza rizik** a **politiky bezpečnosti informací;**
- **Zvládání incidentů;**
- **Kontinuita činností** (tj. business kontinuita), přičemž směrnice tento okruh ještě rozvádí o příklad zálohování, zotavení (disaster recovery) a krizové řízení;
- Bezpečnost v rámci **dodavatelského řetězce;**
- Bezpečnost v rámci **pořízení, vývoje a údržby systémů;**
- Politiky a postupy pro hodnocení účinnosti bezpečnostních opatření (tj. **audit**);
- Praktiky **základní počítačové hygieny a vzdělávání** v oblasti kybernetické bezpečnosti;
- Politiky a postupy týkající se využívání **kryptografie** a tam, kde je to vhodné, také šifrování;
- **Bezpečnost lidských zdrojů, řízení přístupů a aktiv;**
- Využívání **vícefaktorového ověření identity, bezpečných komunikačních nástrojů** a **nástrojů pro nouzovou komunikaci.**

+ Povinné vzdělávání vrcholového vedení organizace (aktuální čl. 17 NIS2)**.**

Zavádění bezpečnostních opatření: Dva režimy



Další změny, o kterých je dobré vědět

- Změny by vzhledem k transpoziční lhůtě měly být platné cca **od poloviny roku 2024**
- **Povinné vzdělávání vrcholového vedení organizace**
- **Zvýšení sankcí** (inspirace GDPR)**:**
  - Dnes max. 5 milionů Kč – nově:
    - **2 % celkového obratu společnosti nebo 10 milionů EUR** (platí vyšší částka) = essentials (režim vyšších povinností)
    - **1,4 % celkového obratu společnosti nebo 7 milionů EUR** (platí vyšší částka) = importants (režim nižších povinností)
- **Nové sankce:**
  - Dočasný zákaz výkonu řídící funkce fyzické osobě v regulované organizaci*
  - Pozastavení certifikace nebo autorizace regulované osoby*

**Platí pro essentials (režim vyšších povinností)*

Registrace a komunikace s NÚKIB

- Je nezbytné změnit styl, jakým dnes probíhá
  - určování povinných osob (nově primárně samoidentifikací)
  - hlášení kybernetických bezpečnostních incidentů
  - komunikace s Úřadem
  - sdílení informací o zranitelnostech

- Aby to fungovalo rychle, pružně a bez zbytečné administrativy je třeba všechny tyto činnosti komplet **elektronizovat** a **zautomatizovat**.

- Řešením je **vznik jednotného systému,** skrze který bude realizována
  - registrace poskytovatele regulované služby,
  - hlášení incidentů (nejen) poskytovatele regulované služby,
  - sdílení informací o známých zranitelnostech a hrozbách.

Odvětví: Veřejné správa

Regulovaná služba		*Transpozice NIS2*
Služba	Kritérium poskytovatele regulované služby	
Výkon svěřených pravomocí	I) poskytovatel regulované služby v režimu vyšších povinností, v případě, že je: a) ústředním orgánem státní správy, b) správním úřadem s celostátní působností, a to včetně ústředí/generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy c) Kanceláří prezidenta republiky, Kanceláří Senátu, Kanceláří Poslanecké sněmovny, Kanceláří Veřejného ochránce práv, d) Českou národní bankou, e) Nejvyšším kontrolním úřadem, f) Policejním prezidiem, g) útvarem policie s celostátní působností, h) orgány soudní moci, i) státním zastupitelstvím, j) zdravotní pojišťovnou, k) krajem, l) hlavním městem Praha, m) obcí s rozšířenou působností, ve které je sídlo krajského úřadu, n) určeným státním podnikem, o) určenou státní příspěvkovou organizací. II) poskytovatel regulované služby v režimu nižších povinností, v případě, že je: a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou, c) vysokou školou, d) Akademií věd České republiky, e) obcí s rozšířenou působností.	*Public administration entities of central governments as defined by a Member State in accordance with national law* *Public administration entities at regional level as defined by a Member State in accordance with national law*

Web NÚKIB k směrnici NIS2

- Spuštěn web – dostupný zde: nis2.nukib.cz

Dotazy?

Děkuji za pozornost!

regulace@nukib.cz
j.henik@nukib.cz