Směrnice NIS2
a hlavní plány její transpozice v České republice

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Martin Švéda
vedoucí oddělení
Oddělení regulace soukromého sektoru
Odbor regulace
NÚKIB

14. září 2022
TLP: CLEAR

-CYBERCON 2022-

O čem to bude

- Navážeme na přednášku „Aktuality v oblasti regulace kybernetické bezpečnosti“ v tématu směrnice NIS2
- Dozvěděli jsme se, že směrnice NIS2 dopadne na nejméně 6 000 subjektů v ČR **– ale na jaké, a jak se poznají?**
- Čtyři dosavadní základní povinnosti ze zákona o kybernetické bezpečnosti
  - Hlášení kontaktních údajů
  - Bezpečnostní opatření
  - Hlášení incidentů
  - Opatření

  – jak to s nimi bude?
- Jak se budou kontrolovat?

Disclaimer

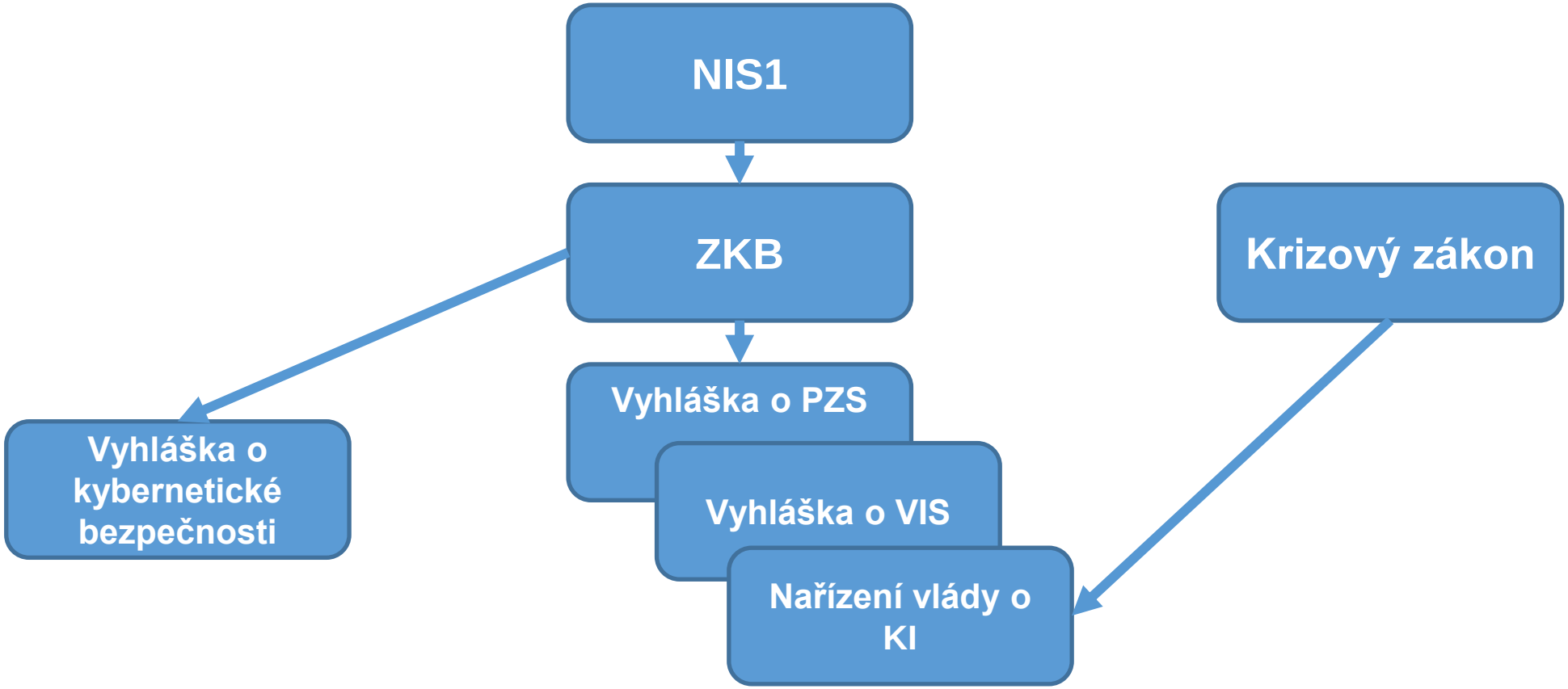
Ačkoli již byla v rámci unijního legislativního procesu nalezena předběžná shoda ohledně budoucí podoby směrnice NIS2, finální text směrnice dosud nebyl schválen a publikován v Úředním věstníku Evropské unie.

Výsledná podoba směrnice se tedy ještě může měnit.

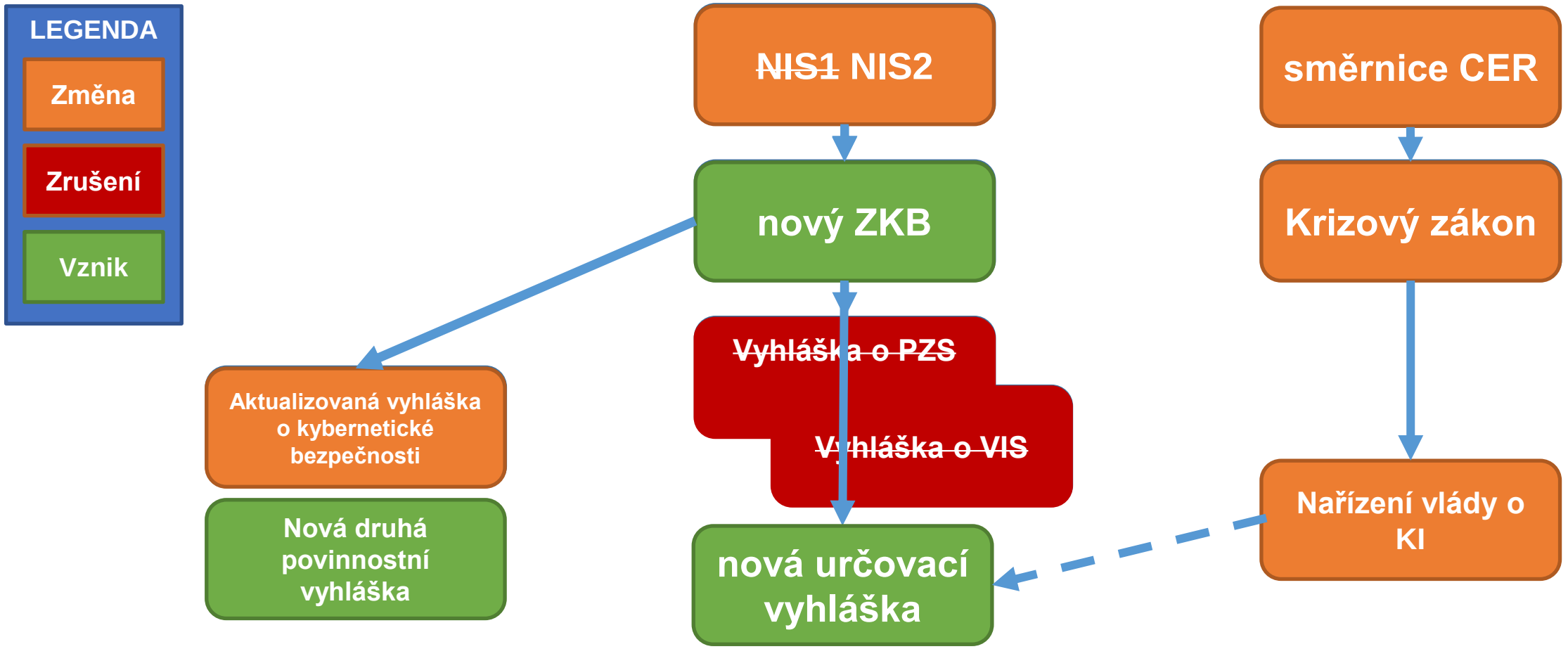
Informace publikované v této prezentaci vycházejí z posledních veřejně dostupných verzí směrnice a mohou být do budoucna upraveny v závislosti na finální podobě textu.

V rámci legislativního procesu mohou prezentované závěry projít změnami.

Návrh změny – současný stav



Návrh změny – budoucí chtěný stav



Konkrétní změny – povinné osoby

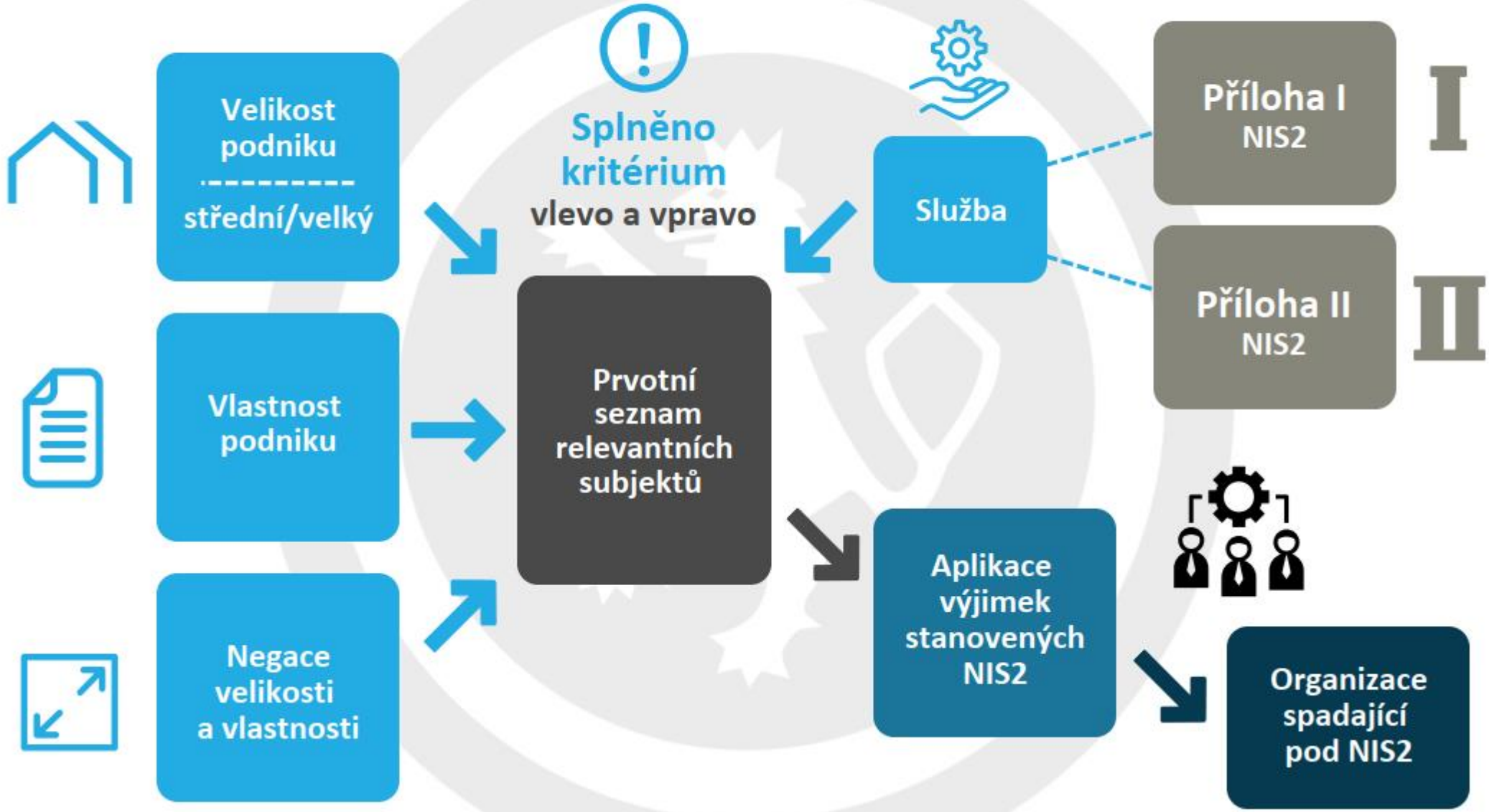
Aktuálně regulováno cca **400** povinných osob

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

Proč?

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB



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.

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 s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

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.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

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 provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

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 computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

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.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

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

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

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

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-N

Pravidla regulace podle směrnice NIS2

Obecné – hlavní – pravidlo:

Organizace poskytuje **alespoň jednu** (regulovanou) **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)).

Doplňující pravidla:

Někdy stačí jen služba, bez ohledu na velikost (např. ISP)

Kdokoliv ze směrnice CER

Jediný poskytovatel služby; narušení služby mohlo mít významný dopad na veřejnou bezpečnost nebo zdraví osob, narušení by mohlo vyvolat významné riziko, …

Pravidla regulace podle směrnice NIS2

Obecné – hlavní – pravidlo:

Organizace poskytuje **alespoň jednu** (regulovanou) **službu** uvedenou v přílohách směrnice, **a zároveň je středním nebo velkým podnikem** (tj. kdy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK)).

nejméně 6 000

Doplňující pravidla:

Někdy stačí jen služba, bez ohledu na velikost (např. ISP)

Kdokoliv ze směrnice CER

Jediný poskytovatel služby; narušení služby mohlo mít významný dopad na veřejnou bezpečnost nebo zdraví osob, narušení by mohlo vyvolat významné riziko, …

Současné znění zákona o kybernetické bezpečnosti

§ 3 Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou

a) **poskytovatel služby elektronických komunikací** a **subjekt zajišťující síť elektronických komunikací,**
b) orgán nebo osoba zajišťující **významnou síť,**
c) správce a provozovatel informačního systému **kritické informační infrastruktury,**
d) správce a provozovatel komunikačního **systému kritické informační infrastruktury,**
e) správce a provozovatel **významného informačního systému,**
f) správce a provozovatel **informačního systému základní služby,**
g) **provozovatel základní služby,** a
h) **poskytovatel digitální služby.**

Současné znění zákona o kybernetické bezpečnosti

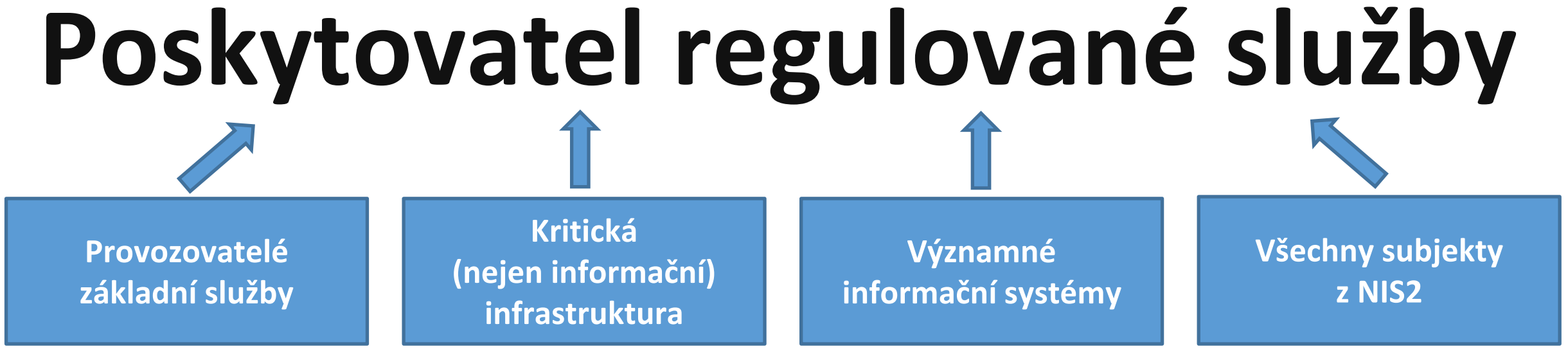
§ 3 Orgány a osobami, kterým [illegible]ládají povinnosti v oblasti kybernetické bezpečnosti, jsou

a) **poskytovat[illegible] elektronických [illegible]unikací** a **subjekt zajišťující síť elekt[illegible]h komunikací**,
b) orgán nebo osoba zajišťu[illegible] **významnou síť,**
c) správce a provozovatel informačního systému **kriti[illegible]é informační infrastruktury,**
d) správce a provozovatel komunikačn[illegible]ího **kritické inf[illegible]ní infrastruktury,**
e) správce a provozovatel **význam[illegible] informač[illegible]stému,**
f) správce a provozovatel i[illegible]ního systé[illegible]u **základní služby,**
g) **provozovatel základ[illegible]žby,** a
h) **poskytovatel digitální služby**.

směrnice NIS2
směrnice NIS2
směrnice NIS2
národní úprava
směrnice NIS2
směrnice NIS2

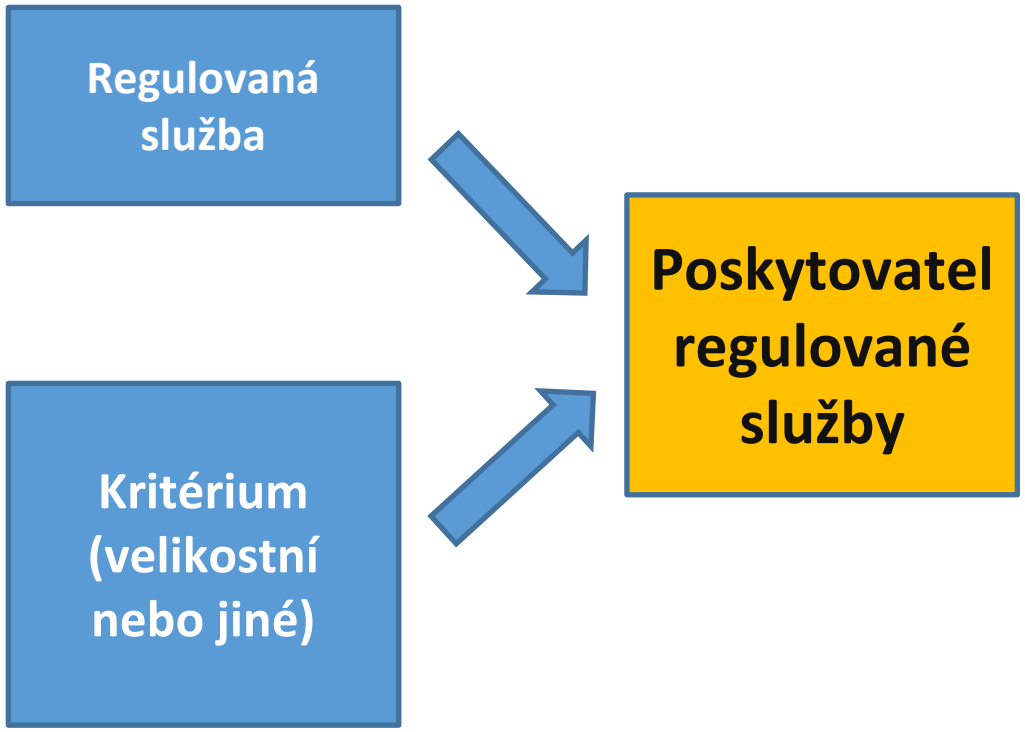
Nové znění zákona o kybernetické bezpečnosti

Jedna jediná povinná osoba*:



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

Shrnutí stanovení povinných osob



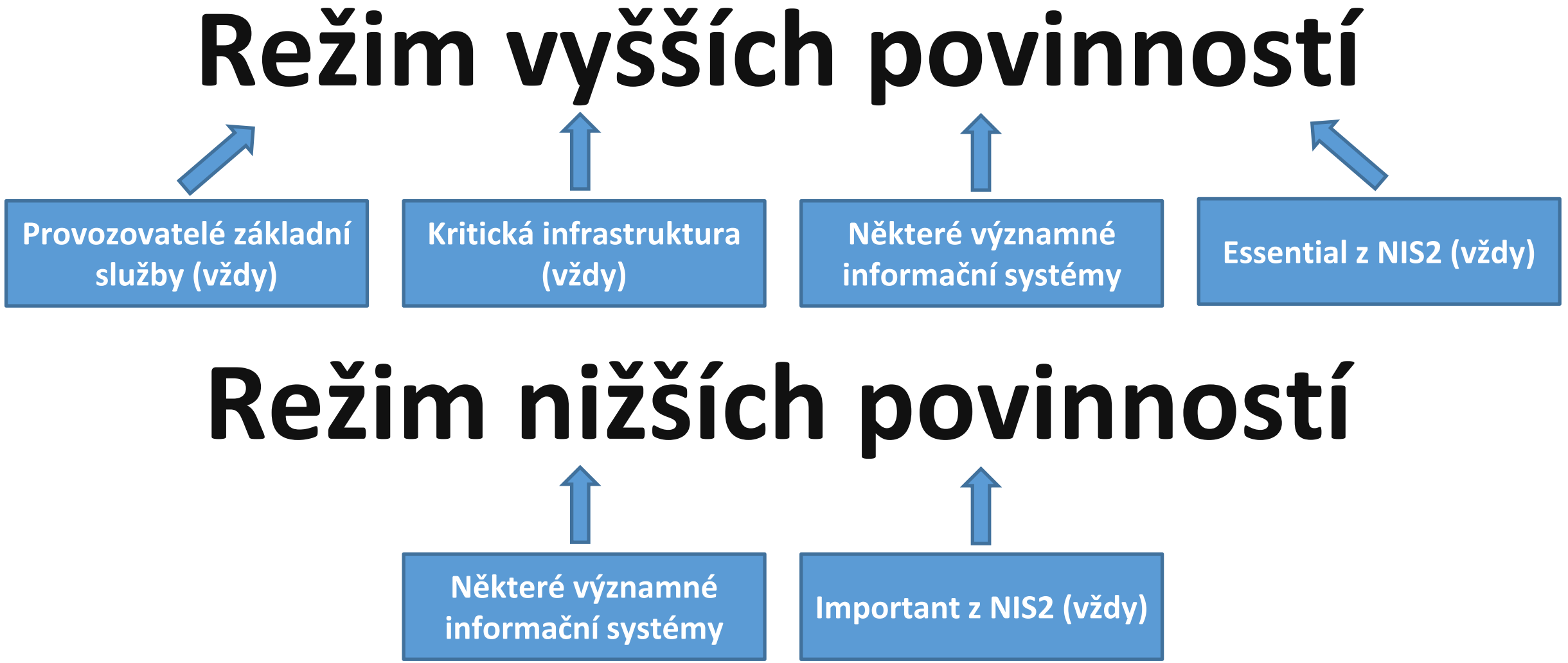
Režimy povinné osoby podle směrnice NIS2

*„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.“*

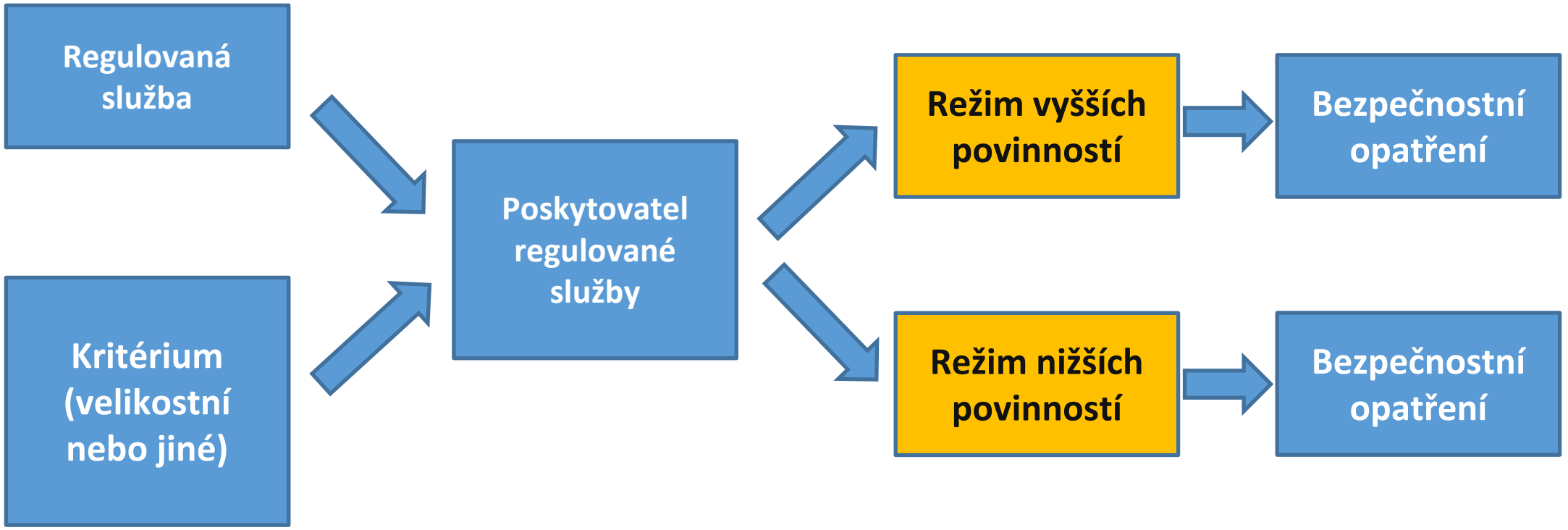
Essential entities (základní)

Important entities (významné)

Nové znění zákona o kybernetické bezpečnosti



Shrnutí stanovení povinných osob



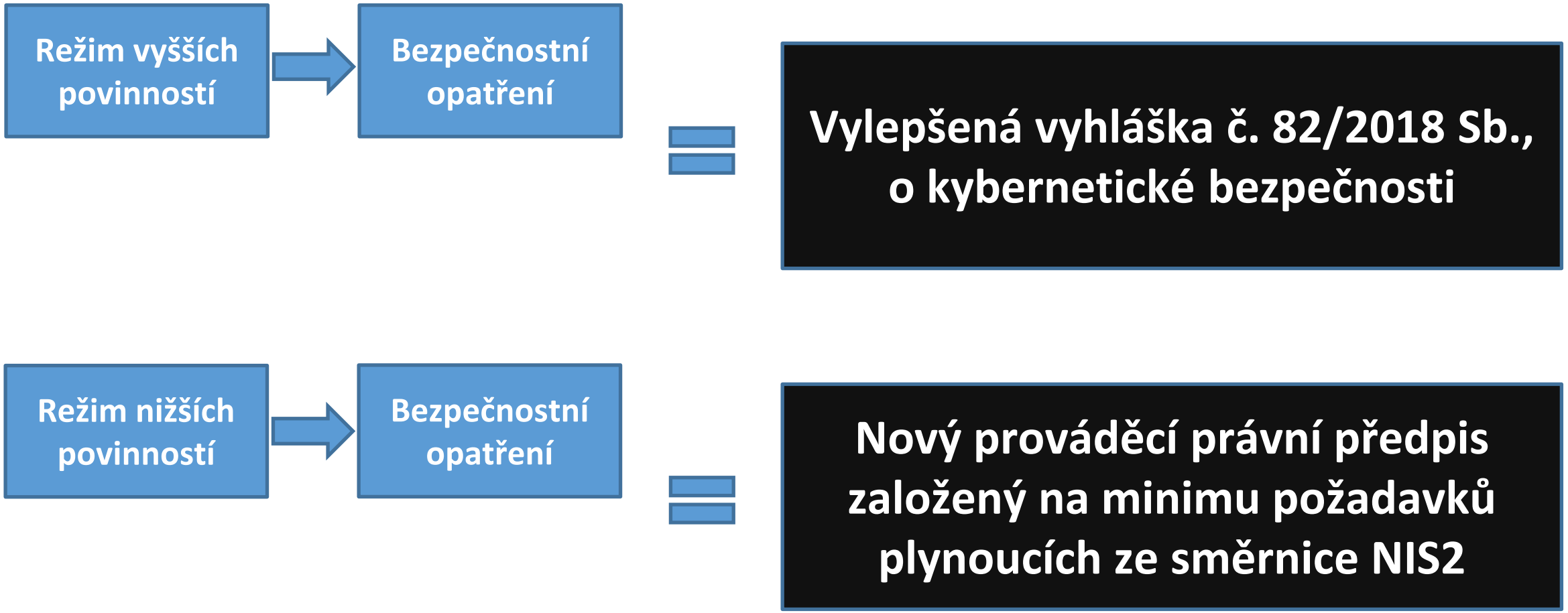
Bezpečnostní opatření

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

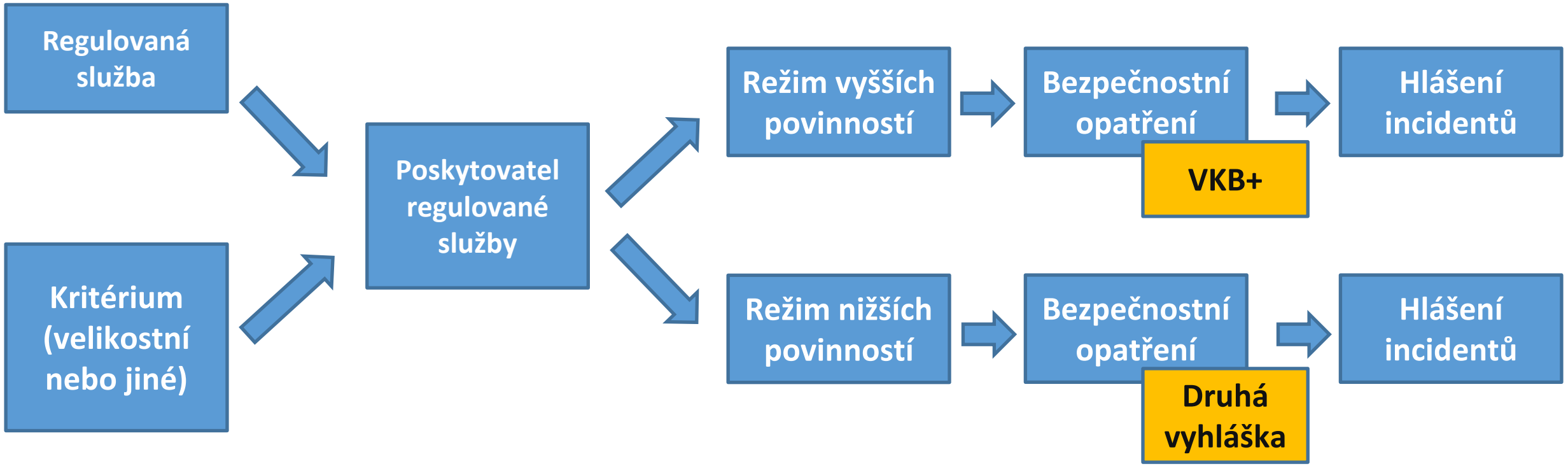
- **Analýza rizik** a **politiky bezpečnosti informací;**
- **Zvládání incidentů;**
- **Kontinuita činností** (tj. business kontinuita), přičemž směrnice tento okruh ještě rozvádí o příklad zálohování, zotavení (disaster recovery) a krizové řízení;
- Bezpečnost v rámci **dodavatelského řetězce;**
- Bezpečnost 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)**.**

Shrnutí stanovení povinných osob



Shrnutí stanovení povinných osob



Hlášení kybernetických bezpečnostních incidentů

Kybernetickým bezpečnostním incidentem se rozumí narušení bezpečnosti informací v rámci aktiv (související s regulovanou službou).

Hlášení kybernetického bezpečnostního incidentu na NÚKIB

= jen ty, které mají původ v kybernetickém prostoru.

Pro hlášení je potřeba posoudit dvě situace:

1) **významný dopad na poskytování regulované služby**
2) **úmyslné zavinění kybernetického bezpečnostního incidentu**

Shrnutí stanovení povinných osob

Poskytovatel regulované služby

Režim vyšších povinností

významný dopad + **úmyslné** zavinění	**významný** dopad + **ne**úmyslné zavinění
nevýznamný dopad + **úmyslné** zavinění	**nevýznamný** dopad + **ne**úmyslné zavinění

Režim nižších povinností

významný dopad + **úmyslné** zavinění	**významný** dopad + **ne**úmyslné zavinění
nevýznamný dopad + **úmyslné** zavinění	

Shrnutí stanovení povinných osob

Poskytovatel regulované služby

Režim vyšších povinností

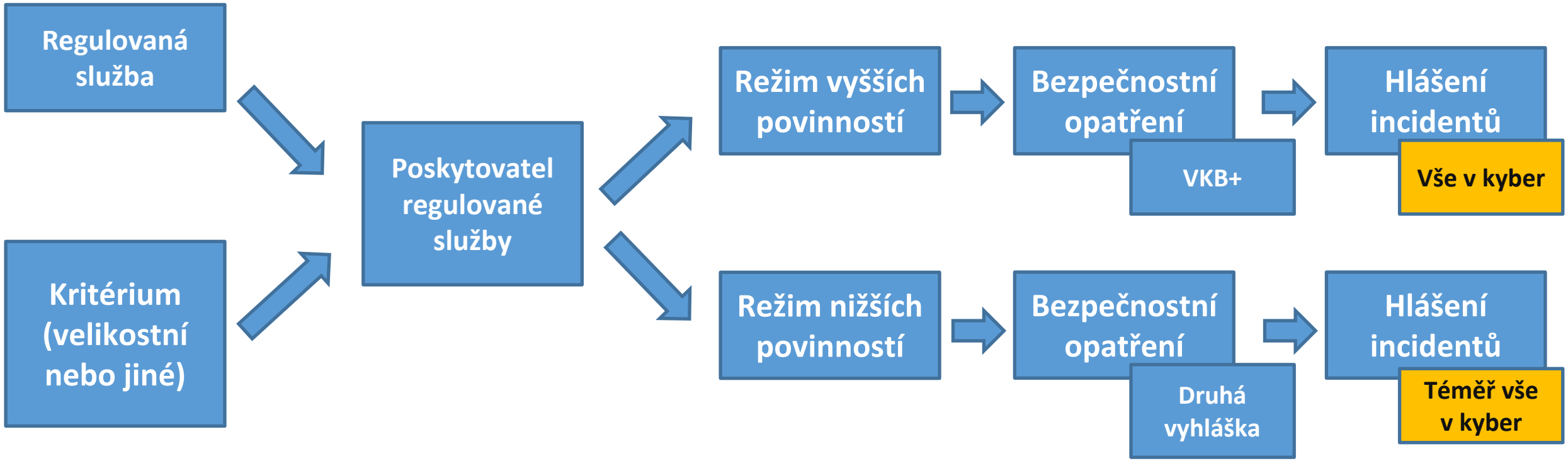
Hlásí vše
(s původem v kybernetickém prostoru)

Režim nižších povinností

Hlásí vše co je úmyslné – nehledě na význam dopadu – a to, co je významné, i kdyby to bylo neúmyslné*
(s původem v kybernetickém prostoru)

*významnost stanoví sám subjekt dle co nejjednoduššího postupu v prováděcím právním předpise

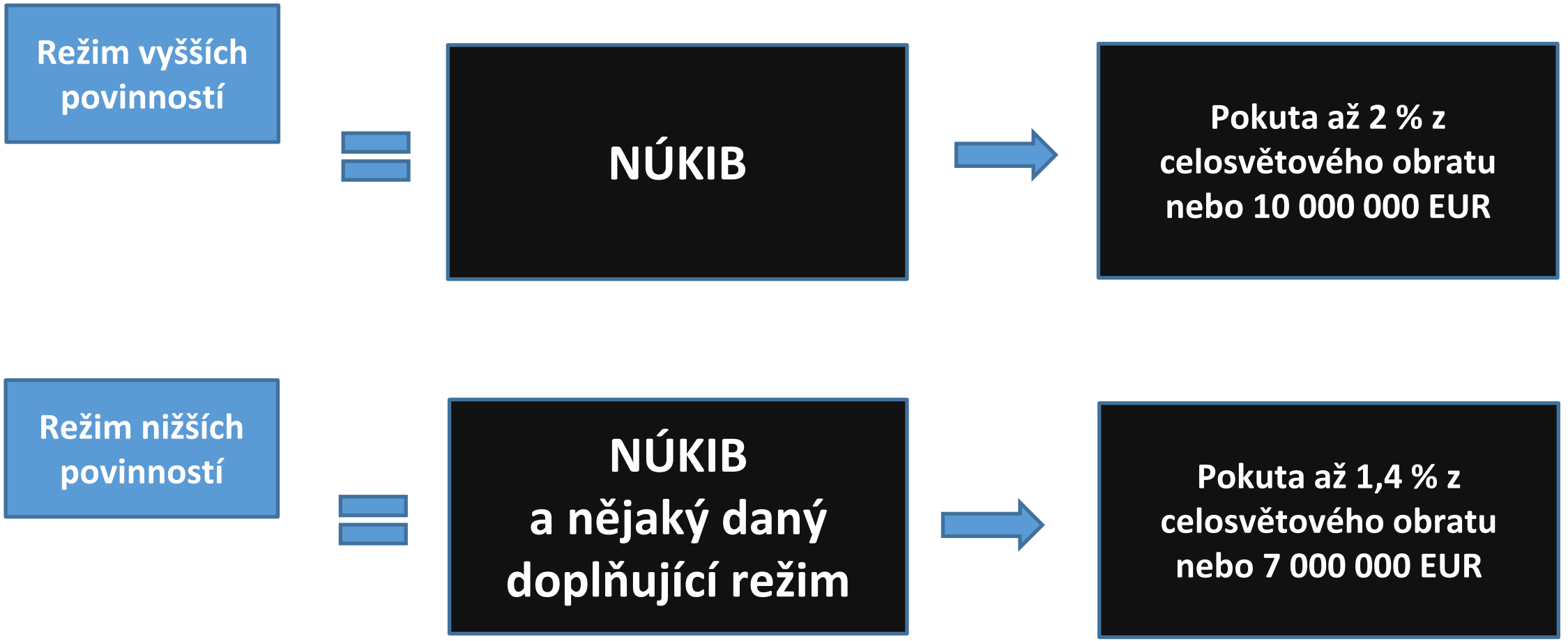
Shrnutí stanovení povinných osob



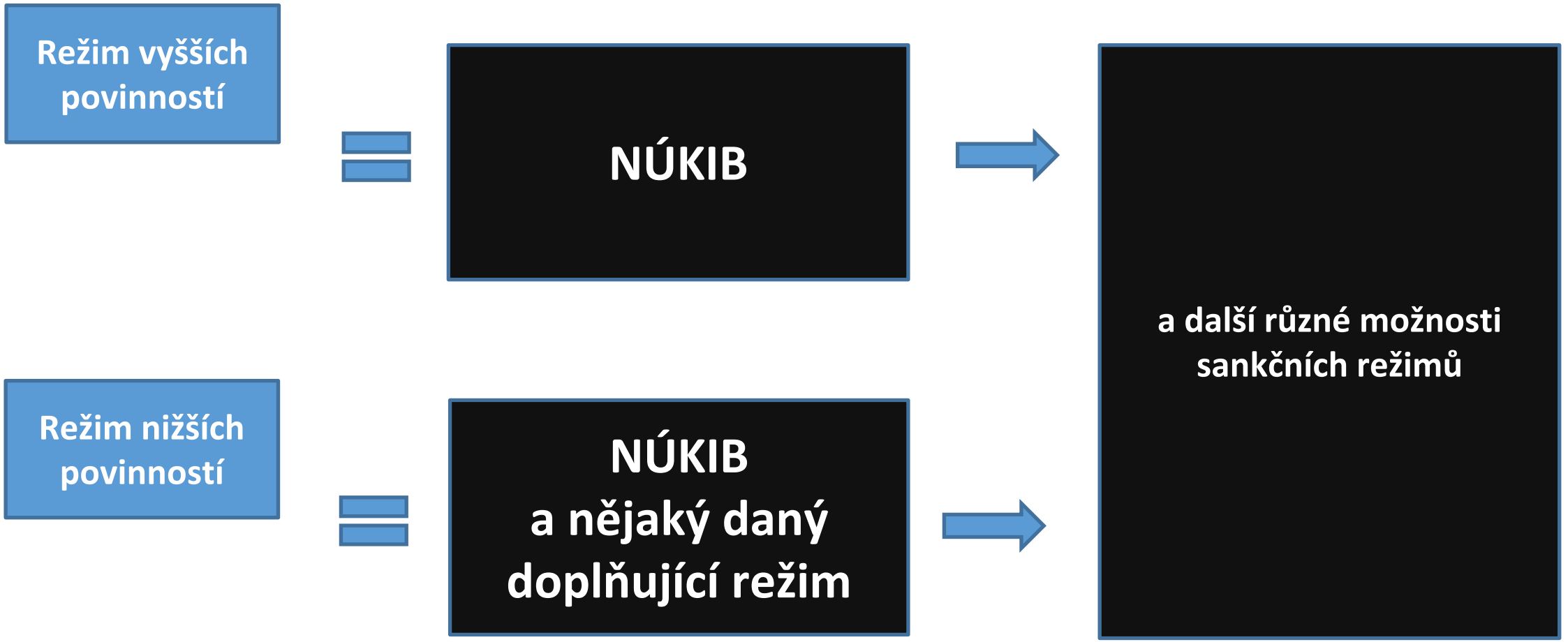
Opatření

Až na drobné, spíše procesní a textové, změny zůstávají tak jako nyní.

Kontrola a sankce



Kontrola a sankce



Registrace a komunikace s NÚKIB

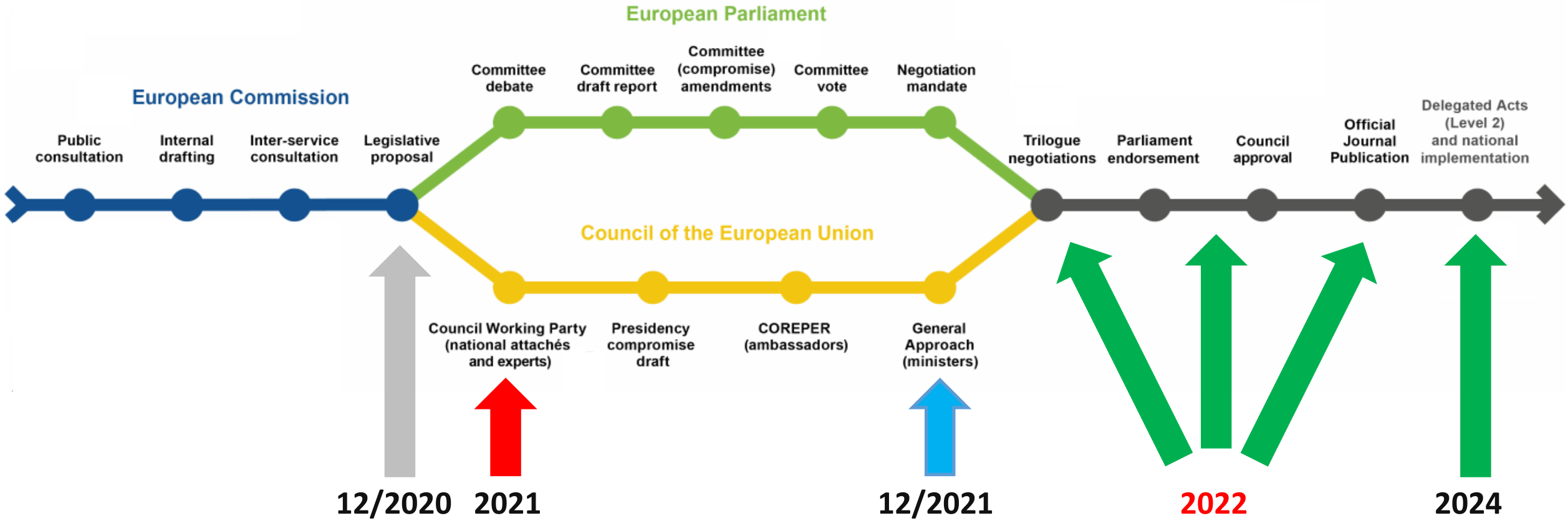
- Aby to celé fungovalo je nezbytné změnit styl, jakým dnes probíhá
  - určování povinných osob
  - hlášení kybernetických bezpečnostních incidentů
  - komunikace s Úřadem
  - sdílení informací o zranitelnostech

- 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.

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.**

One more thing...

na NÚKIB vznikla díky spolupráci odboru regulace, oddělení komunikace a oddělení vzdělávání

stránka

nis2.nukib.cz

Děkuji za pozornost!

regulace@nukib.cz