OBEC JAKO SPRÁVCE ISVS POD NOVÝMI POVINNOSTMI

Co udělat hned zítra?

KATEDRA
INFORMAČNÍCH
TECHNOLOGIÍ
PEF ČZU V PRAZE

LEGISLATIVNÍ RÁMEC

Legislativní rámec kybernetické bezpečnosti

Nejprve oddělit přímou regulaci podle ZKB od přiměřeného dopadu přes správu ISVS.

➢ Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

- Nový rámec kybernetické bezpečnosti v ČR
- Účinný od 1. 11. 2025; ruší původní zákon 181/2014 Sb.

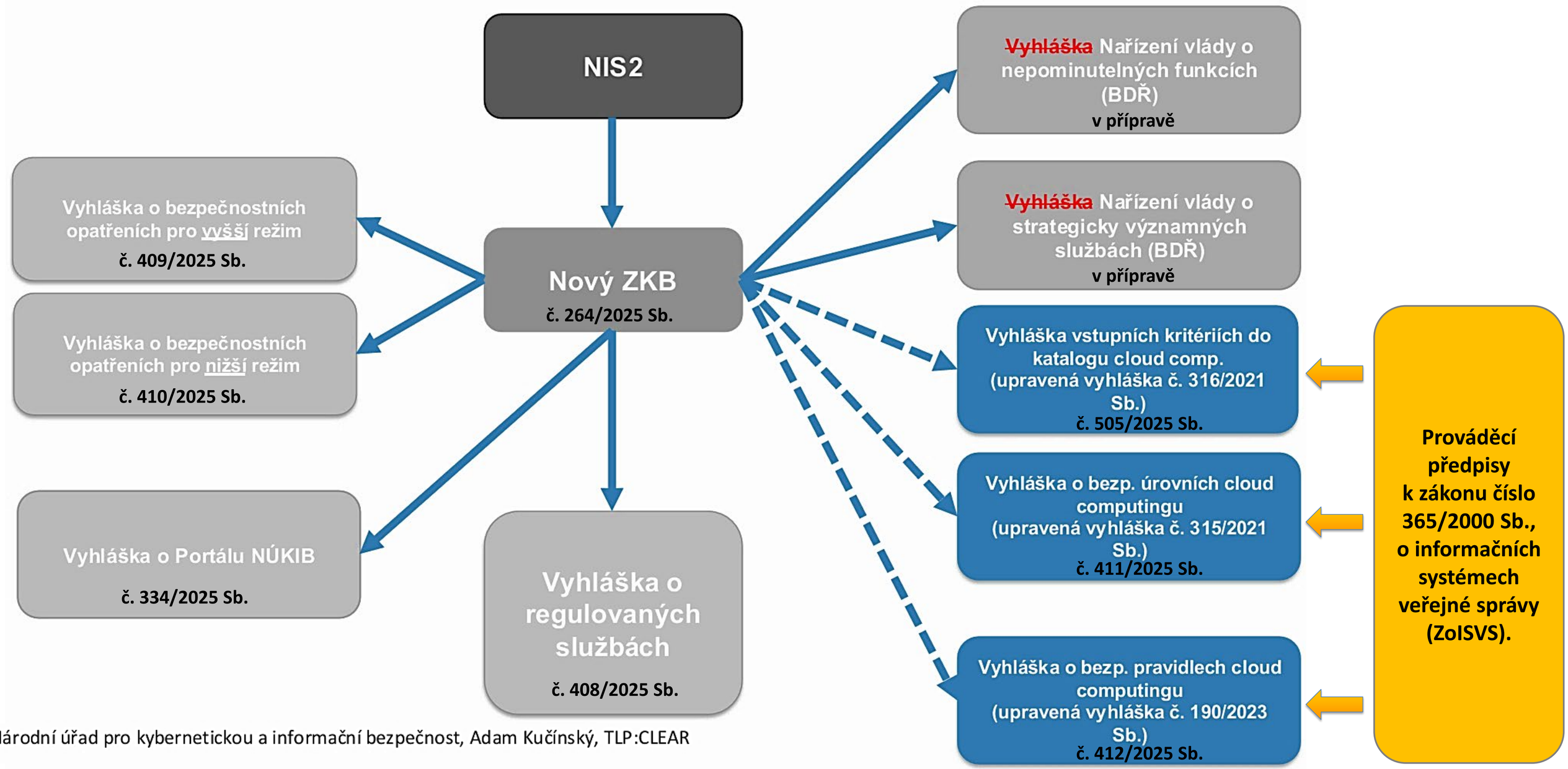
➢ Zákon č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

- Účinný od 1. 11. 2025
- V souvislosti z přijetím nového ZKB **mění 8 zákonů:** *Zákon o prověřování zahraničních investic; Zákon o Celní správě České republiky; Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, Zákon o provádění mezinárodních sankcí, Zákon o elektronických komunikacích,*
  ***Zákon o informačních systémech veřejné správy**, Zákon o poštovních službách, Zákon o bankách)*

➢ Zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře)

- Účinný od 19. 8. 2025
- Stanoví působnost státu, práva a povinnosti k zajištění poskytování „základních služeb“ a k posilování odolnosti subjektů kritické infrastruktury
- Zavádí vládní Strategii pro posílení odolnosti a vymezuje věcnou působnost rezortů, přičemž klade důraz na koordinaci s orgány dle zákona o kybernetické bezpečnost

Ekosystém nového zákona o kybernetické bezpečnosti



Režimy regulace

V ČR máme dvě úrovně regulace kybernetické bezpečnosti

KATEDRA
INFORMAČNÍCH
TECHNOLOGIÍ
PEF ČZU V PRAZE

Režimy regulace v ČR – nižší / vyšší režim

Směrnice NIS2 (EU 2022/2555) zavádí dvě kategorie regulovaných subjektů:

- Essential entities
- Important entities

→ Cílem je proporcionalita požadavků – podle velikosti, sektoru a významu služby

Česká transpozice (zákon č. 264/2025 Sb.) zavádí dvě úrovně regulace:

- Režim nižších povinností (vyhláška č. 410/2025 Sb.)
- Režim vyšších povinností (vyhláška č. 409/2025 Sb.)

Struktura bezpečnostních opatření

Vyšší režim je detailnější; nižší režim je zjednodušené minimum, nikoliv nulová povinnost.

Vyšší režim

ISMS • bezpečnostní role • aktiva • rizika • dodavatelé • změny • audit • technická dostupnost • průmyslová aktiva

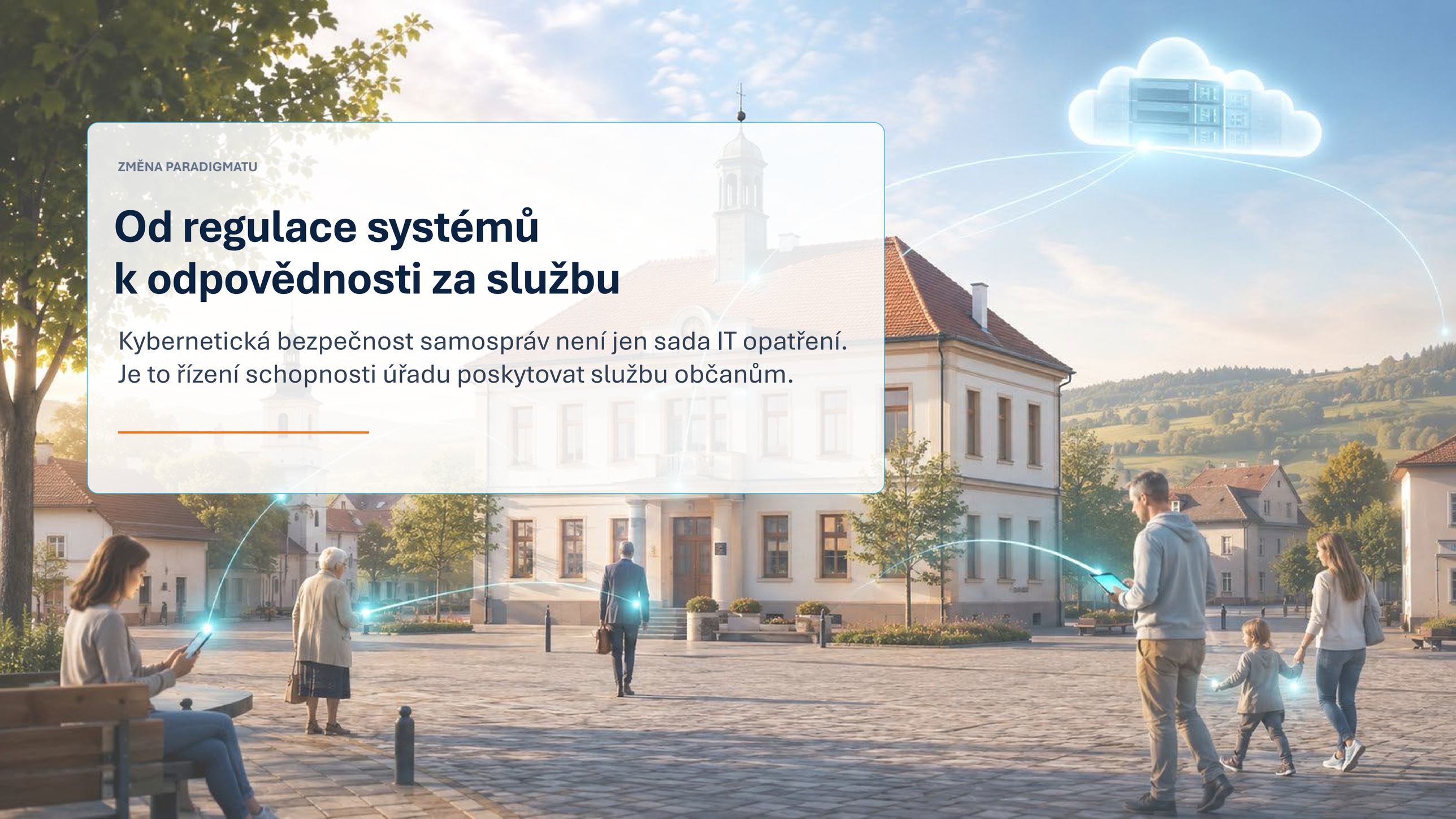
Nižší režim

přehled opatření • vedení • aktiva • lidé • kontinuita • přístupy • detekce • incidenty • sítě • aplikace • kryptografie

Důležité pro § 5b ZoISVS: správce ISVS mimo přímou regulaci aplikuje nižší režim přiměřeně k dopadům CIA, vhodnosti a proveditelnosti.

Struktura vyhlášek o bezpečnostních opatřeních

Vyšší režim (v. č. 409/2025 Sb.)	Nižší režim (v. č. 410/2025 Sb.)
Bezpečnostní opatření - organizační (§ 3–16): • Systém řízení bezpečnosti informací • Požadavky na vrcholné vedení • Stanovení bezpečnostních rolí • Řízení bezpečnostní politiky a bezpečnostní dokumentace • Řízení aktiv • Řízení rizik • Řízení dodavatelů • Bezpečnost lidských zdrojů • Řízení změn • Akvizice, vývoj a údržba • Řízení přístupu • Zvládání kybernetických bezpečnostních událostí a incidentů • Řízení kontinuity činností • Provádění auditu kybernetické bezpečnosti **Bezpečnostní opatření - technická** (§ 17–28): • Fyzická bezpečnost • Bezpečnost komunikačních sítí • Správa a ověřování identit • Řízení přístupových práv a oprávnění • Detekce kybernetických bezpečnostních událostí • Zaznamenávání událostí • Vyhodnocování kybernetických bezpečnostních událostí • Aplikační bezpečnost • Kryptografické algoritmy • Zajišťování dostupnosti regulované služby • Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	**Bezpečnostní opatření** (§ 3–13): • Systém zajišťování minimální kybernetické bezpečnosti • Požadavky na vrcholné vedení • Bezpečnost lidských zdrojů • Řízení kontinuity činností • Řízení přístupu • Řízení identit a jejich oprávnění • Detekce a zaznamenávání kybernetických bezpečnostních událostí • Řešení kybernetických bezpečnostních incidentů • Bezpečnost komunikačních sítí • Aplikační bezpečnost • Kryptografické algoritmy **Stanovení významnosti dopadu kybernetického bezpečnostního incidentu** (§ 14)



ZMĚNA PARADIGMATU

Od regulace systémů k odpovědnosti za službu

Kybernetická bezpečnost samospráv není jen sada IT opatření. Je to řízení schopnosti úřadu poskytovat službu občanům.

Změna paradigmatu

Dříve regulace vybraných IS; nyní důraz na odolnost a kontinuitu služeb.

1

Dříve
(ZKB 2014)

VIS / KII, izolovaná regulace vybraných systémů.

2

Nyní
(ZKB 2025)

Regulovaná služba, organizace, dopady a kontinuita.

3

Odpovědnost

Kybernetická bezpečnost je **agenda vedení, ne IT**.

4

Cíl

Ochrana a kontinuita činnosti, která je podstatou existence organizace
(ochrana „rodinného stříbra“, služeb, dat a důvěry.)

Oblasti regulovaných služeb dle v. č. 408/2025 Sb.– 22 skupin (102 služeb)

1. **Veřejná správa**
2. Energetika – Elektřina
3. Energetika – Ropa a ropné produkty
4. Energetika – Zemní plyn
5. Energetika – Teplárenství
6. Energetika – Vodík
7. Výrobní průmysl
8. Potravinářský průmysl
9. Chemický průmysl
10. Vodní hospodářství
11. Odpadové hospodářství
12. Letecká doprava
13. Drážní doprava
14. Námořní vodní doprava
15. Silniční doprava
16. Digitální infrastruktura a služby
17. Finanční trh
18. Zdravotnictví
19. Věda, výzkum a vzdělávání
20. Poštovní a kurýrní služby
21. Obranný průmysl
22. Vesmírný průmysl

Regulovaná služba → 1. Veřejná správa → 1.1 Výkon svěřených pravomocí

I. Poskytovatelem regulované služby v režimu vyšších povinností je

a) ústřední orgán státní správy,

b) jiný správní úřad s celostátní působností neuvedený v písmeni a),

c) ústředí, generální nebo ústřední inspektorát, generální nebo ústřední ředitelství nebo obdobná součást správního úřadu, kterým jsou podřízeny součásti správního úřadu s krajskou, okresní nebo jinou územní působností,

d) Kancelář prezidenta republiky,

e) Kancelář Senátu,

f) Kancelář Poslanecké sněmovny,

g) Česká národní banka,

h) Policejní prezidium České republiky,

i) krajské ředitelství Policie České republiky,

j) útvar Policie České republiky s celostátní působností, který zajišťuje speciální policejní činnosti v oblasti odhalování nelegální migrace, letecké služby, pyrotechnické služby, kriminalistických expertíz, ochrany ústavních činitelů České republiky, dalších určených osob a chráněných objektů nebo boje proti organizovanému zločinu, terorismu a kybernetické kriminalitě,

k) Generální inspekce bezpečnostních sborů,

l) součást Hasičského záchranného sboru České republiky podle § 5 písm. a) až c) zákona o hasičském záchranném sboru,

m) Kancelář veřejného ochránce práv a ochránce práv dětí,

n) Nejvyšší kontrolní úřad,

o) Úřad pro zastupování státu ve věcech majetkových,

p) Správa úložišť radioaktivních odpadů,

q) Ústavní soud,

r) zdravotní pojišťovna,

s) **kraj**, nebo

t) **hlavní město Praha**.

II. Poskytovatelem regulované služby v režimu nižších povinností je

a) správní úřad nebo jeho součást s krajskou, okresní nebo jinou územní působností,

b) profesní komora,

c) vysoká škola,

d) Akademie věd České republiky,

e) **obec s rozšířenou působností**, nebo

f) **městská část Praha 1 až Praha 22**.

Přímá regulace samospráv

Vyhláška č. 408/2025 Sb. řeší veřejnou správu podle typu subjektu a režimu povinností.

14
krajů včetně hl. m. Prahy
v režimu vyšších povinností

205
obcí s rozšířenou působností
v režimu nižších povinností

22
městských částí Prahy
v režimu nižších povinností

Obce I. a II. typu nejsou přímo poskytovatelem regulované služby podle nového ZoKB.

To ale neznamená, že stojí mimo nový bezpečnostní rámec.

Skrytý most: § 5b zákona č. 365/2000 Sb., o ISVS

Pokud je obec správcem alespoň jednoho ISVS, do hry vstupuje nepřímý dopad přes zákon č. 365/2000 Sb.

Zákon výslovně počítá s přiměřeností: dopad na důvěrnost, integritu a dostupnost konkrétního ISVS + vhodnost a proveditelnost opatření.

metodicky: začít plnit nejpozději do 1. 11. 2026

§ 5b ZoISVS

→ **po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti**

Správci informačních systémů veřejné správy, kteří nejsou poskytovateli regulované služby podle zákona o kybernetické bezpečnosti, jsou povinni na jimi spravované informační systémy veřejné správy zavádět bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností podle § 8, 13 a 14 zákona o kybernetické bezpečnosti, a to **přiměřeně s ohledem na možné dopady narušení důvěrnosti, integrity a dostupnosti** konkrétního informačního systému veřejné správy na činnost jeho správce a jeho schopnost poskytovat své služby občanům, a dále vhodnost a proveditelnost těchto opatření.

§ 5b ZoISVS

→ **po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti**

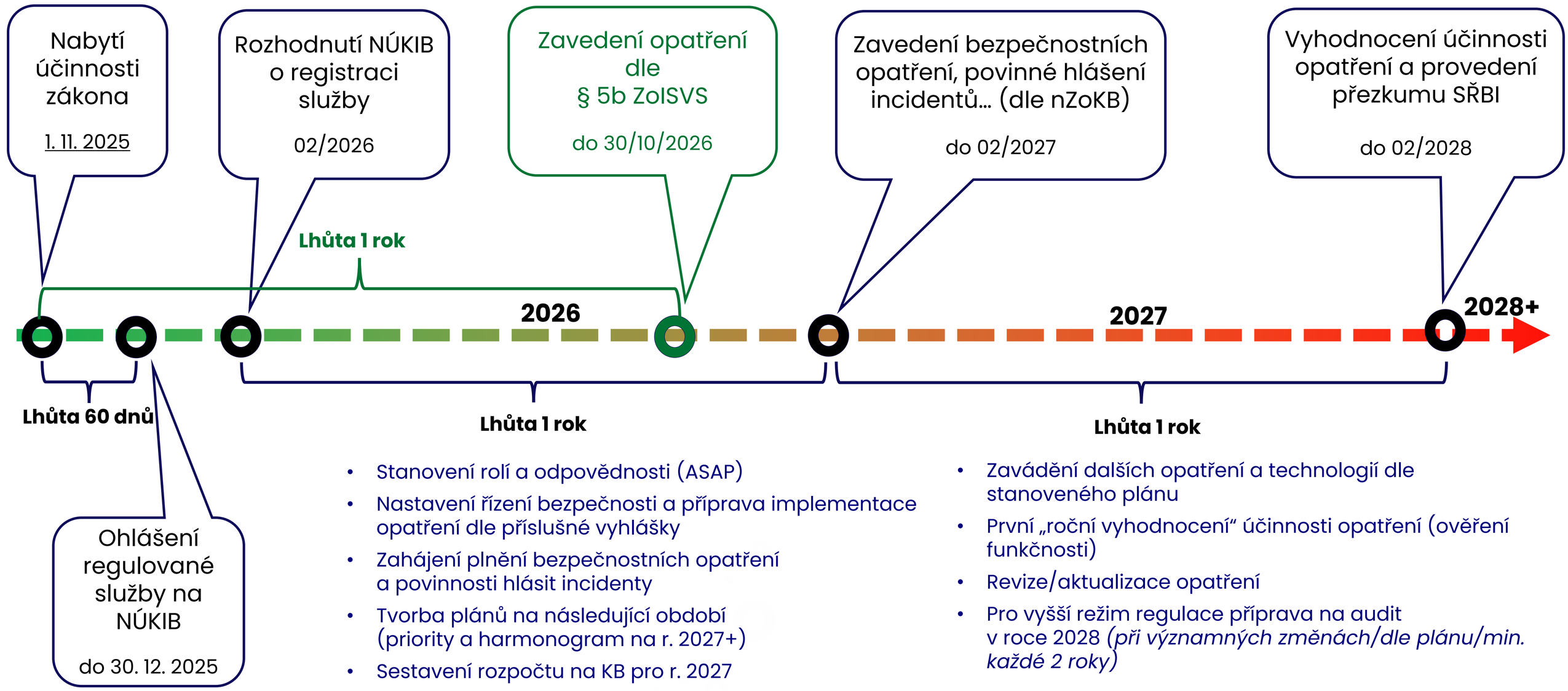
zavádět bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností podle § 8, 13 a 14 zákona o kybernetické bezpečnosti

§ 14 zákona 264/2025 Sb., o kybernetické bezpečnosti

a) systém zajišťování minimální kybernetické bezpečnosti,
b) požadavky na vrcholné vedení,
c) řízení aktiv,
d) řízení rizik,
e) bezpečnost lidských zdrojů,
f) řízení kontinuity činností,
g) řízení přístupu,
h) řízení identit a jejich oprávnění,
i) detekce a zaznamenávání kybernetických bezpečnostních událostí,
j) řešení kybernetických bezpečnostních incidentů,
k) bezpečnost komunikačních sítí,
l) aplikační bezpečnost a
m) kryptografické algoritmy.

Kroky po účinnosti nZoKB

Tento harmonogram ilustruje obecný postup implementace požadavků nového zákona o kybernetické bezpečnosti (nZoKB) pro oba režimy regulace (nižší i vyšší), při respektování rozdílného rozsahu bezpečnostních opatření.



- Stanovení rolí a odpovědnosti (ASAP)
- Nastavení řízení bezpečnosti a příprava implementace opatření dle příslušné vyhlášky
- Zahájení plnění bezpečnostních opatření a povinnosti hlásit incidenty
- Tvorba plánů na následující období (priority a harmonogram na r. 2027+)
- Sestavení rozpočtu na KB pro r. 2027
- Vzdělávání

- Zavádění dalších opatření a technologií dle stanoveného plánu
- První „roční vyhodnocení“ účinnosti opatření (ověření funkčnosti)
- Revize/aktualizace opatření
- Pro vyšší režim regulace příprava na audit v roce 2028 *(při významných změnách/dle plánu/min. každé 2 roky)*

Metodický pokyn k aplikaci § 5b zákona č. 365/2000 Sb., o informačních systémech veřejné správy

Preambule

Digitální a informační agentura vydává na základě § 4 odst. 1 písm. c) zákona č. 365/2000 Sb., o informačních systémech veřejné správy (dále také „Zákon“) tento metodický pokyn pro výkon odborných činností spojených s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy.

Účelem metodického pokynu je výklad § 5b Zákona, pokud jde o okamžik, kdy je nutné jej začít plnit.

Problematika

Ustanovení § 5b Zákona, ve znění účinném od 1. listopadu 2026, zní:

§ 5b

„Správci informačních systémů veřejné správy, kteří nejsou poskytovateli regulované služby podle zákona o kybernetické bezpečnosti, jsou povinni na jimi spravované informační systémy veřejné správy zavádět bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností podle § 8, 13 a 14 zákona o kybernetické bezpečnosti, a to přiměřeně s ohledem na možné dopady narušení důvěrnosti, integrity a dostupnosti konkrétního informačního systému veřejné správy na činnost jeho správce a jeho schopnost poskytovat své služby občanům, a dále vhodnost a proveditelnost těchto opatření.“

Pokyn

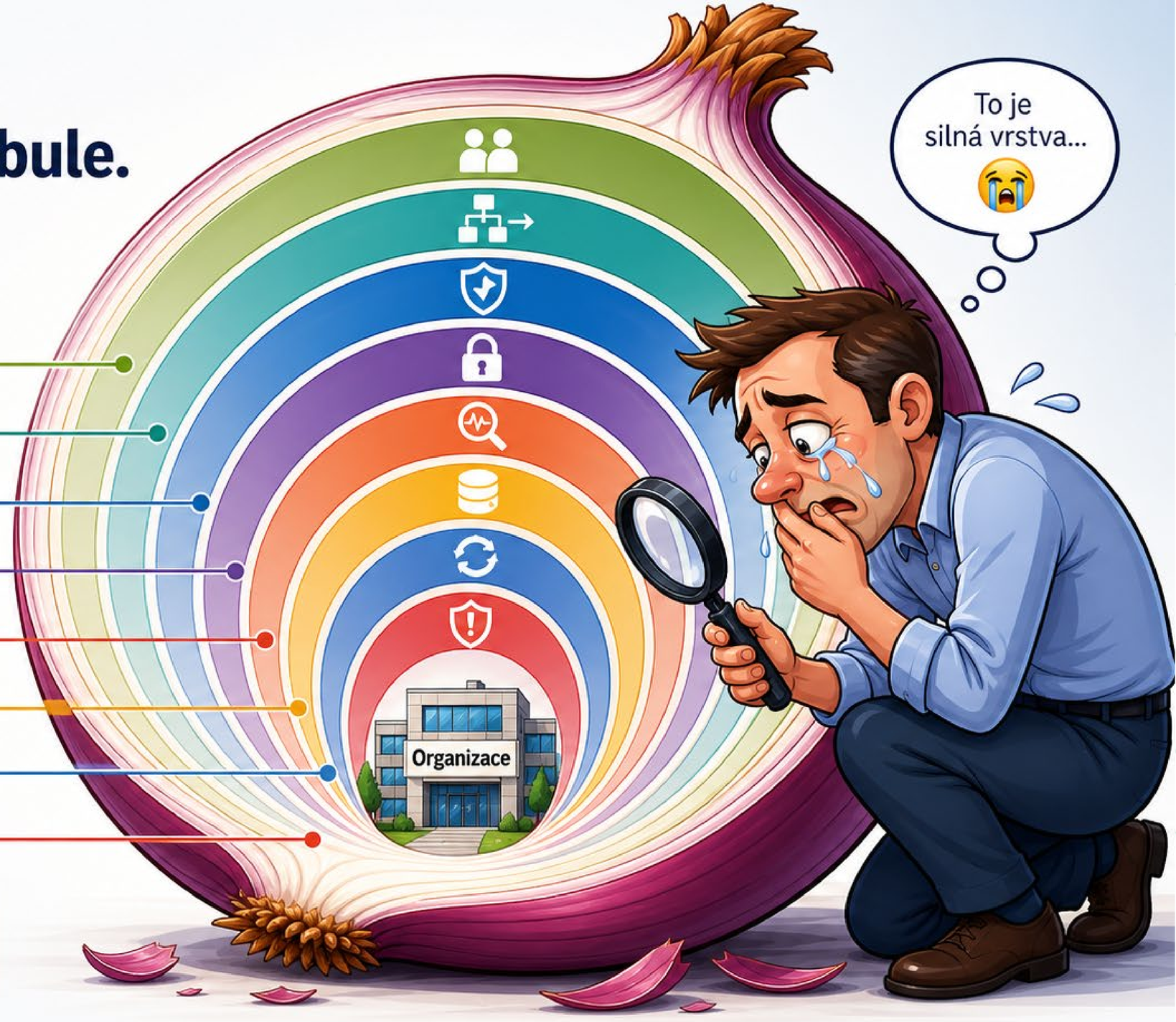
Správce informačního systému veřejné správy je povinen začít plnit povinnosti podle § 5b Zákona do 1 roku ode dne, kdy se stal správcem informačního systému veřejné správy, nejdříve však do 1 roku ode dne nabytí účinnosti § 5b Zákona, tj. do 1. listopadu 2026.

https://www.dia.gov.cz/media/3158/download/Metodicky_pokyn_k_5b_zoisvs-FINAL%283967109514%29.pdf

Zabezpečení organizace je jako cibule.

Má spoustu vrstev a když se dostanete až doprostřed, chce se vám brečet.

- Lidé
- Procesy
- Technologie
- Přístupy
- Monitoring
- Zálohy
- Kontinuita
- Reakce na incidenty



Bezpečnost je celek.

Každá vrstva má svůj význam.
Společně chrání to nejcennější – naši organizaci.

Rozsah ISMS a evidence aktiv

Směrnice NIS2 předpokládá, že bezpečnostní opatření pokryjí celou organizaci a všechny její systémy – tzv. „entity-wide ISMS“.

Jak je to v případě české transpozice NIS2?

Stanovení rozsahu řízení kybernetické bezpečnosti

§ 12 zákona č. 264/2025 Sb., o kybernetické bezpečnosti

(1) Součástí rozsahu řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“) jsou aktiva související s poskytováním regulované služby.

(2) Za účelem vymezení stanoveného rozsahu poskytovatel regulované služby
   a) určí všechna svá primární aktiva,
   b) posoudí, zda primární aktiva souvisí s poskytováním regulované služby, a
   c) u primárních aktiv podle písmene b) určí podpůrná aktiva.

(3) Poskytovatel regulované služby eviduje aktiva, která jsou součástí stanoveného rozsahu, a primární aktiva, která byla ze stanoveného rozsahu vyjmuta, včetně důvodů jejich vyjmutí.

(4) Platí, že primární aktiva, která ještě nebyla posouzena podle odstavce 2 písm. b), a podpůrná aktiva, která ještě nebyla určena podle odstavce 2 písm. c), jsou součástí stanoveného rozsahu.

(5) Stanovený rozsah je poskytovatel regulované služby povinen pravidelně přezkoumávat a aktualizovat.

*Laicky: **NIS2 míří na celou entitu a její systémy** používané pro činnost/služby (prakticky „entity-wide ISMS“). **ZKB § 12 po stanovení rozsahu umožňuje zúžit ISMS** jen na aktiva vázaná na regulovanou službu (s dočasným výchozím rozsahem „celá organizace“, dokud není rozsah formálně stanoven).*

Přestupky poskytovatele regulované služby

§ 59 zákona č. 264/2025 Sb., o kybernetické bezpečnosti

Poskytovatel regulované služby… …se dopustí přestupku tím, že

a) neohlásí změnu regulované služby podle § 9 odst. 1,

b) neohlásí kontaktní nebo doplňující údaje nebo jejich změnu podle § 11,

c) neurčí za účelem vymezení stanoveného rozsahu všechna primární aktiva podle § 12 odst. 2 písm. a) nebo podpůrná aktiva podle § 12 odst. 2 písm. c), nebo jejich určení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,

d) neposoudí za účelem vymezení stanoveného rozsahu, zda primární aktiva určená podle § 12 odst. 2 písm. a) souvisí s poskytováním regulované služby nebo toto posouzení pravidelně nepřezkoumá nebo neaktualizuje podle § 12 odst. 5,

e) neeviduje aktiva podle § 12 odst. 3, ….

Open Management for Information Security

Zadejte hledaný text

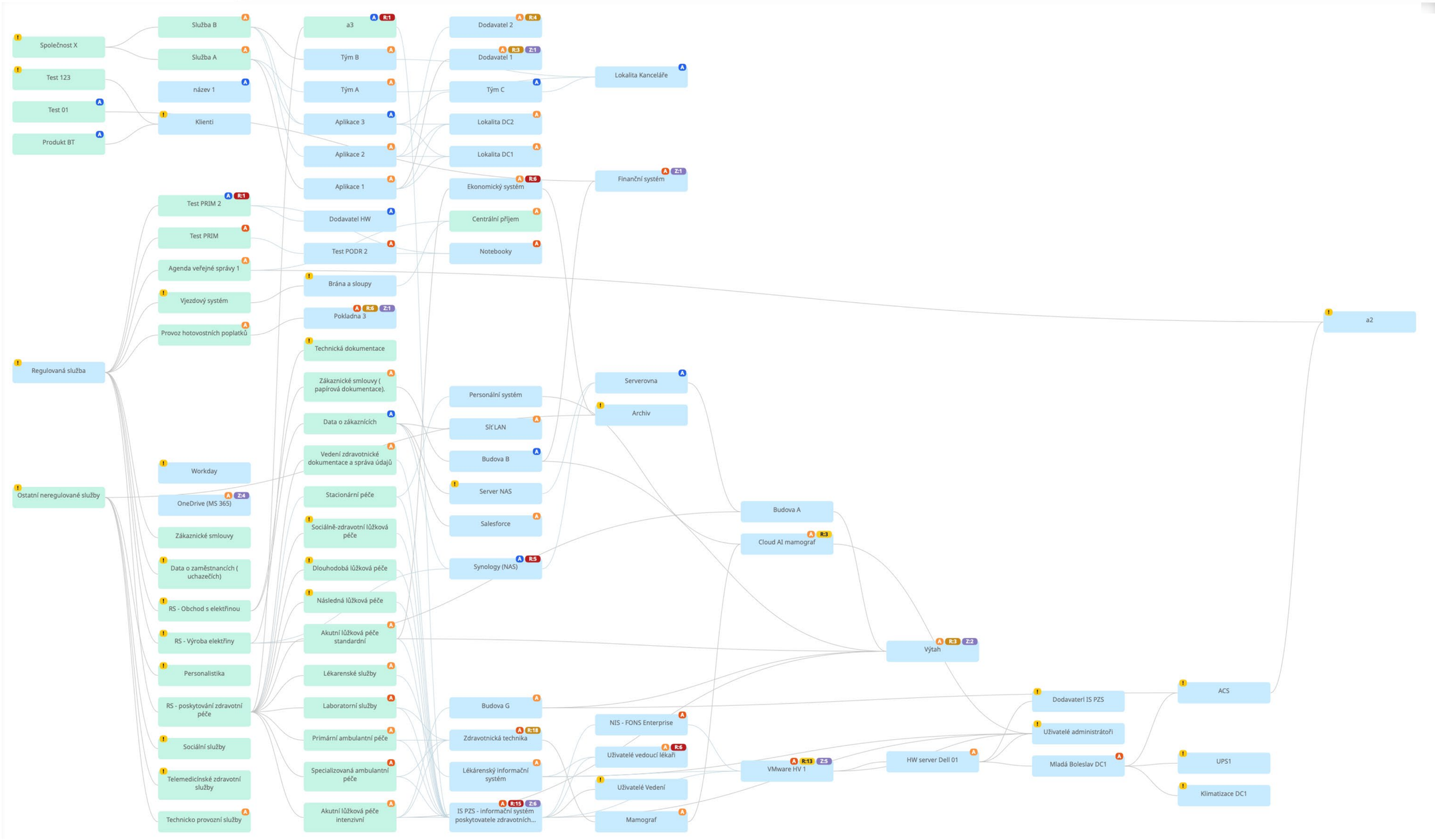
AA

- Přehled
- Aktiva
  - Seznam aktiv
  - Mapa aktiv
- Rizika
  - Seznam rizik
  - Mapa rizik
- Zvládání rizik
- Organizační struktura
- Dodavatelé
- Úkoly a události
  - Seznam úkolů
  - Seznam událostí
  - Kalendář
- Výstupy
- Zjištění
- BU / BI
- Dokumentace
- Audit

Hledat v názvech aktiv

Hloubka zobrazení 8

Filtrování aktiva | Obnovit výchozí zobrazení | + Nové aktivum



Proč nástroj místo excelu?

- Reálně **zachytí a vizualizuje víceúrovňové vazby** mezi regulovanou službou → primárními → podpůrnými → podpůrnými → podpůrnými… → …aktivy.
- Excel je plochý – víceúrovňové závislosti aktiv nezachytí.
- Rychlé **odhalení SPOF** a dopadů, přesné **zacílení a prioritizace opatření**, **auditovatelnost v čase** (verzování, integrace, reporting) **jsou zásadní**.

Život manažerů KB i garantů aktiv je příliš krátký na skládání mozaiky aktiv, rizik a hledání SPOF v Excelu — vztahy patří do vizuální mapy aktiv.

Proč nástroj místo excelu?

Život manažerů KB i garantů aktiv je příliš krátký na skládání mozaiky aktiv, rizik a hledání SPOF v Excelu — vztahy patří do vizuální mapy aktiv.

Povinnosti obcí

Nové povinnosti samospráv podle ZKB a § 5b ZoISVS

§ 11 v. č. 360/2023 Sb., o dlouhodobém řízení ISVS

Struktura provozní dokumentace

(1) Provozní dokumentaci každé etapy životního cyklu informačního systému tvoří sady dokumentací

a) plánování vytvoření a rozvoje informačního systému,
b) zadání a smluv pro vytvoření a rozvoj informačního systému,
c) stavu informačního systému při uvedení do produkčního provozu po jeho vytvoření nebo rozvoji,
d) plánu a zajišťování provozu,
e) změn informačního systému a
f) hodnocení informačního systému, včetně hodnocení ekonomické výhodnosti.

…

(3) Orgán veřejné správy zveřejňuje sady dokumentací podle odstavce 1 **způsobem umožňujícím dálkový přístup**; …

§ 12 v. č. 360/2023 Sb., o dlouhodobém řízení ISVS

Náležitosti provozní dokumentace

(1) Provozní dokumentace obsahuje

a) charakteristiku informačního systému,

b) popis architektury informačního systému,

c) podrobný popis informačního systému,

d) bezpečnostní dokumentaci,

e) provozní řád,

f) postupy a procesy související s provozem informačního systému,

g) protokoly související s provozem informačního systému a

h) smluvní a licenční dokumentaci.

§ 12 v. č. 360/2023 Sb., o dlouhodobém řízení ISVS

Náležitosti provozní dokumentace

(5) **Orgán veřejné správy, kterému nejsou uloženy povinnosti v oblasti kybernetické bezpečnosti podle zákona upravujícího kybernetickou bezpečnost, stanovuje v bezpečnostní dokumentaci alespoň postupy pro**

a) **hodnocení dopadů narušení dostupnosti, důvěrnosti a integrity informací** v informačním systému,

b) způsob řešení a **reakce na bezpečnostní události a bezpečnostní incidenty, sběr a vyhodnocování kybernetických bezpečnostních událostí a incidentů**,

c) zajištění provozu informačních systémů **a bezpečnosti informací** v informačních systémech,

d) **rozvoj bezpečnostního povědomí** a způsob jeho kontroly,

e) zajištění **bezpečnosti komunikační sítě** a

f) zajištění **řízení kontinuity činností**.

ISVS v cloudu

Cloud může malé obci pomoci pokud je pořízen a provozován jako řízená služba ISVS.

§ 6l ZoISVS: základní pravidla cloudu

Podstata právní povinnosti — § 6l odst. 3

- cloud pro ISVS nebo jeho část je **využíván na základě písemné smlouvy**
- **před uzavřením smlouvy** se ISVS nebo jeho část **zařadí do bezpečnostní úrovně**
- po celou dobu využívání cloud computingu musí být dodržována bezpečnostní pravidla
- nejde o nákup „běžného SaaS“ bez určení role, úrovně a odpovědnosti

§ **§ 6l odst. 3**

365/2000

§ 6n ZoISVS: jaký cloud lze využít

Podstata právní povinnosti — § 6n

- cloud musí umožnit **splnění požadavků informační koncepce ČR**
- musí umožnit alespoň základní úroveň ochrany důvěrnosti, integrity a dostupnosti
- musí umožnit dodržování bezpečnostních pravidel stanovených prováděcím předpisem
- **bezpečnostní úroveň cloud computingu musí být stejná nebo vyšší než úroveň ISVS / části ISVS**

§ 6n

365/2000

Bezpečnostní úroveň ISVS

Vyhláška 411/2025 Sb. pracuje s dopady incidentu v oblastech dopadu.

- úrovně: nízká, střední, vysoká, kritická
- posuzuje se nejzávažnější možný dopad v každé oblasti dopadu
- dopady mohou zasáhnout zdraví, osobní údaje, důvěryhodnost, finance nebo poskytování služeb
- výsledek určuje minimální požadavky na cloudovou službu a bezpečnostní pravidla

Oblasti dopadu								
Úroveň dopadu	**A. Bezpečnost nebo zdraví lidí**	**B. Ochrana osobních údajů**	**C. Trestní řízení a páchání trestné činnosti**	**D. Veřejný pořádek**	**E. Mezinárodní vztahy**	**F. Důvěryhodnost orgánu veřejné správy**	**G. Finanční ztráty**	**H. Zajišťování služeb**
1. Nízká	Nemůže vést k poruše zdraví jednotlivce ani skupiny lidí.	Nemůže ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, nebo může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje nejvýše dvě kritéria z první skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	Nemůže vytvořit podmínky pro páchání trestných činů přisvojení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozměnění veřejné listiny ani nemůže ztížit jejich vyšetřování.	Nemůže zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek.	Nemůže negativně ovlivnit obraz České republiky v zahraničí.	Nemůže negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností, nebo může vztahy s nimi negativně ovlivnit, avšak negativní následky mohou být nejvýše lokální.	Nemůže ani nepřímo vést k finančním ztrátám, nebo může vést k finančním ztrátám menším než 1 % běžných výdajů ročního rozpočtu orgánu veřejné správy.	Nemůže způsobit omezení, narušení nebo nedostupnost žádných poskytovaných služeb, nebo může způsobit omezení, narušení nebo nedostupnost poskytovaných služeb pro 5000 a méně osob.
2. Střední	Může vést k poruše zdraví jednotlivce nebo skupiny nejvíce 100 lidí.	Může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje tři a více kritérií z první skupiny kritérií nebo jedno kritérium z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	Může vytvořit podmínky pro páchání trestných činů přisvojení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozměnění veřejné listiny nebo může ztížit jejich vyšetřování.	Může zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek s lokálními dopady.	Může negativně ovlivnit obraz České republiky v sousedních státech.	Může negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše regionální.	Může vést k finančním ztrátám ve výši mezi 1 % a 5 % běžných výdajů ročního rozpočtu orgánu veřejné správy a tyto ztráty odpovídají částce 100000 Kč a vyšší. V případě, že výše finanční ztráty odpovídá částce nižší než 100000 Kč, použije se úroveň dopadu nízká.	Může způsobit omezení, narušení nebo nedostupnost služeb pro více než 5000, nejvíce však 50000 osob.
3. Vysoká	Může vést k poruše zdraví skupiny více než 100 lidí a nejvíce 2500 lidí nebo přímému ohrožení nebo ztrátě života jednotlivce nebo skupiny nejvíce 250 lidí.	Může negativně ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, který naplňuje dvě a více kritérií z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	Může vést k narušení vyšetřování trestné činnosti nebo k narušení soudního řízení trestního.	Může zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s regionálními dopady.	Může negativně ovlivnit obraz České republiky ve světě.	Může negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše celostátní nebo krátkodobé s mezinárodním prvkem.	Může vést k finančním ztrátám vyšším než 5 % a dosahujícím maximálně 10 % běžných výdajů ročního rozpočtu orgánu veřejné správy a tyto ztráty odpovídají částce 1000000 Kč a vyšší, nebo může způsobit hospodářské ztráty České republiky ve výši mezi 0,1 % a 0,5 % hrubého domácího produktu. V případě, že výše finanční ztráty odpovídá částce nižší než 1000000 Kč, použije se úroveň dopadu střední.	Může způsobit omezení, narušení nebo nedostupnost služeb pro více než 50000 osob.
4. Kritická	Může vést k poruše zdraví skupiny více než 2500 lidí nebo k přímému ohrožení nebo ztrátě života skupiny více než 250 lidí.	Může vést k omezení nebo narušení zpracování osobních údajů, které je nezbytné pro zajišťování obranných a bezpečnostních zájmů České republiky.	Může vést k závažnému a dlouhodobému narušení schopnosti vyšetřovat trestnou činnost nebo ke zpochybnění zákonnosti soudního řízení trestního.	Může být dotčena kritická infrastruktura provozovaná orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, zařazuje do bezpečnostní úrovně, a může zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může vést k přímému poškození nebo přerušení diplomatických vztahů České republiky se zahraničními partnery.	Může být dotčena kritická infrastruktura provozovaná orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, zařazuje do bezpečnostní úrovně, a může negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností a negativní následky mohou být dlouhodobé a s mezinárodním prvkem.	Může vést k finančním ztrátám vyšším než 10 % běžných výdajů ročního rozpočtu orgánu veřejné správy a tyto ztráty odpovídají částce 10000000 Kč a vyšší, nebo může způsobit hospodářské ztráty České republiky vyšší než 0,5 % hrubého domácího produktu. V případě, že výše finanční ztráty odpovídá částce nižší než 10000000 Kč, použije se úroveň dopadu vysoká.	Může být dotčena kritická infrastruktura provozovaná orgánem veřejné správy, který informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing, zařazuje do bezpečnostní úrovně, a může dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125000 lidí.

§ 12 zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

→ po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

Zmocňovací ustanovení

(2) Národní úřad pro kybernetickou a informační bezpečnost stanoví vyhláškou

a) požadavky na zajištění základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) a § 6n písm. b),

b) seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c), doklady o jejich splnění a intervaly pro předkládání těchto dokladů podle § 6y odst. 2,

c) požadavky na strukturu a náležitosti zprávy o provedení penetračního testu podle § 6t odst. 6 písm. d) a § 6t odst. 7 písm. e) a intervaly pro její předkládání,

d) požadavky na náležitosti auditní zprávy osvědčující existenci plánu zajištění kontinuity provozu nabízeného cloud computingu a plánu na obnovu poskytování nabízeného cloud computingu po havárii podle § 6t odst. 6 písm. e) a § 6t odst. 7 písm. f),

§ 12 zákona 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

→ po novele zákonem č. 265/2025 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

Zmocňovací ustanovení

(2) Národní úřad pro kybernetickou a informační bezpečnost stanoví vyhláškou

e) požadavky na strukturu a náležitosti dokladu o zhodnocení zdrojů rizik podle § 6t odst. 6 písm. f) a § 6t odst. 7 písm. g),

f) požadavky na strukturu a náležitosti podkladů k ověření splnění požadavku na zajištění důvěrnosti, integrity a dostupnosti informací podle § 6t odst. 6 písm. g) a § 6t odst. 7 písm. h),

g) bezpečnostní úrovně informačních systémů veřejné správy,

h) obsah a rozsah bezpečnostních pravidel pro orgány veřejné správy využívající služeb cloud computingu podle § 6l odst. 3.

Prováděcí předpisy nZoKB vztahující se na ISVS

Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy

→ č. 411/2025 Sb.

- Úprava existující vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci
- V souvislosti s přesunem zmocnění ze zákona o kybernetické bezpečnosti do zákona o informačních systémech veřejné správy dojde ke zrušení stávající vyhlášky č. 315/2021 Sb. a je tedy nutné vydat vyhlášku znovu i s úpravami, které reflektují změny definic v zákoně apod.

Vyhláška o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu

→ č. 412/2025 Sb.

- Úprava existující vyhlášky č. 190/2023 Sb.
- V souvislosti s přesunem zmocnění ze zákona o kybernetické bezpečnosti do zákona o informačních systémech veřejné správy dojde ke zrušení stávající vyhlášky č. 190/2023 Sb. a je tedy nutné vydat vyhlášku znovu i s úpravami, které reflektují změny definic v zákoně apod.

Katalog cloud computingu

Menu stránky

Na čem pracujeme

- Na čem pracujeme
- Portál občana
- CAAIS
- Doklady v mobilním telefonu
- Datové schránky
- Czech POINT
- Kompetenční centra
- eGovernment cloud

Agentura v souladu s § 6k zákona č. 365/2000 Sb., o infomačních systémech veřejné správy vede katalog cloud computingu.

Katalog cloud computingu je seznam, ve kterém se vedou údaje o:

- poptávkách cloud computingu,
- poskytovatelích cloud computingu,
- nabídkách cloud computingu a
- o cloud computingu využívaném orgány veřejné správy.

Nástroj pro vyhledávání v katalogu cloud computingu naleznete ZDE.

Údaje katalogu cloud computingu jsou veřejné s výjimkou těch, jejichž zveřejnění by mohlo ohrozit kybernetickou bezpečnost.

https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/katalog-cloud-computingu/katalog-cloud-computingu

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

ENG

KATALOG CLOUD COMPUTINGU_

Jedná se o vyhledávací nástroj nad katalogem cloud computingu, který je dostupný na webu Digitální a informační agentury.

Aktualizováno:
1. června 2026

Bezpečnostní úroveň zapsaných služeb:

- ☐ "1" - Nízká
- ☐ "2" - Střední
- ☐ "3" - Vysoká
- ☐ "4" - Kritická

Počet zapsaných poskytovatelů v katalogu:

184

Počet poskytovatelů se zapsanou nabídkou:

67

Z toho:

20

materiální poskytovatelé

Počet typů poptávaných služeb:

68

IaaS a PaaS

122

SaaS a smíšené modely

Počet zapsaných služeb v katalogu

6 842

přímý prodej služeb od přeprodejců

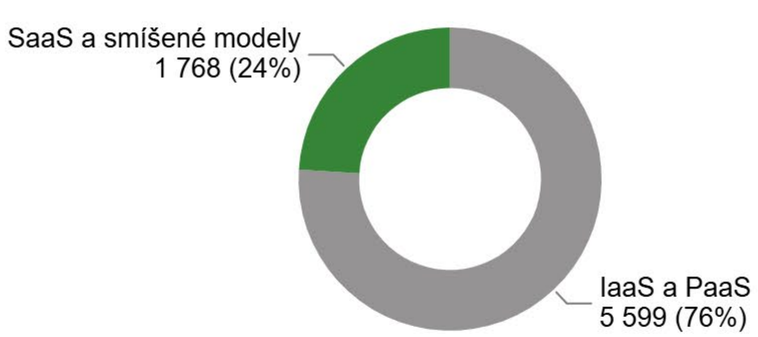
216

přímý prodej služeb od materiálních poskytovatelů

309

nepřímý prodej služeb od materiálních poskytovatelů

Počet zapsaných služeb podle unikátního ID:



Katalog služeb CC_

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

ENG

KATALOG CLOUD COMPUTINGU

Jedná se o vyhledávací nástroj nad katalogem cloud computingu, který je dostupný na webu Digitální a informační agentury.

Poskytovatelé, kteří nabízí své služby OVS přímo. Jedná se buď o materiální poskytovatele, nebo přeprodejce.

Poskytovatelé CC, kteří produkují svoje vlastní služby CC. Tyto služby mohou nabízet OVS buď přímo, nebo nepřímo (přes přeprodejce).

Aktualizováno:
1. června 2026

Bezpečnostní úroveň zapsaných služeb:

- ☐ "1" - Nízká
- ☐ "2" - Střední
- ☐ "3" - Vysoká
- ☐ "4" - Kritická

Počet zapsaných poskytovatelů v katalogu:

184

Počet poskytovatelů se zapsanou nabídkou:

67

Z toho:

20

materiální poskytovatelé

Počet typů poptávaných služeb:

68

IaaS a PaaS

122

SaaS a smíšené modely

Počet zapsaných služeb v katalogu

6 842

přímý prodej služeb od přeprodejců

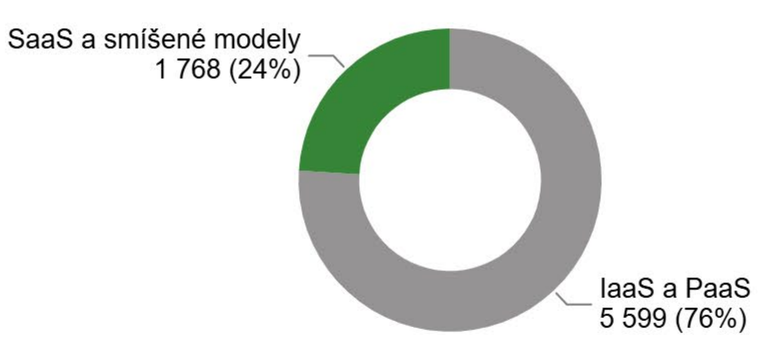
216

přímý prodej služeb od materiálních poskytovatelů

309

nepřímý prodej služeb od materiálních poskytovatelů

Počet zapsaných služeb podle unikátního ID:



Katalog služeb CC_

§ 3 vyhlášky č. 412/2025 Sb.

Požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy

- Bezpečnostní pravidla stanovují **minimální požadavky pro využívání služby cloud computingu** orgánem veřejné správy v příslušné bezpečnostní úrovni informačního systému veřejné správy.

§ 3

412/2025

Řádek	Bezpečnostní pravidlo	Bezpečnostní úroveň
1. Obecné podmínky pro službu cloud computingu		
1.1	Informace o poloze zpracování zákaznických dat Orgán veřejné správy má k dispozici dostatek jasných a srozumitelných informací o provozu služby cloud computingu, poloze zpracování zákaznických dat a rizicích souvisejících se zpracováním zákaznických dat v dané poloze pro vyhodnocení rizik pro bezpečnost informací.	nízká střední vysoká kritická
1.2	Posouzení rizika předání nebo zpřístupnění dat cizozemským orgánům Orgán veřejné správy vyhodnocuje rizika pro bezpečnost informací vyplývající z polohy zpracování zákaznických dat a specifických provozních údajů, zejména z možných žádostí cizozemských orgánů o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, a s tím souvisejícím předáním, nebo zpřístupněním zákaznických dat nebo specifických provozních údajů. Orgán veřejné správy může využívat službu cloud computingu, u které vyhodnotil rizika pro bezpečnost informací jako přijatelná. Vyhodnocení rizik orgán veřejné správy písemně	nízká střední vysoká kritická

Národní architektura veřejné správy ČR jako zdroj pravidel a povinností v oblasti správy a rozvoje IT a ISVS

KATEDRA
INFORMAČNÍCH
TECHNOLOGIÍ
PEF ČZU V PRAZE

https://archi.gov.cz

Informační koncepce ČR / Informační koncepce OVS

Zákonná povinnost:

- **Každý orgán veřejné správy (OVS)** – **tedy i každá obec** – musí mít zpracovanou a vydanou **Informační koncepci** svého úřadu (IK OVS) podle ZoISVS.

Obsah IK OVS:

- Stanovuje dlouhodobé **cíle úřadu v oblasti řízení a rozvoje ICT**, zejména **řízení kvality a bezpečnosti spravovaných systémů**.
- Vymezuje **zásady pro pořizování, vytváření a provozování ISVS.**

Informační koncepce ČR (IK ČR):

- Vládou schválený strategický dokument (usnesení č. 629/2018) definující celostátní vize, cíle a principy digitalizace veřejné správy.
- Představuje rámec eGovernmentu ČR, ke kterému se musí přihlásit všechny úřady.

https://archi.gov.cz/ikcr

Rychlá navigace

Národní architektura veřejné správy ČR
1.Architektonické dokumenty
Informační koncepce ČR
Metody řízení ICT VS ČR
Slovník pojmů eGovernmentu
Národní architektonický rámec
Národní architektonický plán
Rozšiřující znalostní báze
2.Klíčové oblasti architektury
Potřebnost a ekonomická výhodnost informačních systémů
Koncepce a strategie úřadů
Obslužné kanály veřejné správy
Elektronický oběh dokumentů
Identifikace v informačních systémech
Strukturovaná data v ISVS, datové fondy a jejich sdílení
Referenční rozhraní veřejné správy
Sdílené agendové a provozní informační systémy
Komunikační infrastruktura veřejné správy
Cloudové služby
3.Schvalování projektů a záměrů ICT
Kdo má povinnost žádat o stanovisko OHA
Co předkládat OHA ke schválení?
Jaké formuláře využít?
Jak vyplnit žádost o stanovisko?
Kde se dozvědět více informací?
Výroční zprávy o posuzování
4. Seznam reportů

Překlady této stránky: Česky (cs) English (en)

Informační koncepce ČR

Aktuální znění Informační koncepce ČR vychází z usnesení vlády č. 810 ze dne 22. října 2025.

K informační koncepci ČR se také úzce váže usnesení vlády č. 83 ze dne 05. února 2025, které přináší vůči Informačním koncepcím jednotlivých orgánů veřejné správy další povinnosti, mimo jiné:

1. Každé ministerstvo zveřejní Informační koncepci.
2. Každé ministerstvo upraví proces tvorby Informační koncepce, doplní koncepci personální politiky v oblasti ICT a konkrétní cíle.
3. Sdílet kritické role a zkušené zaměstnance a používat „klíčové zaměstnance“ u ICT specialistů, či změnit systém ohodnocení u těchto specialistů.
4. Identifikovat způsob, jak sdílet znalosti např. formou létajícího úředníka nebo etického hackera. Používat „klíčové zaměstnance“ nebo obdobné instituty podle platné legislativy u ICT specialistů v souladu s Informační koncepcí ČR a informačními koncepcemi jednotlivých úřadů. Sjednotit podmínky a výklad používání klíčových míst.

Přílohou usnesení je Závěrečná zpráva revize výdajů v oblasti ICT

Všechny povinné subjekty podle zákona č. 365/2000 Sb., o informačních systémech jsou povinny vést své vlastní informační koncepce a ty vždy uvést do souladu s Informační koncepcí České republiky. Informační koncepce České republiky je koncepcí rozvoje informačních systémů veřejné správy a eGovernmentu. Zpracovává ji Rada vlády pro informační společnost a schvaluje vláda. Je vypracována na základě ustanovení § 5a, Zákona č. 365/2000 Sb., o informačních systémech veřejné správy a jedná se o základní dokument obsahující především:

- Architektonické principy eGovernmentu a elektronizace veřejné správy
- Zásady pro řízení ICT ve veřejné správě
- Základní koncepční povinnosti pro budování, rozvoj a provoz ISVS a jejich propojování a pro budování sdílených služeb EG
- Hlavní a dílčí cíle pro efektivní rozvoj eGovernmentu a ISVS

Na této wiki je informační koncepce prezentována v jiné grafické podobě, jinak text u jednotlivých objektů je shodný se schváleným originálním dokumentem vlády.

Úvod

Působnost Informační koncepce ČR

Informační koncepce České republiky (dále také jako „IKČR“) je základním dokumentem, který stanovuje na základě zmocnění podle § 5a odst. 1 zákona 365/2000 Sb., o informačních systémech veřejné správy (dále také jako „ZoISVS“), cíle České republiky v oblasti informačních systémů veřejné správy (dále také jako „ISVS“) a obecné principy pořizování, vytváření, správy a provozování informačních systémů veřejné správy v České republice na období 5 let.

Koncepce má charakter tzv. klouzavého plánu a každé schválení aktualizace Koncepce tak znovu nastavuje její platnost na dalších 5 let, viz kap. Přehled verzí.

IKČR je závazná pro všechny subjekty, které se řídí usnesením vlády popř. jsou těmto subjektům podřízené. Je ale žádoucí, aby informační koncepce orgánu veřejné správy obsahovala uplatnění principů a zásad IKČR pro strategické řízení rozvoje informačních systémů a informatiky jako celku i v případech, kdy pro ně IK ČR není závazná.

Informační koncepce ČR / Informační koncepce OVS

Soulad IK ČR a IK OVS:

- Každá **IK OVS musí vycházet z IK ČR** a být s ní v souladu – pro jednotlivé OVS platí povinnost uvést svou koncepci **do souladu s cíli, principy a zásadami IK ČR**.
- **Lokální ICT strategie obce** tedy **navazuje na národní koncepci** a podporuje naplnění jejích cílů.

Národní architektonický plán (NAP):

- Klíčová **příloha IK ČR** – jedná se o soubor referenčních modelů a jednotných architektonických pravidel eGovernmentu.
- Vydává jej a průběžně aktualizuje Odbor hlavního architekta DIA jako navazující dokument k IK ČR
- **IK ČR spolu s NAP** stanovují **závazné principy a standardy**, které musí orgány veřejné správy respektovat při budování či **pořizování svých informačních systémů**
  (NAP například popisuje sdílené služby, datové integrace, bezpečnostní standardy apod., čímž usměrňuje rozvoj ICT ve všech úřadech v souladu s národní architekturou.)

https://archi.gov.cz/znalostni_baze:ik_ovs

Osnova vzorové informační koncepce OVS

Struktura a náležitosti Informační koncepce stanovuje vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy.

Bližší představu o obsahu informační koncepce ústředního OVS s novou strukturou lze získat např. prostudováním informačních koncepcí ústředních OVS, které již při aktualizacích svých informačních koncepcí postupují v souladu s dokumentem Metody řízení ICT VS ČR, jako je např. mj. i v přímé návaznosti na celostátní strategii Digitální Česko aktualizovaná Informační koncepce Ministerstva průmyslu a obchodu ČR

Textová verze ke stažení

Úvod

Identifikace Informační koncepce

Doplňte v případě potřeby obecný úvod o informace týkající se vašeho úřadu.

Aktuálním smyslem Informační koncepce (IK) úřadu je především stanovit jeho cíle v oblasti digitalizace a popsat, jak budou pro naplnění těchto cílů rozvíjeny informační systémy a IT služby úřadu. Stručně to shrnuje Zásada řízení ICT Z3: Strategické řízení pomocí IK OVS, která je součástí Informační koncepce ČR.

Orgán veřejné správy (OVS) vydává tuto Informační koncepci v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy (§ 5a). V Informační koncepci OVS stanovuje své dlouhodobé cíle v oblasti řízení architektury úřadu, řízení ICT služeb.

Popište vztah IK ke klíčovým strategickým dokumentům úřadu a eGovernmentu

Základní údaje Informační koncepce

Název orgánu veřejné správy	**XY**
IČO	**XXXXXXX**
Typ organizace	**Orgán státní správy**
Adresa sídla	**XYZ**

Web odboru Hlavního architekta eGovernmentu (OHA)

Národní architektonický plán

Národní architektonický plán je přílohou Informační koncepce ČR dle zákona 365/2000 Sb. a toto je základní rozcestník na jeho jednotlivé kapitoly/stránky.

Struktura NAP

1. Kapitola Úvod
2. Kapitola Architektonická vize eGovernmentu ČR
3. Kapitola Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury
4. Kapitola Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR
5. Kapitola Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí úřady
6. Kapitola Modely NAP v centrálním úložišti a v OVS

Můžete se podívat i na Náhled na celkový Národní architektonický plán složený ze všech kapitol

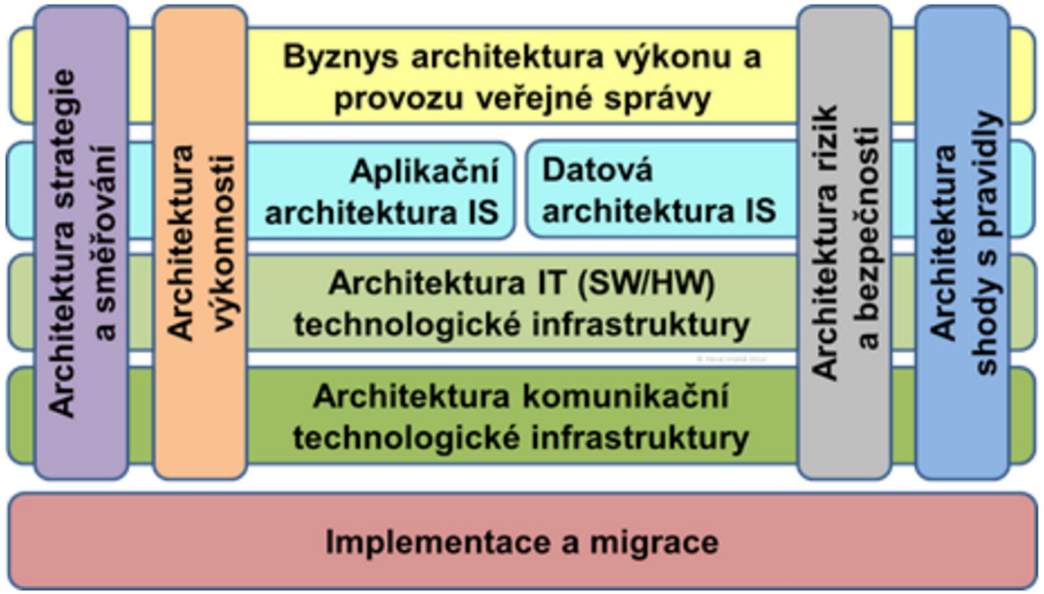
NÁRODNÍ ARCHITEKTONICKÝ PLÁN NAP

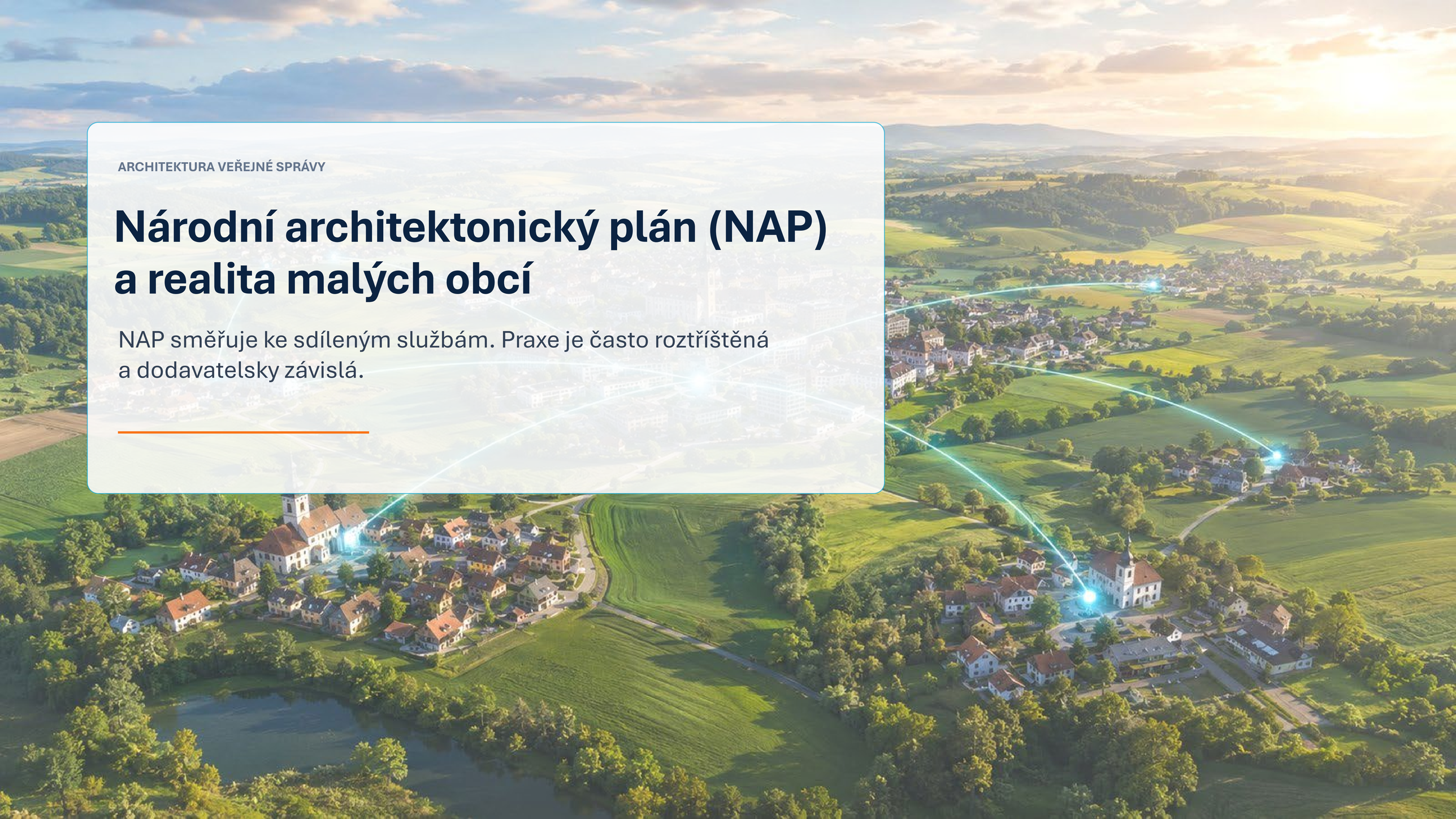
Web odboru Hlavního architekta eGovernmentu (OHA)

Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury

Tato kapitola popisuje architekturu úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu. Jde o jiný přístup k popisu požadavků na využívání systémů a služeb eGovernmentu než v části Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí jednotlivých úřadů, kde se požadavky popisují v celé šíři (v celé architektuře) sdílené služby, funkčního celky či tematické oblasti.

Skladba této kapitoly odpovídá doménám národní architektury





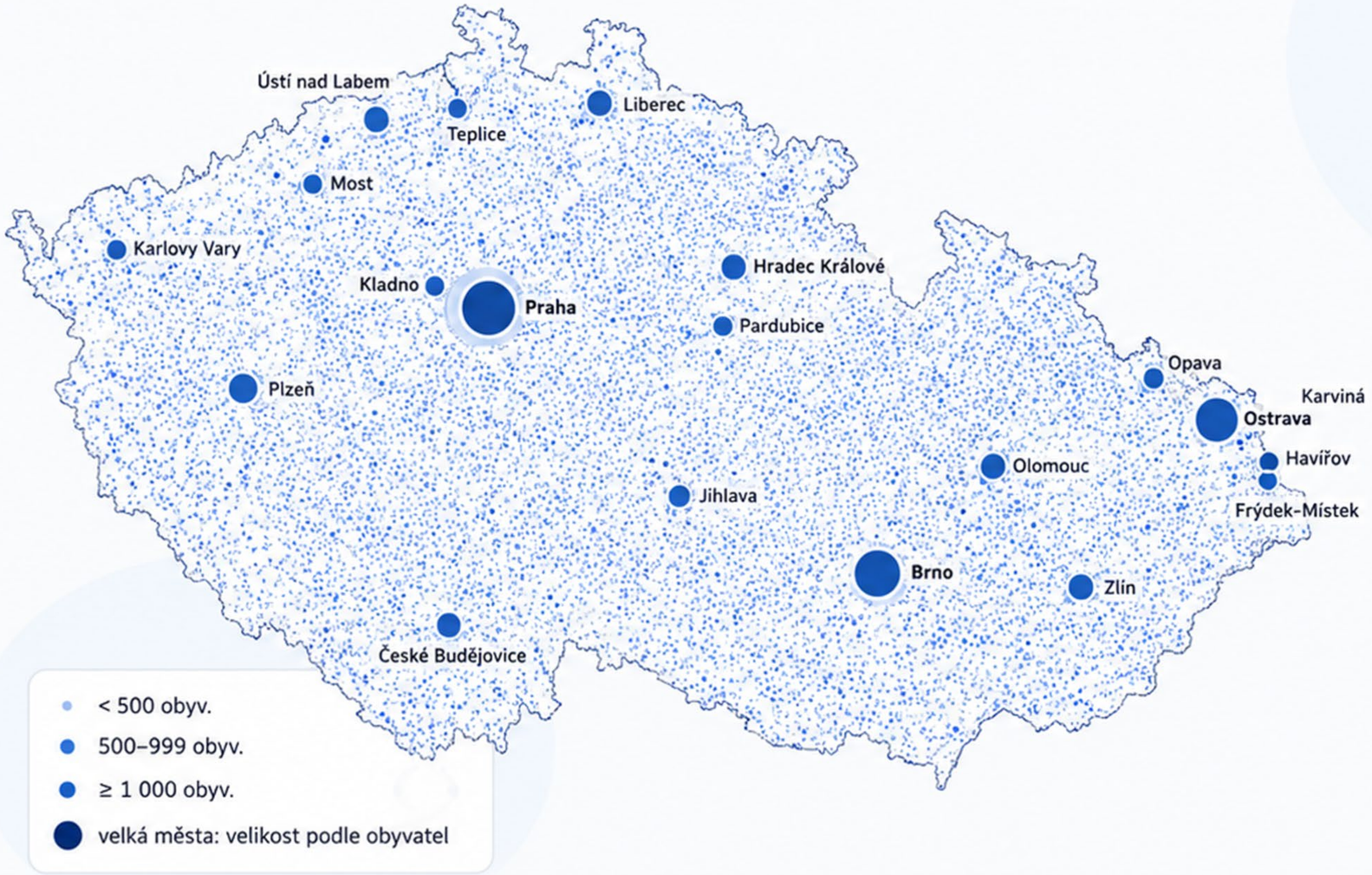
ARCHITEKTURA VEŘEJNÉ SPRÁVY

Národní architektonický plán (NAP) a realita malých obcí

NAP směřuje ke sdíleným službám. Praxe je často roztříštěná a dodavatelsky závislá.

Roztříštěné územní uspořádání ČR

Skutečné bodové polohy obcí; velikost zvýrazněných piktogramů odpovídá počtu obyvatel



Struktura obcí

Ověřeno z dat ČSÚ k 1. 1. 2025

6 258
obcí

453
medián obyvatel

75,5 %
obcí < 1 000 obyvatel
4 723 obcí

53,5 %
obcí < 500 obyvatel
7,6 % populace

Poznámka k mapě

Velikost zvýrazněných piktogramů je škálována podle počtu obyvatel. Výpočty vycházejí z dat ČSÚ k 1. 1. 2025.
Mapa zobrazuje skutečný tvar ČR a bodové umístění obcí v přibližně reálné poloze.

Zdroj dat: ČSÚ – Počet obyvatel v obcích ČR k 1. 1. 2025; ČSÚ – Struktura území podle počtu obyvatel.

Národní architektonický plán – role KÚ a ORP

Specifická pravidla pro architekturu úřadů - Pravidla pro architekturu dle velikosti a možností úřadů

Pro obce 1. a 2. typu má vize architektury veřejné správy následující podobu:

Architekturu IT úřadu obce 1. a 2. typu (do určité velikosti, viz níže) tvoří pouze koncová zařízení pro uživatele, síťovou infrastrukturu jim jako sdílenou poskytuje kraj, aplikační služby pro státní správu v přenesené působnosti poskytnou ohlašovatelé agend a aplikační služby pro samosprávní působnost poskytne vyšší stupeň územní samosprávy (ORP, kraj) jako sdílenou službu.

Pro oblast samosprávy tak vychází koncepce z následujících principů:

1. NAP je závazný pro všechny subjekty samosprávy, které mají více než 10 zařízení.
2. Informační systémy pro činnosti a agendy v přenesené působnosti přebírají v plném rozsahu od centrálních úřadů. Samosprávné činnosti si každý územněsprávní celek zajišťuje sám.
3. Subjekty s méně než 10 zařízeními si pořizují pouze uživatelský HW a SW, tj. tato koncová zařízení, **SW produkty pro výkon veřejné správy jim jako službu zajišťují subjekty, v jejichž správním obvodě leží.**

https://archi.gov.cz/nap_dokument:celkovy_dokument#specificka_pravidla_pro_architekturu_uradu

Národní architektonický plán – role KÚ a ORP

Specifická pravidla pro architekturu úřadů - Pravidla pro architekturu dle velikosti a možností úřadů

- Zákon č. 129/2000 Sb., o krajích, výslovně upravuje některé povinnosti krajů v oblasti ICT/ISVS.
- Klíčový je § 67 odst. 1, který stanoví působnost krajského úřadu v přenesené působnosti.
- Krajský úřad mj. **„poskytuje odbornou a metodickou pomoc obcím“** a dále **„zabezpečuje koordinaci výstavby a provozu informačního systému kompatibilního s informačními systémy veřejné správy“.**

https://archi.gov.cz/nap_dokument:celkovy_dokument#specificka_pravidla_pro_architekturu_uradu

Shrnutí nejdůležitějších informací

1. 11. 2025
účinnost nové úpravy

→

1. 11. 2026
počáteční společný termín
zahájení plnění § 5b

→

2027+
první reálné cykly evidence,
dokumentace, obnovy
a zlepšování

1) **I malé obce mají povinnosti podle nZoKB, pokud („jelikož“) spravují ISVS.**

2) **Malé obce (do 10 zařízení) nemají budovat vlastní ICT infrastrukturu.**

3) **Bezpečnost je jen jedna a týká se všech, bez ohledu na zákony.**
Řešit bezpečnost je pudem sebezáchovy, ne dodržováním právních norem.

Nečekat na konec přechodného období, první kroky jsou evidenční
a organizační, nikoli investiční.

Systémová doporučení

Co musí vzniknout, aby § 5b nezůstal jen formální povinností.

1	**Čistá evidence rolí**	jednoduchý postup oprav v AIS RPP a ve smluvní dokumentaci
2	**Sdílené balíčky služeb**	správa stanic, identita, zálohy, hosting, spisová služba
3	**Metodické minimum**	vzor evidence ISVS, rizik, provozní dokumentace a obnovy
4	**Nástrojová podpora**	společná evidence, úkoly, důkazy plnění, kontrolní přehledy

Bez těchto čtyř prvků vznikne spíše compliance papír než skutečná odolnost.

Prvních 180 dnů pro obec jako správce ISVS

Harmonogram pro obec, která začíná od nuly; cílem je prokazatelné řízení § 5b ZoISVS, ne „papír pro papír“.

0-30 dní
odpovědnost a rozsah

- rozhodnutí vedení + odpovědná osoba
- seznam systémů a rolí
- AIS RPP / Katalog ISVS
- dodavatelé a nouzové kontakty
- rychlá kontrola záloh a účtů

31-60 dní
evidence a závislosti

- evidence ISVS, dat, účtů a smluv
- závislosti: ICT, cloud, eSSL, ISDS
- kritické služby obce
- první C/I/A dopady podle § 5b
- rozdíly RPP vs. skutečnost

61-90 dní
rizika a plán opatření

- základní analýza rizik
- priority a plán opatření
- MFA, přístupy, zálohy, incidentní karta
- smluvní mezery a plán oprav
- zápis vedení: kdo / co / kdy / náklady

91-180 dní
provedení a důkaz

- realizace prioritních opatření
- test obnovy a revize oprávnění
- školení a poučení vedení
- provozní a bezpečnostní dokumentace
- cílový model ORP / kraj / eGC

Po 90 dnech obec nemusí být „hotová“.

Musí ale vědět, co je ISVS, kdo odpovídá, co je nejrizikovější a jaký plán je schválen.

Do 180 dnů mají být doloženy první výsledky.

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ PEF ČZU V PRAZE

Vhodný nástroj pro řízení bezpečnosti

Excel je dobrý začátek. Trvalé řízení bezpečnosti ale potřebuje evidenci, úkoly a důkazy na jednom místě.

Aktiva a ISVS	co obec spravuje a používá
Rizika a dopady	co řešit jako první
Úkoly	kdo, co, termín, stav
Dodavatelé	smlouvy, SLA, kontakty, incidenty
Důkazy	školení, revize, testy obnovy, záznamy

Doporučení: pořiďte nebo sdíleně využívejte nástroj, který vede obec krok za krokem a ukládá důkazy plnění.

Řízení kontinuity činností

Jak udržet klíčové činnosti v provozu
i při výpadku, krizi nebo narušení.

Plánování, náhradní provoz, obnova a odolnost.

Výpadek
Narušení nebo
přerušení činnosti

Dopad
Ovlivnění služeb,
procesů nebo zdrojů

Náhradní provoz
Dočasné postupy
udrží činnost v chodu

Obnova
Postupné obnovení
systémů a činností

Odolnost
Organizace je připravena
pokračovat

Pojmy

Business continuity, BIA, BCP a DRP: co je co

Nejde o synonyma; jde o navazující vrstvy jednoho řídicího řetězce.

BCM / řízení kontinuity činností

Řídicí rámec: cíle, role, politika, zdroje a rozhodování o tom, jak službu udržet nebo obnovit při narušení.

→

BIA / analýza dopadů

Vyhodnotí, co se stane se službou v čase, určí MÚPS/MBCO, RTO, RPO, priority obnovy a kritické závislosti.

→

BCP / plány kontinuity činností

Popisují, jak organizace udrží nebo obnoví regulovanou službu alespoň na přijatelnou úroveň.

→

DRP / plány obnovy

Technická vrstva: jak obnovit systémy, konfigurace, data, konektivitu a další podpůrná aktiva.

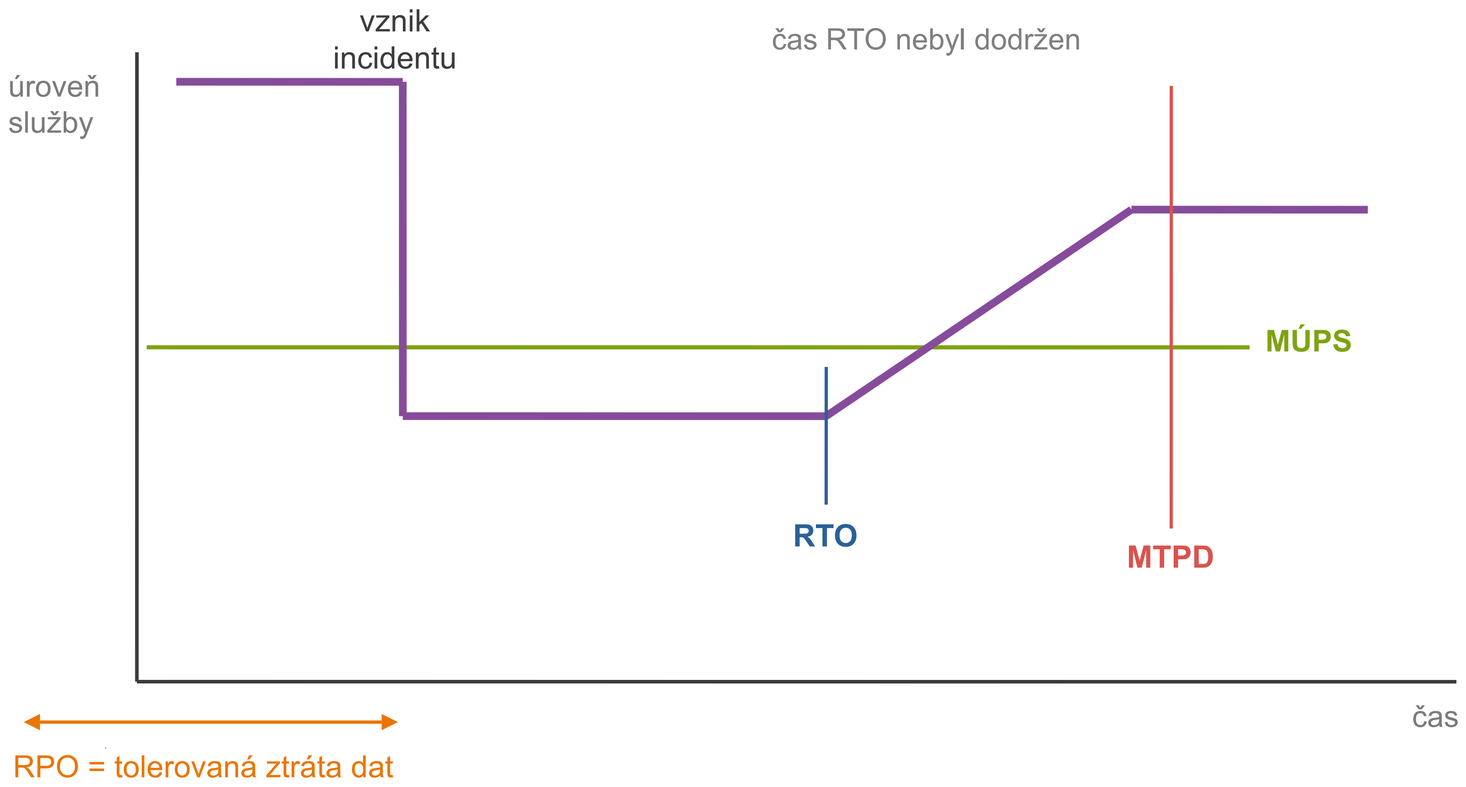
Důležité rozlišení

Incident response řeší samotný incident; business continuity drží službu pro uživatele; disaster recovery vrací do provozu technologie a data.

NGSS Next Generation Security Solutions

Pojmy

RTO, RPO, MTPD a MBCO v jedné logice



MBCO / MÚPS

Minimum Business Continuity Objective

Minimální úroveň poskytované služby, která je ještě přijatelná pro užívání, provoz a správu regulované služby (akceptovatelný degradovaný stav).

SL / ÚPS

Service Level / úroveň poskytované služby

Aktuální stav služby v čase – dostupnost, výkon, kapacita nebo kvalita vůči požadované úrovni.

RTO

Recovery Time Objective

Cílová doba obnovy: od incidentu do obnovení služby alespoň na MBCO. RTO ≤ MTPD.

RPO

Recovery Point Objective

Cílový bod obnovení dat: stav dat, k němuž se obnova vrací. Prakticky vyjadřuje tolerovanou ztrátu dat.

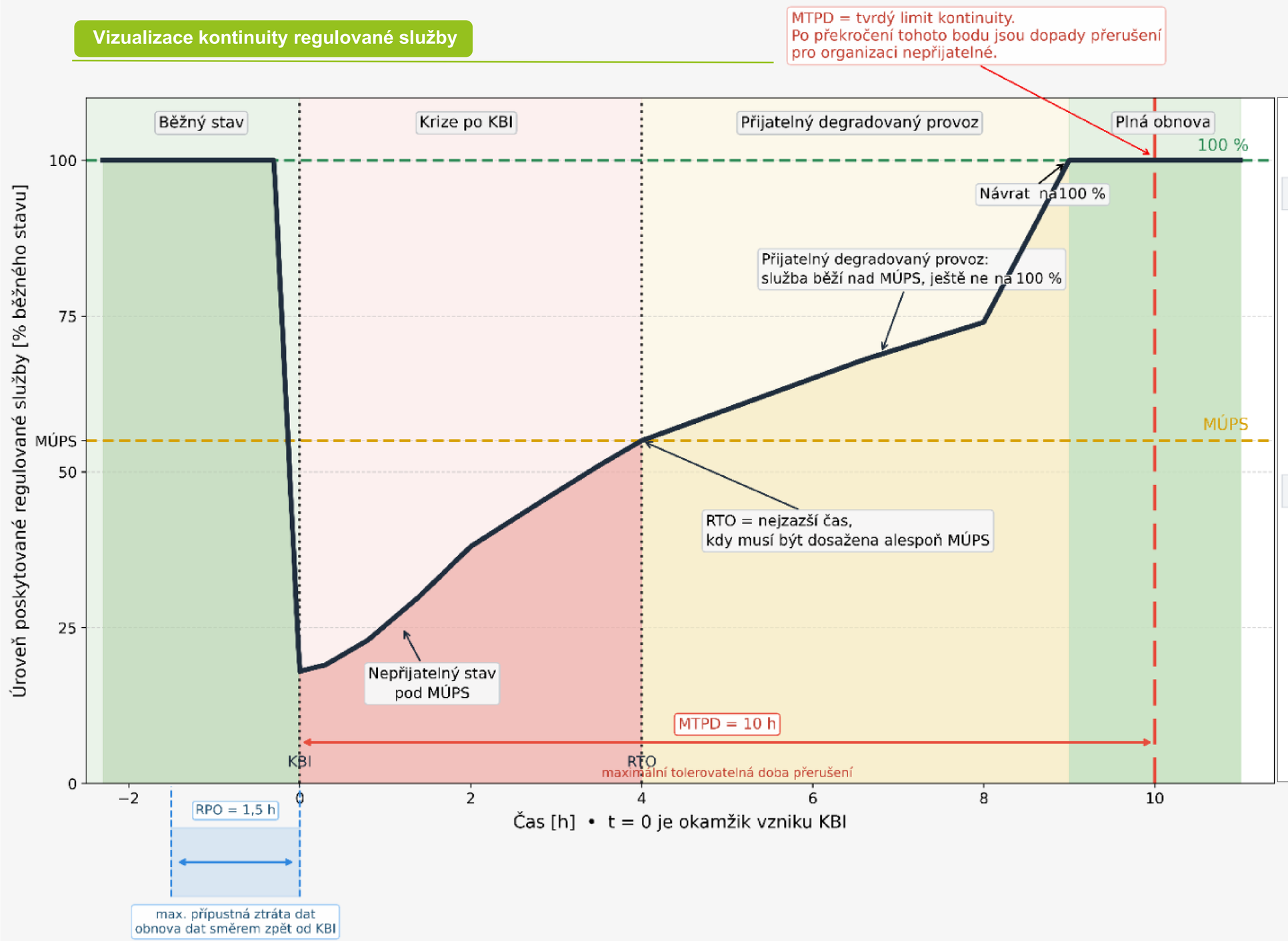
MTPD

Maximum Tolerable Period of Disruption

Nejdelší ještě tolerovatelná doba narušení. Je to horní limit kontinuity; není cílem obnovy (cílem je RTO).

Pozn.: ve vyhl. č. 409/2025 Sb. není pojem explicitně uveden.

Vizualizace kontinuity regulované služby



Legenda

vizualizace kontinuity regulované služby

Pojmy a milníky

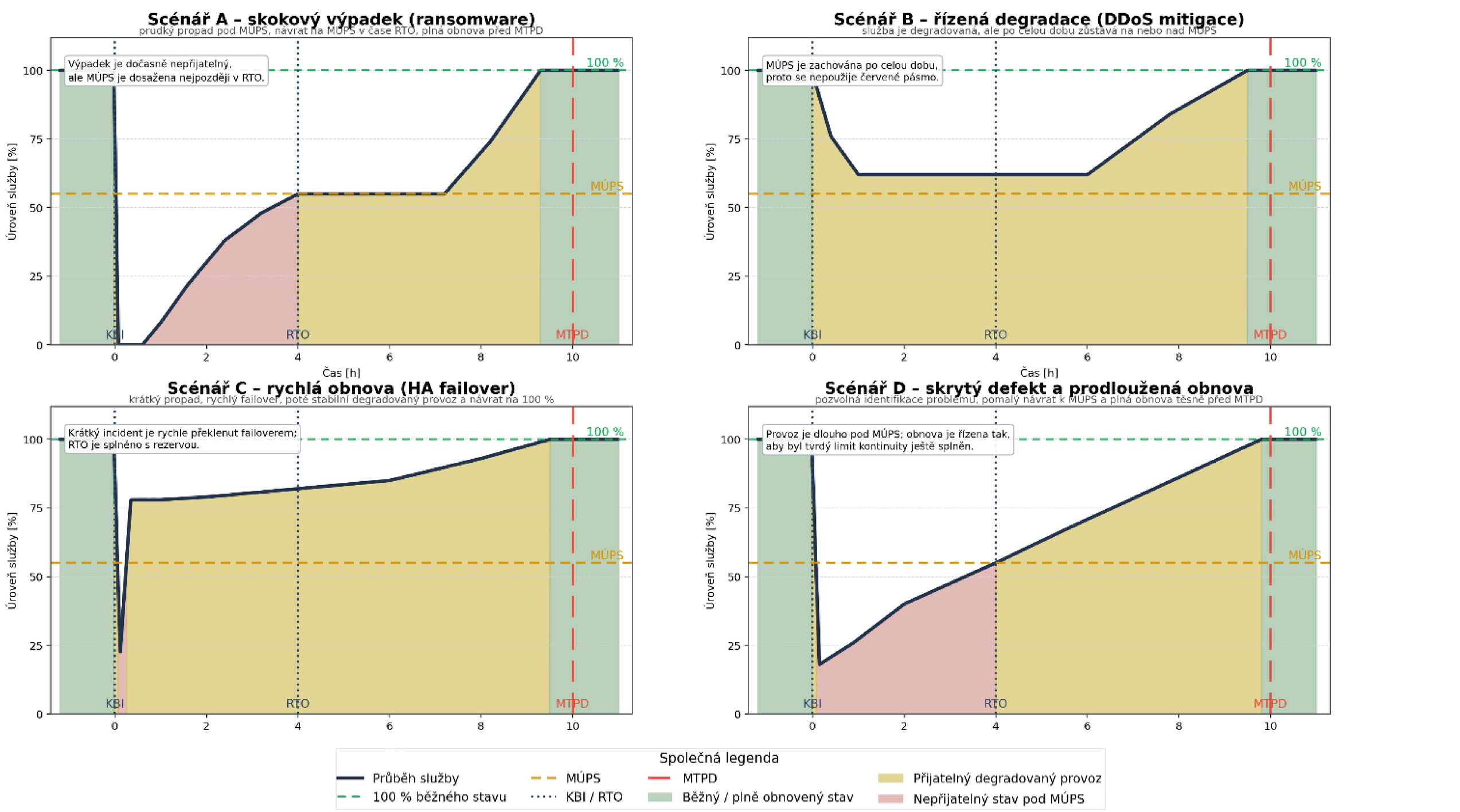
- průběh poskytované služby
- 100 % běžného stavu
- MÚPS – minimální přijatelná úroveň
- KBI / RTO – časové milníky
- MTPD – mezní tvrdý limit kontinuity
- RPO – max. přípustné okno ztráty dat

Barvy a stavy

světlý odstín = fáze • sytější odstín = aktuální úroveň služby

- běžný stav / plná obnova
- krize a aktivní obnova
- přijatelný degradovaný provoz

Modelová referenční vizualizace kontinuity regulované služby: MÚPS, RTO a RPO odpovídají logice kontinuity regulované služby; MTPD je zobrazeno jako nadřazený BCM limit.


Scénář A – skokový výpadek (ransomware)
prudký propad pod MÚPS, návrat na MÚPS v čase RTO, plná obnova před MTPD
Výpadek je dočasně nepřijatelný,
ale MÚPS je dosažena nejpozději v RTO.
100 %
MÚPS
KBI
RTO
MTPD
Úroveň služby [%]
Čas [h]
Scénář B – řízená degradace (DDoS mitigace)
služba je degradovaná, ale po celou dobu zůstává na nebo nad MÚPS
MÚPS je zachována po celou dobu,
proto se nepoužije červené pásmo.
Scénář C – rychlá obnova (HA failover)
krátký propad, rychlý failover, poté stabilní degradovaný provoz a návrat na 100 %
Krátký incident je rychle překlenut failoverem;
RTO je splněno s rezervou.
Scénář D – skrytý defekt a prodloužená obnova
pozvolná identifikace problému, pomalý návrat k MÚPS a plná obnova těsně před MTPD
Provoz je dlouho pod MÚPS; obnova je řízena tak,
aby byl tvrdý limit kontinuity ještě splněn.
Společná legenda
Průběh služby
100 % běžného stavu
MÚPS
KBI / RTO
MTPD
Běžný / plně obnovený stav
Přijatelný degradovaný provoz
Nepřijatelný stav pod MÚPS

Řízení kontinuity v režimu vyšších povinností

Jak udržet klíčové činnosti krajů v provozu i při výpadku systému

§ 14 zákona č. 264/2025 Sb. a vyhlášky č. 409/2025 Sb.

Vyšší režim = řízený systém kontinuity

Kontinuita je zde provázána s governance, riziky, aktivy, dokumentací i pravidelným ověřováním.

Vrcholné vedení

cíle, zdroje, účast na analýze dopadů, zajištění testování a přezkoumání výsledků

Manažer KB

řídí ISMS a pravidelně informuje vedení

Architekt KB

zajišťuje bezpečnou architekturu regulované služby

Garant aktiva

odpovídá za rozvoj, použití a bezpečnost aktiva

Auditor KB

nezávisle ověřuje správnost a účinnost opatření

Povinné výstupy, se kterými vedení a osoby v bezpečnostních rolích pracují

zpráva z hodnocení rizik, plán zvládání rizik, prohlášení o aplikovatelnosti, výsledky BIA, plány kontinuity obnovy, výsledky testů a auditů

Vyšší režim staví kontinuitu na správě a řízení: bez účasti vedení, rolí a přezkumu nejde o funkční systém.

NGSS Next Generation Security Solutions

§ 4 vyhlášky č. 409/2025 Sb.

Požadavky na vrcholné vedení

(1) Statutární orgán nebo jiná osoba nebo skupina osob v obdobném postavení (dále jen **„vrcholné vedení“**) s ohledem na systém řízení bezpečnosti informací

h) se podílí na **vypracování analýzy dopadů** podle § 15,

i) zajistí **testování plánů kontinuity činností**, **plánů obnovy** a procesů spojených se zvládáním kybernetických bezpečnostních incidentů,

NGSS Next Generation Security Solutions

§ 15 vyhlášky 409/2025: Řízení kontinuity činností

Povinná osoba při řízení kontinuity činností

a) stanoví metodiku pro **provedení analýzy dopadů**, **BIA**

b) provádí analýzu dopadů, vyhodnocuje a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 8,

BCM

c) na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) **stanoví cíle řízení kontinuity činností** formou určení

MBCO 1. **minimální úrovně poskytovaných služeb**, která je přijatelná pro užívání, provoz a správu regulované služby,

RTO 2. **doby obnovení chodu**, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby, a

RPO 3. **bodu obnovení dat** jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání technického aktiva,

d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c), a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,

e) vypracuje, aktualizuje a pravidelně testuje **plány kontinuity činností** a **plány obnovy související** s poskytováním regulované služby a

BCP **DRP**

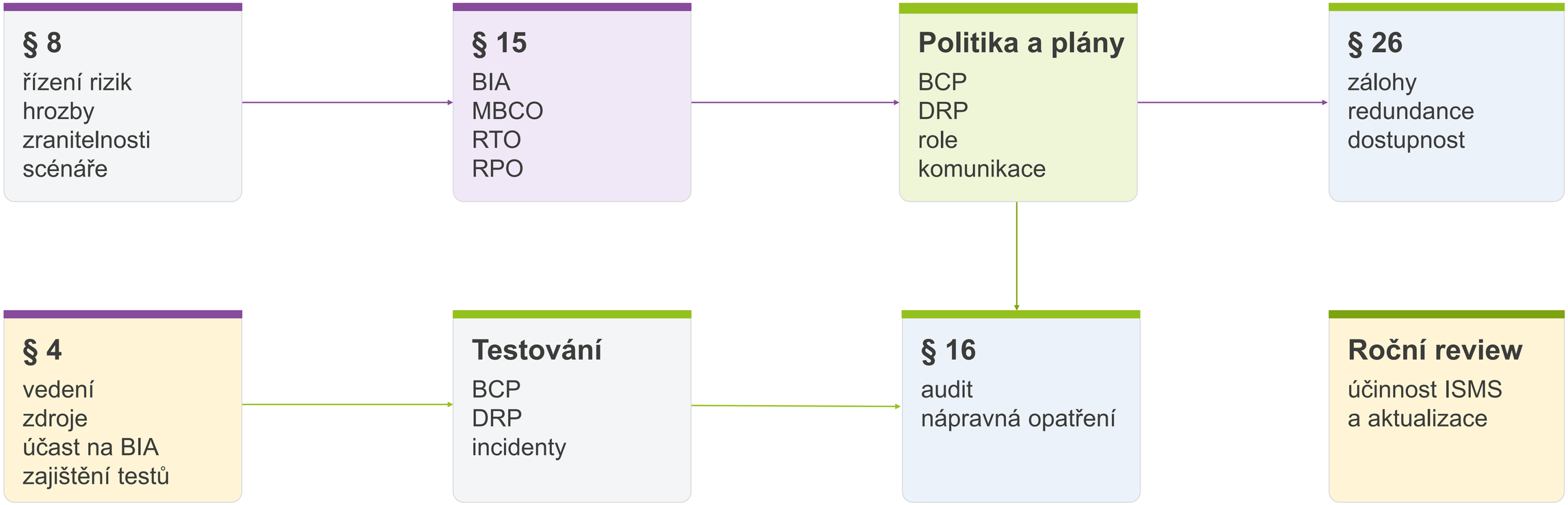
f) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 26.

NGSS Next Generation Security Solutions

VYŠŠÍ POVINNOSTI

Jak na sebe § 4, § 8, § 15, § 16 a § 26 navazují

Samotný § 15 dává smysl teprve ve vazbě na vedení, rizika, audit a technickou dostupnost.



Výstup BIA má být použitelný pro rozhodnutí vedení, plány, testování i technická opatření dostupnosti.

NGSS Next Generation Security Solutions

Řízení kontinuity v režimu nižších povinností

Jak udržet klíčové činnosti obce v provozu i při výpadku systému

§ 14 zákona č. 264/2025 Sb. a vyhláška č. 410/2025 Sb.

§ 4 vyhlášky č. 410/2025 Sb.

Požadavky na vrcholné vedení

Statutární orgán povinné osoby nebo jiná osoba anebo skupina osob v obdobném řídícím postavení povinné osoby (dále jen **„vrcholné vedení“**) s ohledem na zajišťování minimální kybernetické bezpečnosti

f) **stanoví prioritu obnovy primárních aktiv.**

NGSS
Next Generation
Security Solutions

§ 6 vyhlášky č. 410/2025 Sb.

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

a) **stanoví prioritu technických aktiv, pořadí a postupy jejich obnovy a zohlední přitom stanovenou prioritu relevantního primárního aktiva** podle § 4 písm. f),

b) **stanoví povinnosti a odpovědnost konkrétních osob za jednotlivé činnosti pro zajištění kontinuity činností a k obnově** podle písmene a) a

c) vytváří **pravidelné zálohy** informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména **pro účely obnovy regulované služby** pro případ kybernetického bezpečnostního incidentu.

NGSS Next Generation Security Solutions

KYBERNETICKÁ BEZPEČNOST V SAMOSPRÁVĚ JE JAKO EMENTÁL!

POKLÁDÁME PLÁTKY (KOMBINUJEME OPATŘENÍ) TAK, ABYCHOM PŘEKRYLI DÍRY A DOSÁHLI CELKOVÉ BEZPEČNOSTI.

MĚNĚ RIZIK
Každá vrstva snižuje pravděpodobnost vzniku incidentu.

KOMBINACE OPATŘENÍ
Žádná vrstva není dokonalá, ale společně fungují.

OCHRANA SLUŽEB
Chráněná data, systémy a důvěra občanů.

ODOLNÁ SAMOSPRÁVA
Bezpečný úřad = spolehlivě sloužící veřejnosti.

Vaše dotazy ?

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ PEF ČZU V PRAZE

Ing. Miroslav Pavelka, pavelka@pef.czu.cz

Zdroje a doporučené materiály

PODKLAD

Pavelka, M.; Jarolímek, J.: Nové povinnosti tisíců obcí v oblasti bezpečnosti po novele ZoISVS. Sborník ISSS 2026, str. 53.
Zákon č. 264/2025 Sb., o kybernetické bezpečnosti; zákon č. 265/2025 Sb.; zákon č. 365/2000 Sb.
DIA: Metodický pokyn k aplikaci § 5b zákona č. 365/2000 Sb.
NÚKIB: Manuál pro poskytovatele regulovaných služeb v režimu nižších povinností; podpůrné materiály pro obce.
Vyhlášky č. 408/2025 Sb., 410/2025 Sb., 411/2025 Sb., 412/2025 Sb.; vyhláška č. 360/2023 Sb.
AIS RPP Působnostní / Katalog ISVS.
Národní architektonický plán a archi.gov.cz.