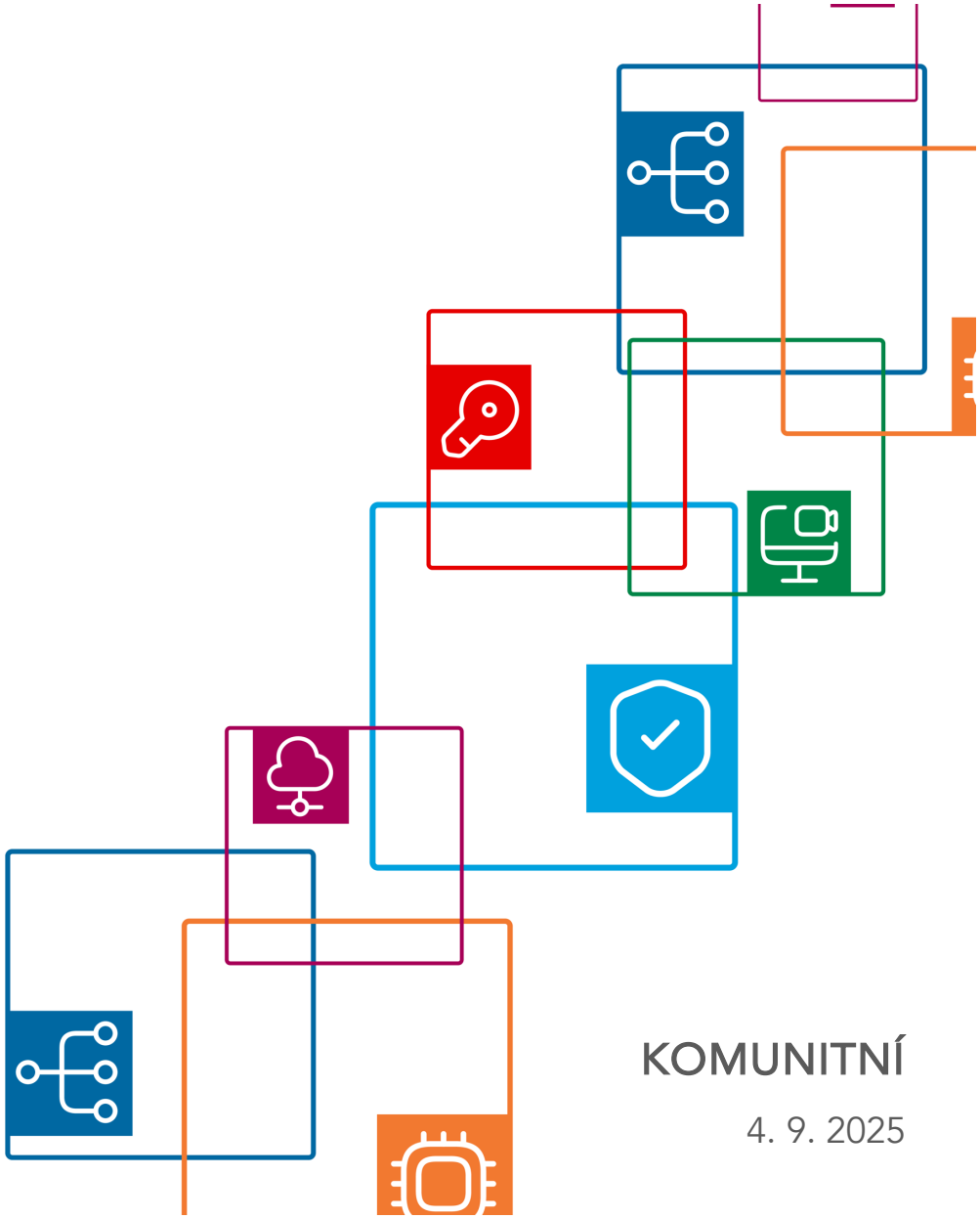
cesnet

nZKB v teorii a praxi

A. Kropáčová, M. Pospíšilová

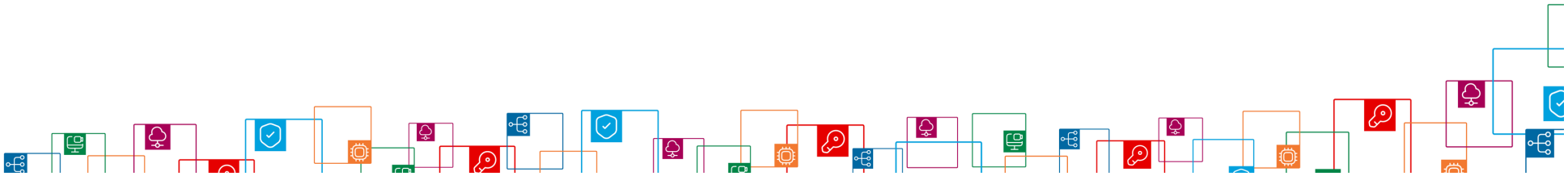


KOMUNITNÍ

4. 9. 2025

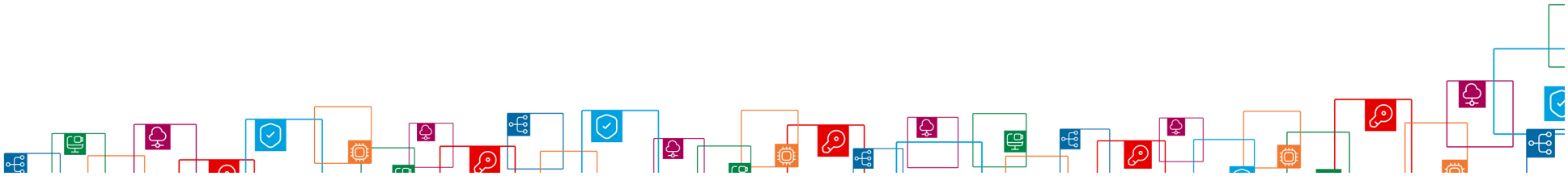
Slovo úvodem

- cíle a struktura našich WS
- nabízíme pohled MKB a compliance manažera organizace, na který zákon 100% dopadne
- naše zkušenosti:
  - zavádění ISMS a compliance programu
  - souladění s GDPR, stávajícím ZKB atd.



historie zavedení ISMS v CESNET

- 2014: Rozhodnutí představenstva sdružení CESNET zavést ISMS
  - reakce na připravovaný zákon o kybernetické bezpečnosti
  - scope – jedna oblast nebo všechno? Všechno.
  - MKB: nový zaměstnanec, AKB: stávající zaměstnanec
- Dilema: Norma nebo ZKB?
  - Pojedeme podle ZKB a doplníme prvky ISMS
  - ... a nakonec jsme jeli podle normy a doplnili povinnosti ZKB
- Základ: Pravidelné rozhovory s vedoucími pracovníky, databáze aktiv a analýza rizik
- 6/2018: Certifikace ISMS
- 1/2022: Subjektem KII



Panika?

- nová legislativa v oblasti KB je velké téma (NIS2 z konce roku 2022) – široce diskutovaná problematika
- nyní čas na praktické kroky, CESNET nabízí pomoc:
  - sdílení zkušeností
  - návody
  - vzory dokumentů

- bez platných vyhlášek nemáme 100% jasno o úplně všech požadavcích, které máme plnit

X **máme platný nZKB a z něj jsou základní požadavky patrné**

- bez vyhlášek fakticky nelze realizovat kroky požadované nZKB

X **máme 7 kroků, které lze realizovat ještě před vydáním vyhlášek (a několik dalších, které lze realizovat před jejich účinností)**

Proces souladňování s nZKB

máme platný nZKB

1. Seznámit se s problematikou nZKB
2. Sestavit tým
3. Identifikovat požadavky nové legislativy
4. Provést gap analýzu
5. Sestavit seznam opatření a harmonogram
6. Informova/zapojit vedení organizace
7. Nachystat politiku KB v organizaci

máme platné nVKB

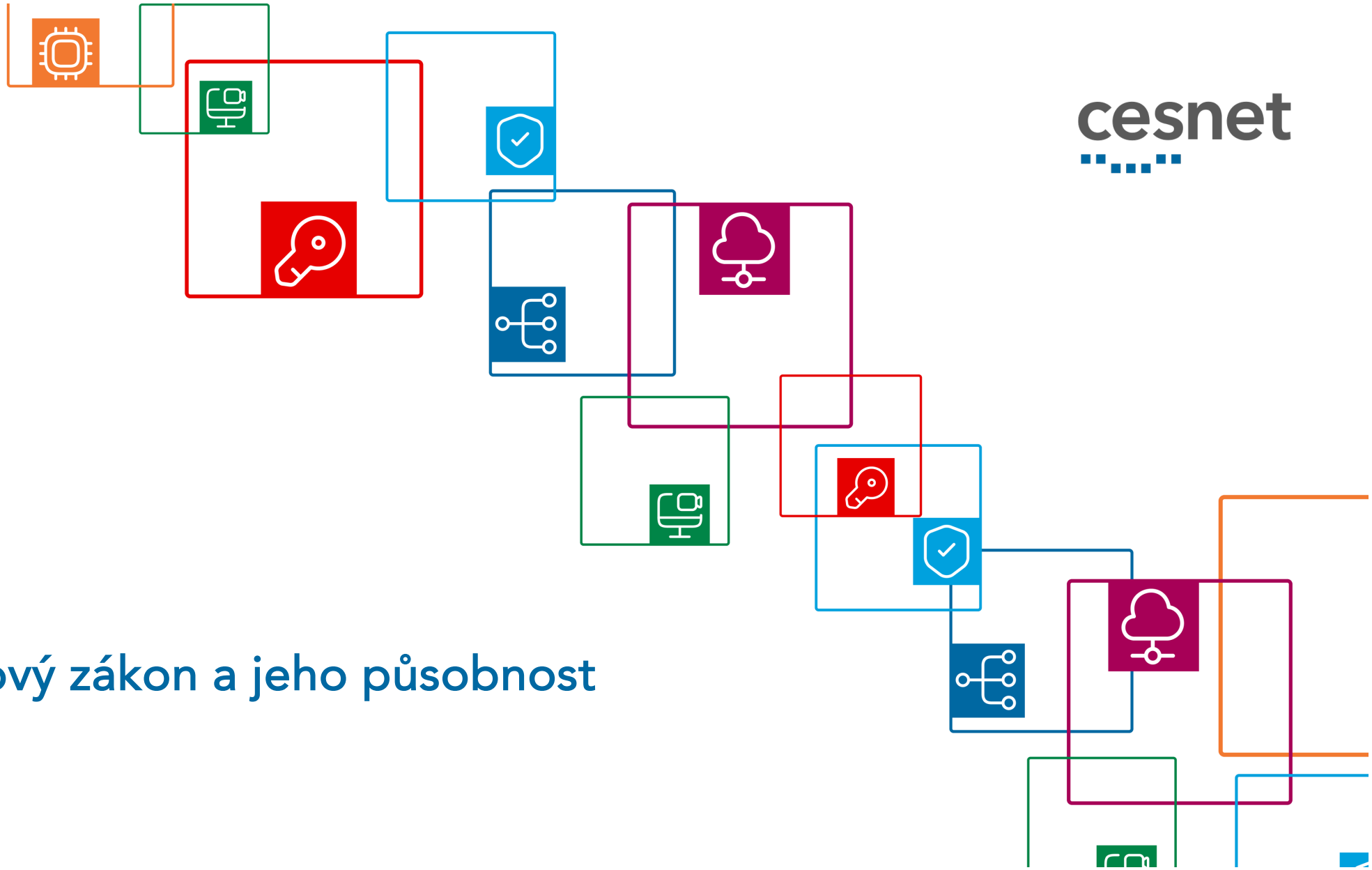
1. Provést samoidentifikaci
2. Dopracovat gap analýzu, seznam opatření, harmonogram a politiku
3. Nechat vše schválit vedením

máme účinné nVKB

do 60 dní provést úkony vůči NUKIB

máme rozhodnutí o registraci

do 1 roku zesouladit a začít plnit opatření



cesnet

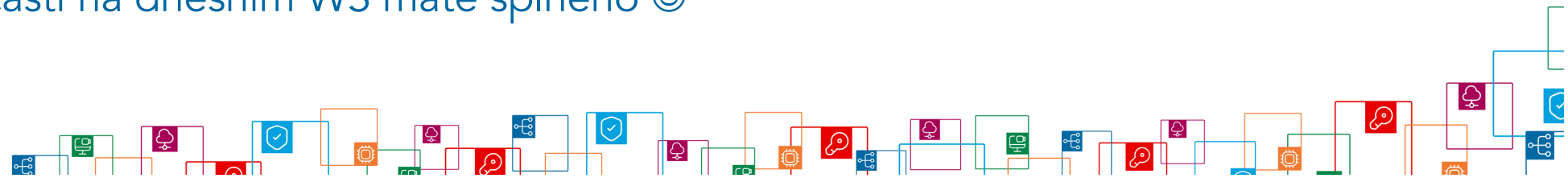
Nový zákon a jeho působnost

Krok č. 1: Seznámit se s nZKB

- Seznámit se s novou právní úpravou
  - zákon č. 264/2025 Sb., o kybernetické bezpečnosti
    - www.zakonyprolidi.cz
    - upravuje PaPO osob v oblasti zajišťování KB
  - vyhlášky NUKIB
    - čekáme na platné znění: https://odok.gov.cz/portal/veklep/hledat
    - rozpracovávají zásadní ustanovení nZKB

- Opatrně projít doprovodné zdroje – dobré pro kontext
  - hlavní zdroj: autor zákona = www.nukib.cz https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti
  - důvodová zpráva k nZKB
  - směrnice NIS2

- Účastí na dnešním WS máte splněno ☺



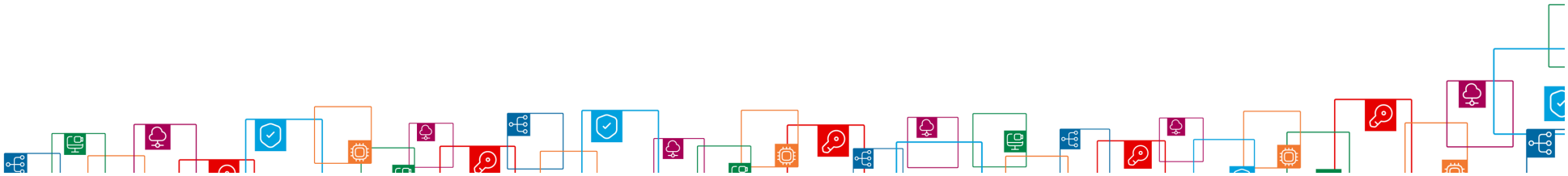
cesnet

Působnost nZKB

- na koho se nZKB vztahuje?
  - na **všechny osoby**, které provozují některou z tzv. regulovaných služeb
  - X dnes IS a KS + digitální služby
- co jsou regulované služby?
  - vybrané služby s významem pro zajištění KB v ČR
  - jejich výčet bude obsahovat příslušná prováděcí vyhláška NUKIB
- ... to se nás netýká...
  - KAŽDÁ organizace se musí s nZKB vypořádat
    - tj. alespoň konstatovat, že se na ni nZKB nevztahuje
    - vhodné o tom uchovat **ZÁZNAM**
    - **nutno vyhodnocovat opakovaně!**

Záznamy?

- Dříve nebo později přijde audit nebo kontrola
  - nebo kontrola „proč jste se neidentifikovali ...“
- Záznamy – dokumentují provedení činností v daném časovém období
  - důkaz pro kontroly (auditora), že se problematickou zabýváte a jak
  - pro MKB defacto deník činností
  - pro vedení jako výkaz činností – a podpůrný nástroj pro nárokování zdrojů
- Záznamy – RT lístky, excel, txt/doc soubor, wiki stránka, zápisy ...

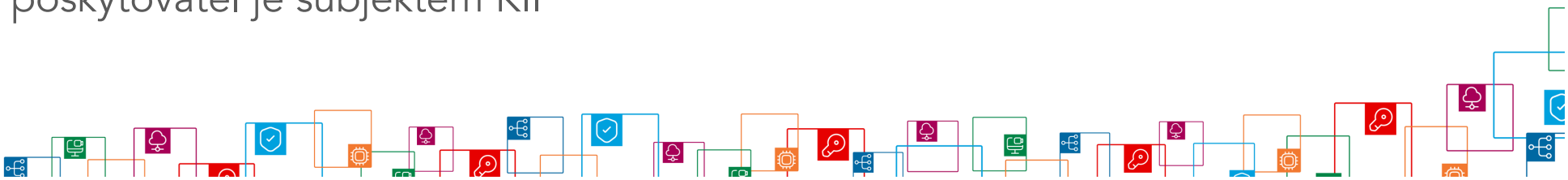


cesnet

Jak poznat povinnou osobu

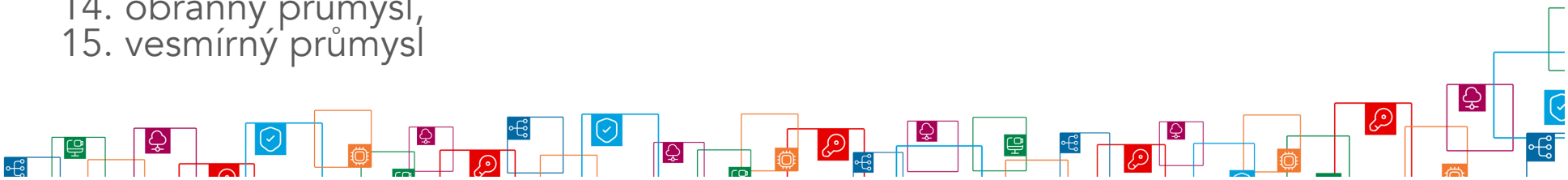
1. Určí se sama (samoidentifikace podle § 4 nZKB) – takto:
   - určí svoje regulované služby **(pomůcka: https://portal.nukib.gov.cz/kalkulacka)**
   - určí svůj režim povinností (vyšší x nižší)
   - ohlášení NUKIB poskytování regulované služby (do 60 dní od naplnění podmínek)
   - NUKIB rozhodne o registraci regulované služby

2. Určí ji NUKIB (z moci úřední podle § 5 nZKB a v režimu vyšších povinností) – pokud:
   - jediný či zásadní poskytovatel služby kritické pro ČR či region
   - narušení služby by mělo závažné dopady na bezpečnost ČR, dopady do zahraničí, dopady na jiné regulované služby
   - dopad narušení do života 125+ tis. osob
   - poskytovatel je subjektem KII



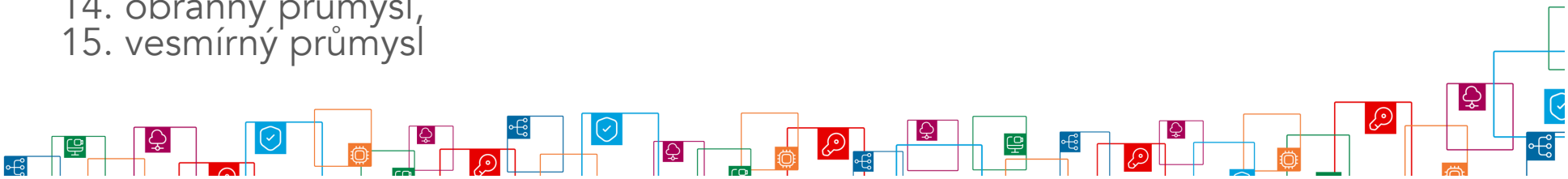
Samoidentifikace – krok 1

- Působím v některém z těchto odvětví (§ 4 odst. 1 nZKB):
  1. veřejná správa,
  2. energetika,
  3. výrobní průmysl,
  4. potravinářský průmysl,
  5. chemický průmysl,
  6. vodní hospodářství,
  7. odpadové hospodářství,
  8. doprava,
  9. digitální infrastruktura a služby,
  10. finanční trh,
  11. zdravotnictví,
  12. věda, výzkum a vzdělávání,
  13. poštovní a kurýrní služby,
  14. obranný průmysl,
  15. vesmírný průmysl



Samoidentifikace – CESNET

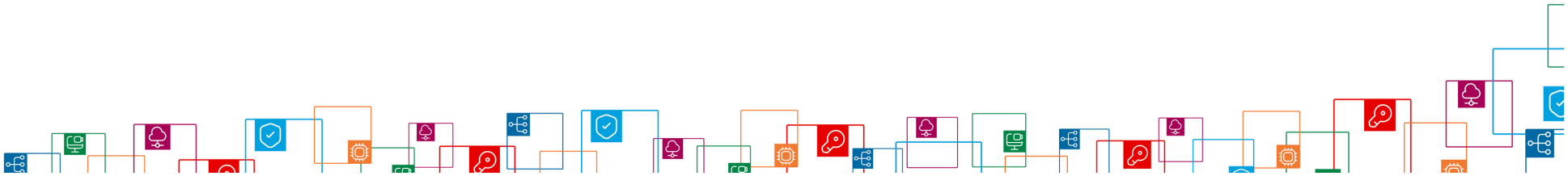
- Zařadit službu do některého z těchto odvětví (§ 4 odst. 1 nZKB):
  1. veřejná správa,
  2. energetika,
  3. výrobní průmysl,
  4. potravinářský průmysl,
  5. chemický průmysl,
  6. vodní hospodářství,
  7. odpadové hospodářství,
  8. doprava,
  9. digitální infrastruktura a služby,
  10. finanční trh,
  11. zdravotnictví,
  12. věda, výzkum a vzdělávání,
  13. poštovní a kurýrní služby,
  14. obranný průmysl,
  15. vesmírný průmysl



cesnet

Samoidentifikace – krok 2

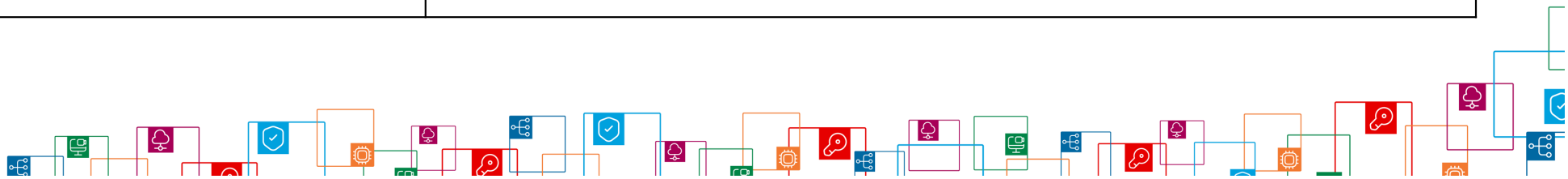
- Dohledat svoji službu v seznamu
  - seznam služeb bude v prováděcí vyhlášce NUKIB
  - pozor na definice služeb



Samoidentifikace – CESNET

- Dohledat svoji službu v seznamu

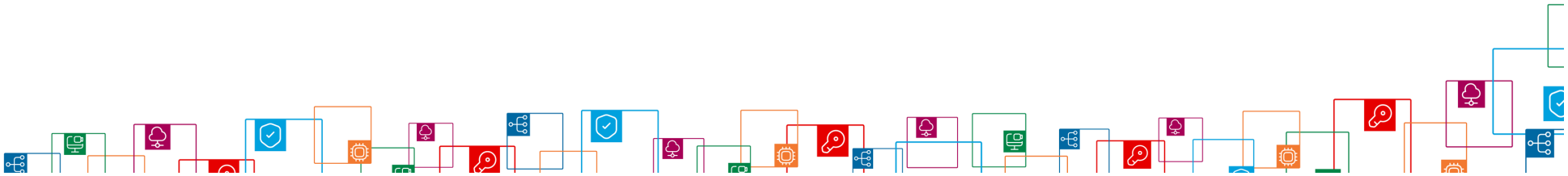
16.8 Poskytování služby cloud computingu	Poskytovatel služby cloud computingu je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) velkým podnikem, nebo b) poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy), nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.



cesnet

Samoidentifikace – krok 3

- Určit svoji významnost pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR
  - u každé služby v seznamu je uvedeno, zda poskytovatelem regulované služby je:
    - střední podnik
    - velký podnik
    - jiný významný poskytovatel

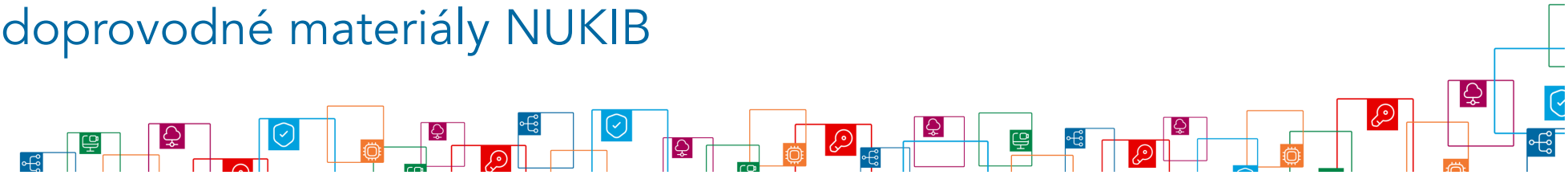


Jak určit velikost podniku

- doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků
  - kategorie:
    - mikropodniky (méně než 10 zaměstnanců a roční obrat max 2 mio EUR)
    - malé podniky (méně než 50 zaměstnanců a roční obrat max 10 mio EUR)
    - střední podniky (méně než 250 zaměstnanců a roční obrat max 50 mio EUR)
    - velké podniky (ty ostatní)

- odchylky **viz § 7 nZKB**
  - výslovná použitelnost doporučení Komise i na „ne-podniky“ z oblasti VVV

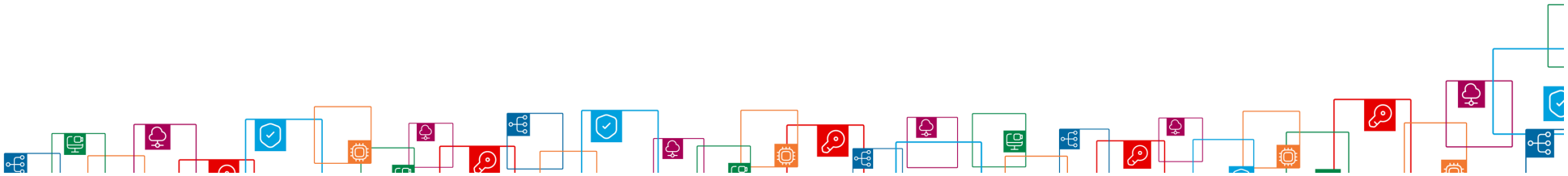
- viz doprovodné materiály NUKIB



Jak určit velikost podniku - CESNET

- doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků
  - kategorie:
    - mikropodniky (méně než 10 zaměstnanců a roční obrat max 2 mio EUR)
    - malé podniky (méně než 50 zaměstnanců a roční obrat max 10 mio EUR)
    - střední podniky (méně než 250 zaměstnanců a roční obrat max 50 mio EUR)
    - velké podniky (ty ostatní)

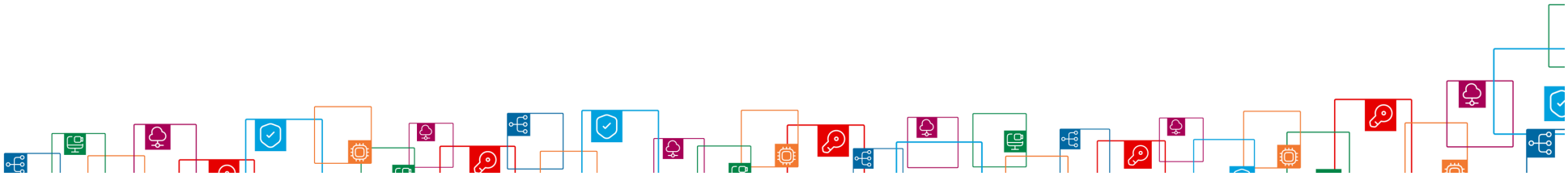
- odchylky **viz § 7 nZKB**
  - výslovná použitelnost doporučení Komise i na „ne-podniky“ z oblasti VVV



Významnost poskytovatele

- Určit svoji významnost pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR

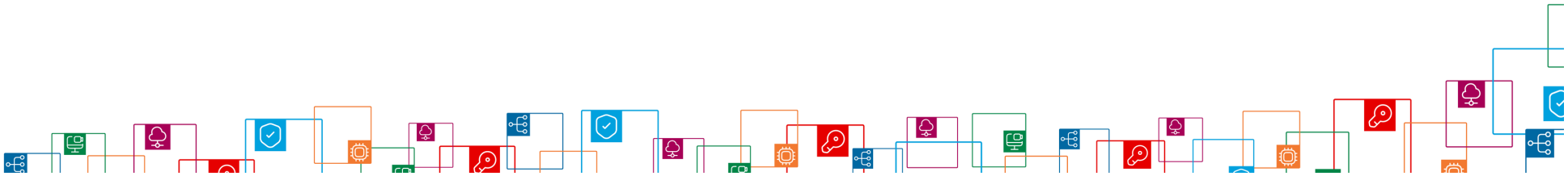
16.8 Poskytování služby cloud computingu	Poskytovatel služby cloud computingu je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) **velkým podnikem**, nebo b) **poskytovatelem státního cloud computingu** podle zákona o informačních systémech veřejné správy), nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je **středním podnikem**.



Významnost poskytovatele - CESNET

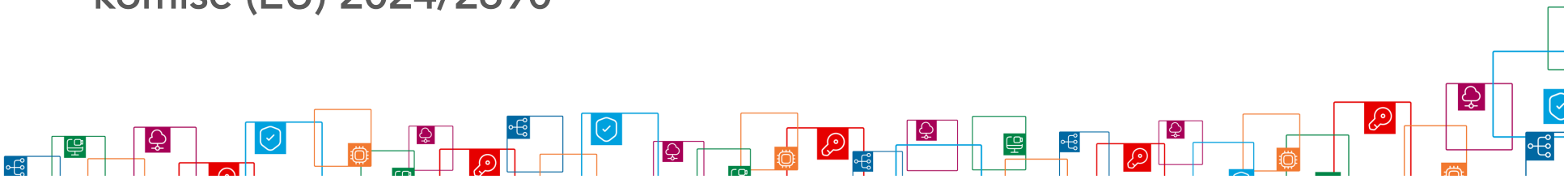
- Určit svoji významnost pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v ČR

16.8 Poskytování služby cloud computingu	Poskytovatel služby cloud computingu je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) **velkým podnikem**, nebo b) **poskytovatelem státního cloud computingu** podle zákona o informačních systémech veřejné správy), nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je **středním podnikem**.



Samoidentifikace – krok 4

- Určit svůj režim povinností
  - režim vyšších/nižších povinností
  - v seznamu regulovaných služeb bude vždy uvedeno, jaký režim povinností se vztahuje na střední podnik, na velký podnik a příp. na jiné významné poskytovatele
  - pro stanovení „celkového“ režimu povinností platí „vyšší bere“
  - každý režim povinností má vlastní pravidla pro povinnou osobu dle nZKB a bude mít vlastní prováděcí vyhlášku k bezpečnostním opatřením
  - **digitální služby mají vlastní režim (§18 nZKB) + Prováděcí nařízení komise (EU) 2024/2690**

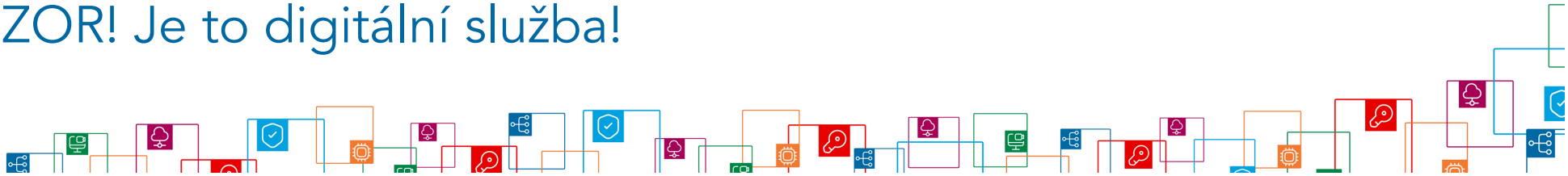


Samoidentifikace – CESNET

- Určit režim povinností

16.8 Poskytování služby cloud computingu	Poskytovatel služby cloud computingu je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) velkým podnikem, nebo b) poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy), nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.

- POZOR! Je to digitální služba!



cesnet

FAQ

Jsem povinnou osobou dle stávajícího ZKB – od kdy se musím řídit nZKB?

- účinnosti nZKB 1. 11. 2025
- viz přechodná ustanovení - § 71 nZKB

Subjekt podle § 3 ZKB + regulovaná služba podle § 4 odst. 1 nZKB = povinnost plnit základní povinnosti dle nZKB:

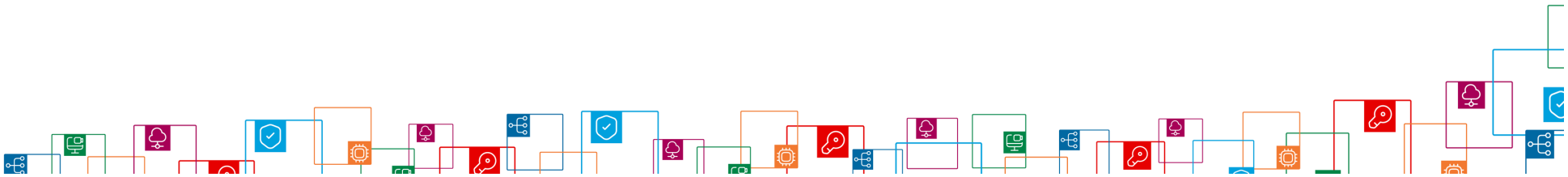
- zavést a provádět bezpečnostní opatření (dle režimu) – od účinnosti nZKB do uplynutí lhůty pro plnění povinností dle nZKB
- plnit opatření NUKIB - od účinnosti nZKB
- hlásit KBI – hned od registrace služby

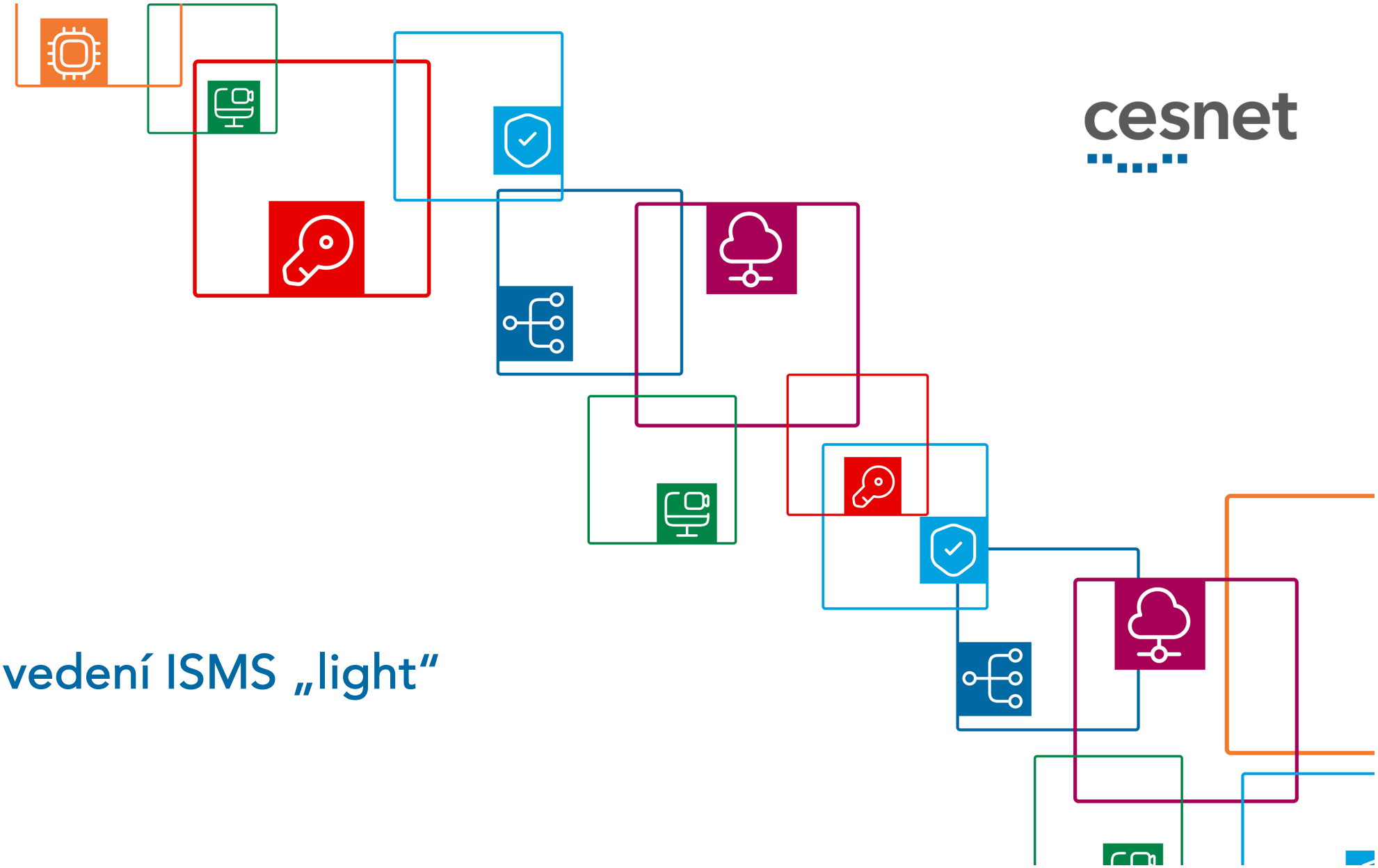
cesnet

A co s tím dál?

- Ohlásíme regulované služby a režimu NUKIB
- NUKIB posoudí podmíny a službu registruje
- Hlásíme změny

... a mezitím realizujeme další kroky soulaďování





cesnet

Zavedení ISMS „light“

Proces souladňování s nZKB

máme platný nZKB

1. ~~Seznámit se s problematikou nZKB~~
2. Sestavit tým
3. Identifikovat požadavky nové legislativy
4. Provést gap analýzu
5. Sestavit seznam opatření a harmonogram
6. Informova/zapojit vedení organizace
7. Nachystat politiku KB v organizaci

máme platné nVKB

1. Provést samoidentifikaci
2. Dopracovat gap analýzu, seznam opatření, harmonogram a politiku
3. Nechat vše schválit vedením

máme účinné nVKB

do 60 dní provést úkony vůči NUKIB

máme rozhodnutí o registraci

do 1 roku zesouladit a začít plnit opatření

Krok č. 2: Sestavení týmu

- Jak to udělal CESNET:
  - MKB na 0.5, AKB na 0.5
  - Partnery pro zavedení ISMS/ZKB byli vedoucí pracovníci
  - Další AKB, GDPR specialista
  - ISMS iniciovalo vznik pozice compliance manažera
  - Manažer služeb (ISO20tis/ITSM)
- Aktuální stav:
  - VKB (10 členů)
  - MKB, 2x AKB (a ještě by se hodil třetí),
  - Compliance manažer, GDPR specialista, manažer služeb,
  - garant, pověřený správce
    (1x ročně „velká“ schůzka celého týmu a komplet revize daného oddělení)

Proces souladňování s nZKB

máme platný nZKB

1. ~~Seznámit se s problematikou nZKB~~
2. ~~Sestavit tým~~
3. Identifikovat požadavky nové legislativy
4. Provést gap analýzu
5. Sestavit seznam opatření a harmonogram
6. Informova/zapojit vedení organizace
7. Nachystat politiku KB v organizaci

máme platné nVKB

1. Provést samoidentifikaci
2. Dopracovat gap analýzu, seznam opatření, harmonogram a politiku
3. Nechat vše schválit vedením

máme účinné nVKB

do 60 dní provést úkony vůči NUKIB

máme rozhodnutí o registraci

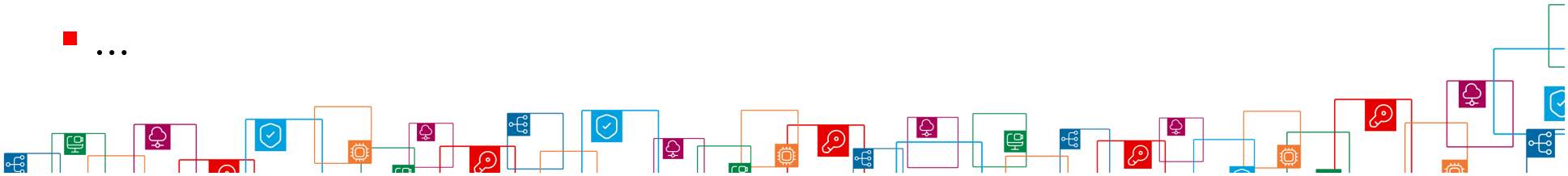
do 1 roku zesouladit a začít plnit opatření

Krok č. 3: Požadavky legislativy

- Identifikace požadavků nové legislativy
  - společný úkol pro compliance, právníka, MKB, vedoucího IT
  - zdroje: legislativa, důvodová zpráva, NUKIB, ...
- nZKB obsahuje 3 typy požadavků:
  - administrativní úkony
  - technická a organizační opatření
  - operativa
- Související krok: určit rozsah řízení KB
  - určit všechna primární aktiva organizace
  - identifikovat aktiva související s poskytováním regulované služby
  - zdůvodnit, proč ostatní nesouvisí
  - určit podpůrná aktiva pro aktiva související s poskytováním služby
  - POZOR! Dokud aktiva „kvalifikovaně“ nevyjmu, do rozsahu patří!

Jak určit rozsah?

- jsme v oblasti KB, důležité jsou regulované služby
- hlavní krok: určení aktiv (viz zákonná definice)
  - zahrnout jenom některá aktiva, nebo všechna?
  - CESNET: všechny, protože...
    - všechna – proč (viz příklad CESNETu)
- tj. co zahrnuje regulovaná služba a co potřebuji k jejímu provozu
  - HW, SW
  - zaměstnanci (správci)
  - lokalita
  - data, informace
  - ...



Příklad 1

- Regulovaná služba = služba komunikační infrastruktury
- Popis: Služba zajišťující připojení organizací do e-infrastruktury CESNET. Společná komunikační infrastruktura (e-infrastruktura CESNET), páteřní infrastruktura a její komponenty. Směrem k zákazníkům realizuje katalogovou službu *Připojení internetovým protokolem*.
- Primární aktivum
- Garant: vedoucí 701, DDI, hodnota
- Podpůrná aktiva
  - síťové prvky
  - fyzická infrastruktura (trasy, okruhy, POP)
  - HW, SW, aplikace
  - personál = správci
  - informace – informace přenášené po síti, metadata, konfigurace

Příklad 2

- Regulovaná služba = e-INFRA CZ Cloud
- Popis: Služba e-INFRA CZ Cloud nabízí flexibilní výpočetní a úložné prostředí vhodné pro širokou škálu aplikací. Patří mezi ně mimo jiné webové služby a portály, kontejnerové hostitele, pracovní uzly HPC, pracovní uzly CI/CD, hostitele databází a řadu komplexních vědeckých případů užití.
- Primární aktivum
- Garant: vedoucí oddělení 702, *DDI, hodnota*
- Podpůrná aktiva
  - servery, disková úložiště
  - AAI infrastruktura zajišťující řízení přístupových oprávnění
  - fyzická místa přítomnosti
  - SW, aplikace, databáze
  - personál = správci
  - informace – konfigurace, metadata, provozní informace, informace o zranitelnostech, KBU a KBI, obsah (uživatelská data) … (nakonec také primární aktiva)
  - síť, síťové prvky

Proces souladňování s nZKB

máme platný nZKB

1. ~~Seznámit se s problematikou nZKB~~
2. ~~Sestavit tým~~
3. ~~Identifikovat požadavky nové legislativy~~
4. Provést gap analýzu
5. Sestavit seznam opatření a harmonogram
6. Informova/zapojit vedení organizace
7. Nachystat politiku KB v organizaci

máme platné nVKB

1. Provést samoidentifikaci
2. Dopracovat gap analýzu, seznam opatření, harmonogram a politiku
3. Nechat vše schválit vedením

máme účinné nVKB

do 60 dní provést úkony vůči NUKIB

máme rozhodnutí o registraci

do 1 roku zesouladit a začít plnit opatření

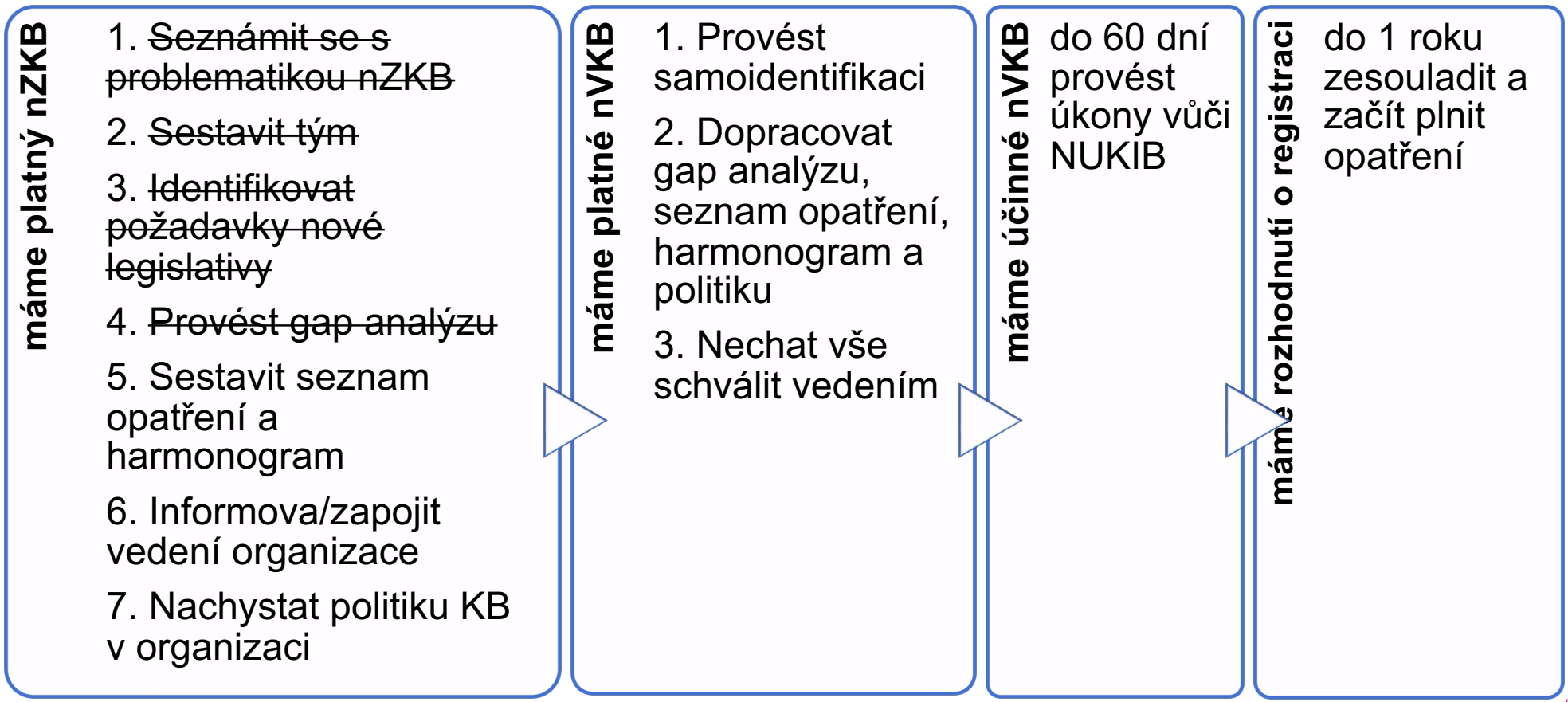
Krok č. 4: Gap analýza

- **gap analýza = analýza mezer**
  - - obsahuje popis současného stavu (AS-IS) a požadovaného stavu (TO-BE), identifikaci mezer (GAP) mezi nimi a návrh konkrétních kroků k jejich překlenutí (BRIDGE).
  - základní nástroj compliance - ... stejný postup, jako souladění s jakýmikoliv novými požadavky na organizaci (legislativními i jinými)
- X pro potřeby compliance vhodnější toto pořadí:
  1. zjistit, co se po mě chce
  2. zjistit, jak to plním
  3. splňuji ANO/NE? + určit, co je nutné udělat pro úplný soulad

+ zamyslet se nad závažností dopadů nesouladu (technická x administrativní apod)

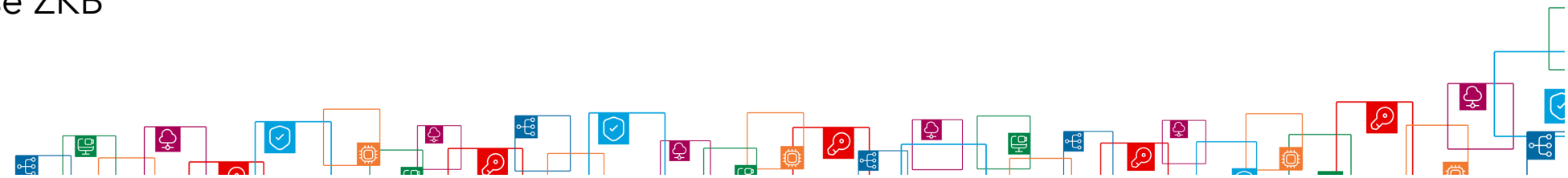
požadavek	**§ 12 nZKB – určit rozsah řízení KB**
aktuální stav	nemáme nic
splněno? to-do?	NE, je potřeba: (1) vytvořit databázi primárních aktiv, (2) určit primární aktiva pro regulovanou službu, (3) zdůvodnit nezařazení ostatních, (4) určit podpůrná aktiva pro zařazené

Proces souladňování s nZKB



Krok č. 6: Seznam opatření a harmonogram

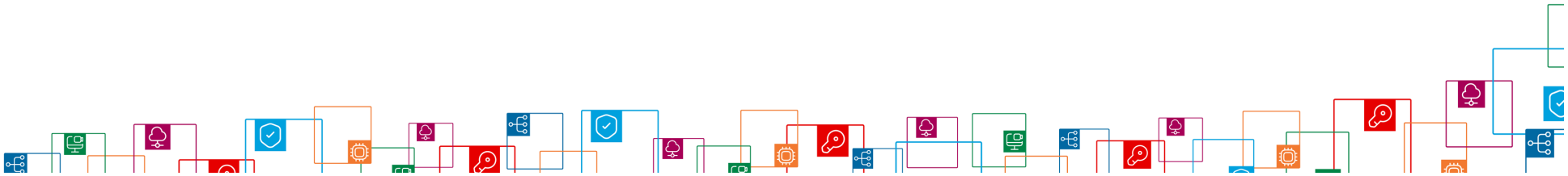
- GAP analýza = vím, kde nesplňuji
- Co musím udělat, abych danou povinnost splňoval?
  - Rozhodnout, co s tím budu dělat neboli stavit ***opatření***.
- K jednomu nesouladu může být stanoveno více ***opatření***.
- Opatření
  - Popis (např. formou cílového stavu)
  - Garant zodpovědný za plnění
  - Termín plnění
  - Finanční náklad
  - Urgence
- Seznam opatření = Plán zvládání rizik = Harmonogram činností pro dosažení souladu se ZKB



cesnet

PŘÍKLAD

- § 20 řízení přístupů
  - Výsledek GAP analýzy: nemáme dvoufaktor
  - Co musím udělat, abych danou povinnost splňoval?
    - zavést dvoufaktor ... nebo ...
    - alternativní řešení?
  - Rozhodnutí: zavedu dvoufaktor



Krok č. 6: Seznam opatření, PZR, harmonogram

Opatření	Znění opatření	Garant (zodpovídá za realizaci)	Finanční náklady	Termín	Priorita
1.	Podpora 2-faktoru na IDP.	Pepa Pádlo	interní zdroje	30.06.2026	MUST
2.	Implementace podpory na straně klientů (password manager apod.)	Karel Veslo	200 tis. za licenci na PM	31.03.2026	MUST
3.	Proškolení uživatelů v používání 2-faktoru.	Aneta Veselá	interní zdroje	30.04.2026	SHOULD
4.	Otestování celé infrastruktury před nasazením do ostrého provozu za účasti vybraných zaměstnanců.	Igor Přísný	interní zdroje/50tis dodavatelsky	31.05.2026	SHOULD

Proces souladňování s nZKB

máme platný nZKB

1. ~~Seznámit se s problematikou nZKB~~
2. ~~Sestavit tým~~
3. ~~Identifikovat požadavky nové legislativy~~
4. ~~Provést gap analýzu~~
5. ~~Sestavit seznam opatření a harmonogram~~
6. Informova/zapojit vedení organizace
7. Nachystat politiku KB v organizaci

máme platné nVKB

1. Provést samoidentifikaci
2. Dopracovat gap analýzu, seznam opatření, harmonogram a politiku
3. Nechat vše schválit vedením

máme účinné nVKB

do 60 dní provést úkony vůči NUKIB

máme rozhodnutí o registraci

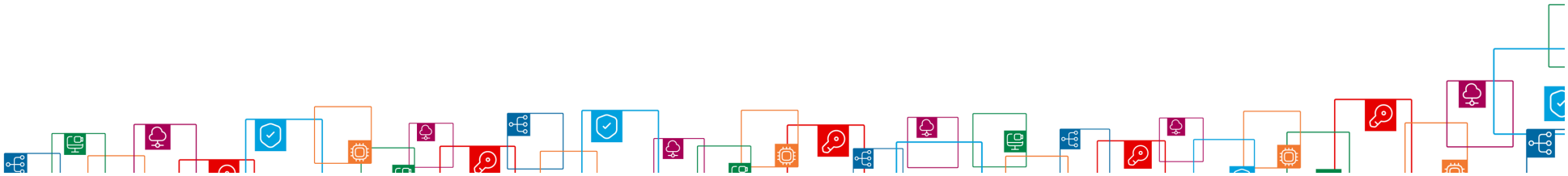
do 1 roku zesouladit a začít plnit opatření

Krok č. 7: Informovat/zapojit vedení organizace

- Mám-li:
  - tým (min MKB)
  - určení
  - registraci
  - GAP analýzu
  - harmonogram adresace nálezů z GAP analýzy (harmonogram prací)

= mám základ, který v nouzi NUKIB (v případě kontroly) uspokojí, protože sice nemám soulad, ale zabýval jsem se a mám plán, jak souladu pomalu dosáhnout

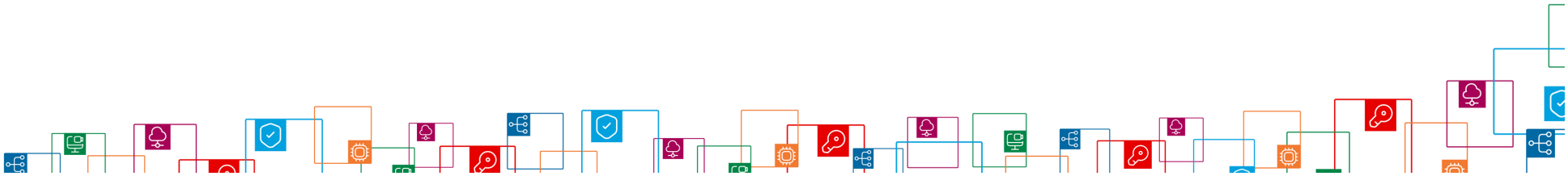
  - ano, součástí plánu může být také opatření: vytvořit DB aktiv
- Zpráva z GAP analýzy
  - nutno předložit vedení (informuji a získávám souhlas pro další kroky) - ideálně rovnou s harmonogramem prací, opatřeními a zodpovědnými osobami



Jak pracovat s vedením

- Vedení musí být informováno o všech krocích, identifikovaných problémech a návrzích řešení – tím se posiluje jejich povědomí o jejich zodpovědnosti

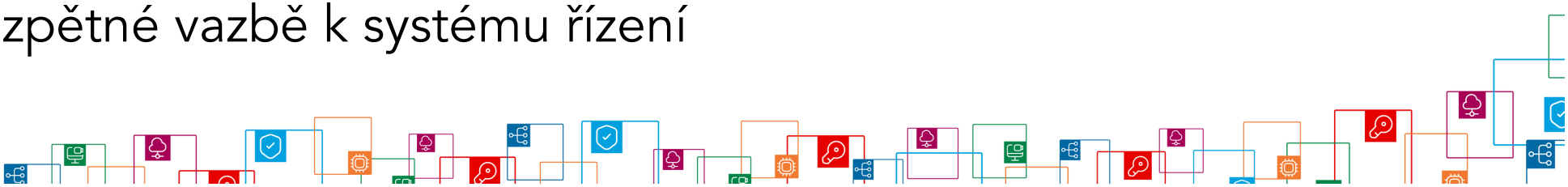
- O čem je informovat:
  - Jsme povinný subjekt – ANO, NE, proč
  - Zpráva z GAP analýzy (tj. splňujeme/nesplňujeme tyto oblasti)
  - základní plán, jak souladu dosáhnout
    - kdo, co, kdo, jak (= mám harmonogram)



Managament review

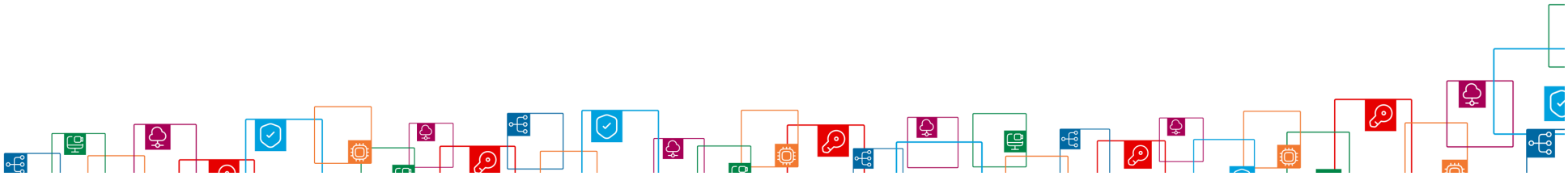
- = Zpráva o přezkoumání systému řízení bezpečnosti informací podle písmene § 4 písm. g)

- Prostředek pro pravidelné (min. 1x za rok) informování vedení o:
  - stavu souladu se ZKB
  - plnění plánu
  - problémech
  - zpětné vazbě k systému řízení



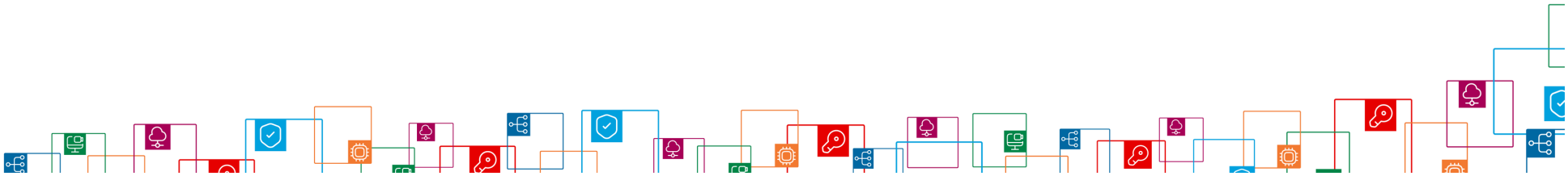
Struktura management review

1. vyhodnocení cílů systému řízení bezpečnosti informací směřujících k zajištění kybernetické bezpečnosti regulované služby,
2. posouzení naplňování plánu zvládání rizik zpracovaného podle § 9 odst. 1 písm. g),
3. hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik,
4. posouzení výsledků provedených auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
5. výsledky předchozího hodnocení účinnosti systému řízení bezpečnosti informací provedených podle tohoto písmene,
6. posouzení dopadů kybernetických bezpečnostních incidentů na oblast kybernetické bezpečnosti a na poskytované služby podle § 16 a
7. posouzení významných změn podle § 12



Význam management review

- Komunikační prostředek především s managementem
  - vyhodnocení, jak si v oblasti kyberbezpečnosti organizace stojí
- Prostředek k naplňování „přezkoumávání“ a „aktualizací“
- Prostředek ke sdělení, kolik kybernetická bezpečnost „stojí“
  - kolik zaměstnanců se na tom podílí a jakým úvazkem
  - všechny činnosti, které se uskutečnily …
    - mj. ony „vícepráce“ ala reagování na reaktivní opatření od NÚKIB
      - hrozbou DeepSeek
      - hrozbou spočívající v předávání dat a ve výkonu vzdálené správy z Čínské lidové republiky



PDCA cyklus

- Být v souladu se zákonem není jednorázová akce, řada činností se musí opakovat … a kdo si to má pamatovat?
- ZKB používá termíny – nejčastěji *přezkoumávat* a *aktualizovat*
- PDCA cyklus ISMS je užitečná pomůcka
  - vede zodpovědné osoby (MKB, AKB, garanty, vedení…) k plnění povinností
  - dává „roku“ řád

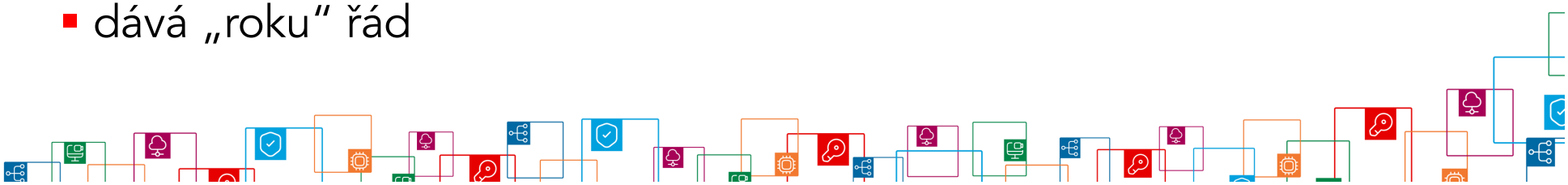
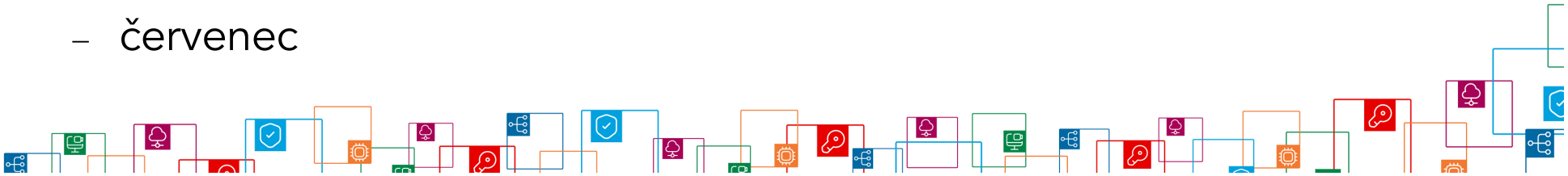


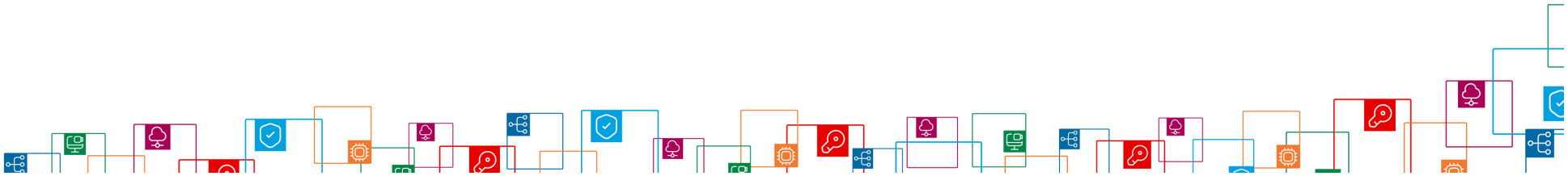
Schéma PDCA cyklu v CESNET

- PDCA v CESNET: červenec – červen
  - červen: ISMS audit (recertifikační nebo dozorový), tím je PDCA dán
- PDCA schéma – období:
  - červenec – srpen
  - září – prosinec
  - leden
  - únor – březen
  - duben – květen
  - červen
  - červenec



červenec - prosinec

červenec - srpen	• stanovení opatření k nálezům z recertifikačních a dozorových auditů • vydechnutí po auditu a období zvýšené činnosti ;-)
září - prosinec	• interní kontroly – užitečný nástroj, kontrola shody teorie s praxí • setkání VKB • aktualizace nebo tvorba vnitřních předpisů



cesnet

leden

leden	▪ velká profylaxe plnění povinností ▪ checklist: ▪jsem dobře určen? nezměnilo se moje určení? nemám novou regulovanou službu? ▪potřebuji aktualizovat nahlášené kontaktní informace? ▪legislativa – nedopadl na mě další zákon? ▪jsou naplánována/realizována školení zaměstnanců? ▪sešel se VKB? ▪reaktivní opatření, varování apod. od NÚKIBu – plním? Mám záznamy o plnění? ▪plníme plány a cíle činností schválené/nařízené vedením? ▪v jakém stavu je plnění stanovených opatření, tj. Plán zvládání rizik/harmonogram z GAP? ▪potřebuji aktualizovat metodiky pro identifikaci aktiv a rizik? ▪ spolupráce s garanty i vedením – radí, stanovuje náhradní opatření, přehodnocuje, informuje, hlásí...

únor - duben

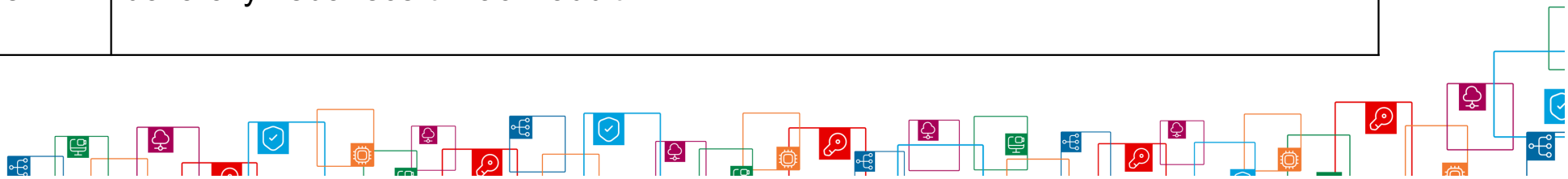
únor – březen	• setkávání s garanty - aktualizace DB aktiv... program setkání:
	  • máme nová aktiva?
	  • rušíme aktiva?
	  • přeskupujeme aktiva?
	  • máme nové – garanty, pověřené osoby, mění se hodnota, DDI, vazby?
	• aktualizace analýzy rizik:
	  • nové hrozby
	  • nové skutečnosti
	  • zohlednění např. výsledků interních kontrol, penetračních testů, identifikovaných KBU a KBI

duben	• zpráva z analýzy rizik --> předložit vedení • stanovení opatření k nálezům z analýzy rizik – aktualizace Plánu zvládání • školení zaměstnanců – mohu zohlednit některá zjištění z AR

květen - červen

květen	▪ interní audit
	▪ VKB
	  ▪ výsledky AR
	  ▪ plány a cíle na další období
	▪ zpracovat/zajistit a předložit vedení:
	  ▪ zpráva z auditu + nápravná opatřeními k nálezům
	  ▪ POA
	  ▪ Kontext organizace
	  ▪ Management review (samotné MR je jeden velký checklist)
	  ▪ Plán činností a cíle na další období

červen	dozorový nebo recertifikační audit



Proces souladňování s nZKB

máme platný nZKB

1. ~~Seznámit se s problematikou nZKB~~
2. ~~Sestavit tým~~
3. ~~Identifikovat požadavky nové legislativy~~
4. ~~Provést gap analýzu~~
5. ~~Sestavit seznam opatření a harmonogram~~
6. ~~Informova/zapojit vedení organizace~~
7. Nachystat politiku KB v organizaci

máme platné nVKB

1. Provést samoidentifikaci
2. Dopracovat gap analýzu, seznam opatření, harmonogram a politiku
3. Nechat vše schválit vedením

máme účinné nVKB

do 60 dní provést úkony vůči NUKIB

máme rozhodnutí o registraci

do 1 roku zesouladit a začít plnit opatření

Krok č. 8: Politika KB

- MKB není osoba zodpovědná za soulad s povinnostmi ZKB,
  - zodpovědné je vedení
  - MKB řídí proces, dohlíží, pomáhá, informuje, úkoluje
  - Úkoly vedoucí k naplnění povinností musí být vhodně přiděleny zodpovědným pracovníkům (vedoucí, garanti aktiv, pověření správci aktiv)
- Proto musí být v rámci organizace vyjasněné
  - cíle v oblasti kybernetické bezpečnosti
  - role a odpovědnosti – MKB, AKB, garant, pověřený správce
- Vhodná forma je vnitřní předpis „Politika kybernetické bezpečnosti organizace“
  - Závazný obsah stanoví prováděcí vyhláška
  - Je nutné s ní zaměstnance prokazatelně seznámit – např. formou školení
- Školení = dvě mouchy jednou ranou
  - zavedl jsem politiku
  - proškolil jsem zaměstnance (a o obojím si udělám záznam)

Jak napsat politiku

- Politika KB organizace = vnitřní předpis organizační povahy
  - účelem není opisovat zákon či sepsat obecné deklarace
  - má definovat základní pojmy, určit PaPO zaměstnancům v jednotlivých rolích a popsat konkrétní procesy a pravidla, jak jednotlivé role naplňují nZKB
  - forma dle vnitřních pravidel organizace (směrnice, pokyn, metodika, závazná pravidla,...)
  - na tuto politiku budou navazovat další z oblasti KB (budou se na tuto odkazovat)
- Doporučení:
  - NE: „organizace je povinna“, „zaměstnanci zpravidla dodržují“
  - ANO: „MKB je povinen“, „není-li dále stanoveno jinak, jsou zaměstnanci povinni dodržovat...“
  - pozor na děravá ustanovení
  - pozor na adresáty (komu chci dát PaPO?)
  - důraz na jednoznačnost a srozumitelnost (měřítko: průměrný zaměstnanec)
  - viz vzor CESNET

Proces souladňování s nZKB

máme platný nZKB

1. ~~Seznámit se s problematikou nZKB~~
2. ~~Sestavit tým~~
3. ~~Identifikovat požadavky nové legislativy~~
4. ~~Provést gap analýzu~~
5. ~~Sestavit seznam opatření a harmonogram~~
6. ~~Zapojit vedení organizace~~
7. ~~Nachystat politiku KB v organizaci~~

DONE!

máme platné nVKB

1. Provést samoidentifikaci
2. Dopracovat gap analýzu, seznam opatření, harmonogram a politiku
3. Nechat vše schválit vedením

máme účinné nVKB

do 60 dní provést úkony vůči NUKIB

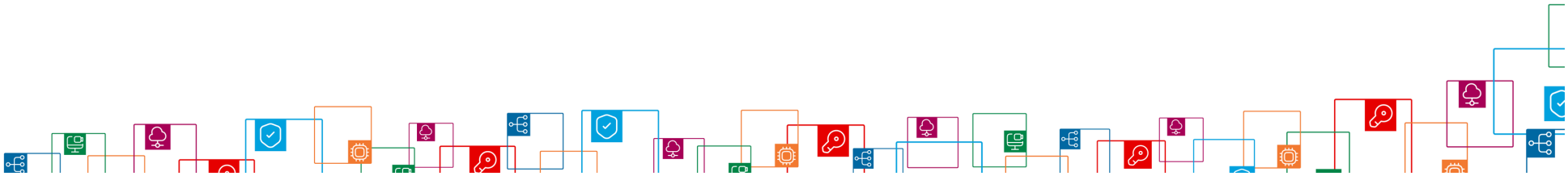
máme rozhodnutí o registraci

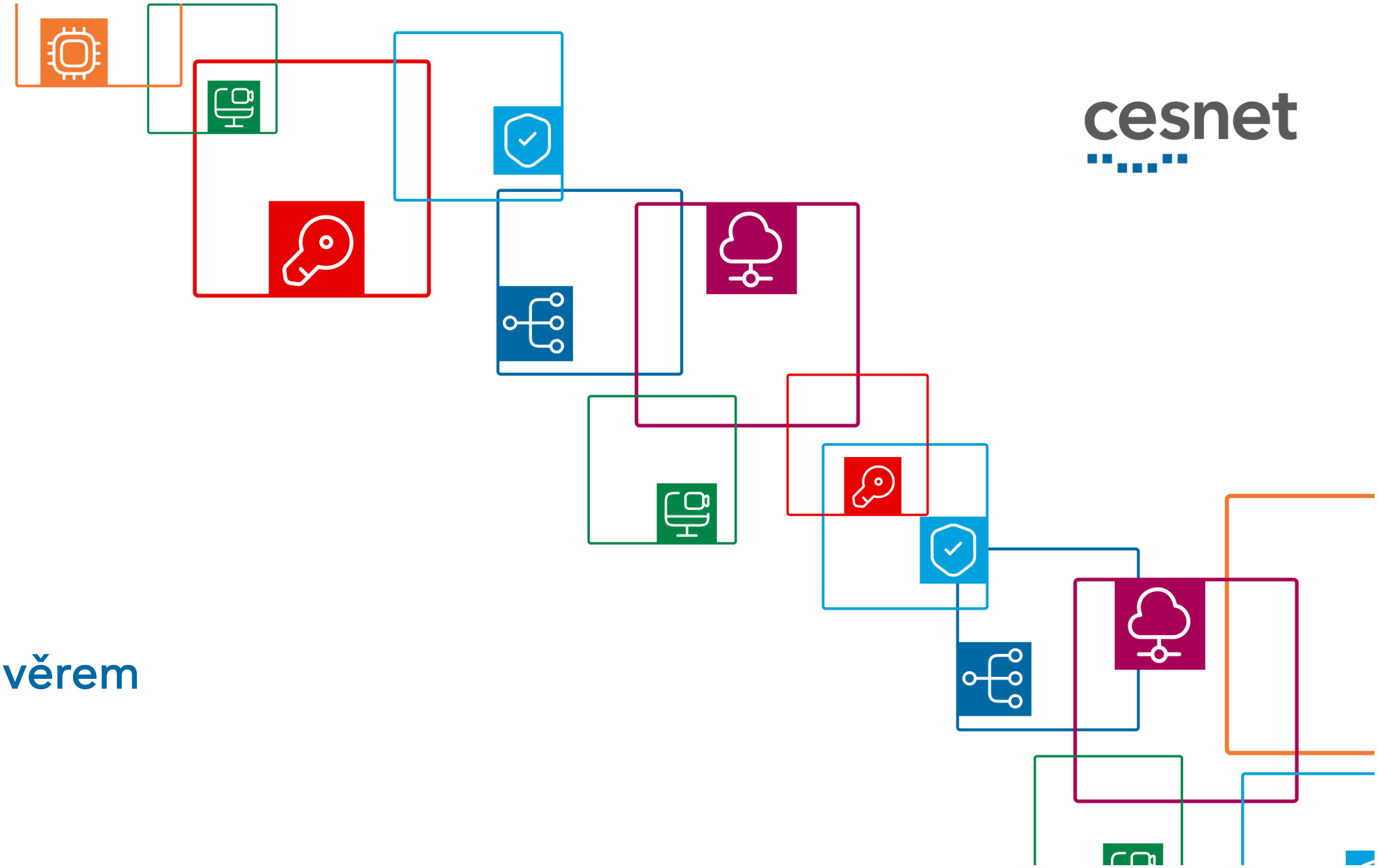
do 1 roku zesouladit a začít plnit opatření

Skoro…

- GDPR
  - řadu věcí lze použít (i GDPR opisuje normu ISMS)
  - i osobní údaje jsou data a informace, tj. aktiva
  - také vyžaduje popsaná „bezpečnostní opatření“

- Pro digitální služby:
  - digitální služby mají vlastní režim (§18 nZKB)
  - nutno dodržovat i prováděcí nařízení komise (EU) 2024/2690
  - X stávající ZKB funguje stejně





cesnet

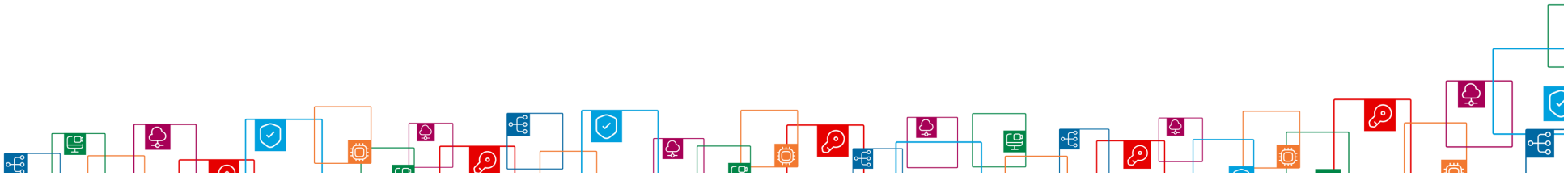
Závěrem

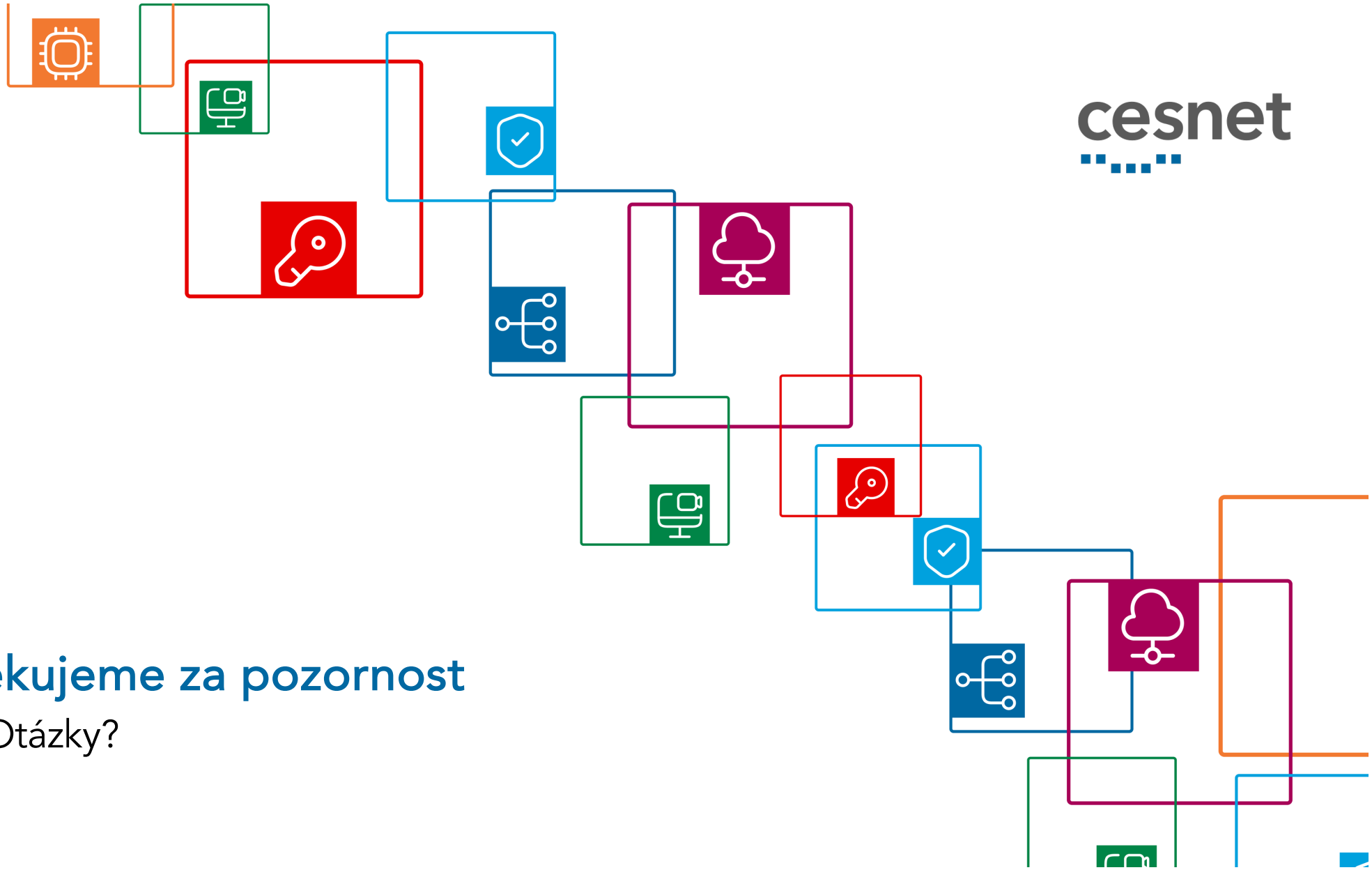
Závěr

- Není důvod panikařit, rok je dost dlouhá doba
  - nikdo nepojede úplně z nuly
  - postupně zjistíte, že řadu povinností plníte, protože prostě musíte
  - rok je dost času na základní úkony
- Po roce se neočekává 100% soulad, to ani nelze, protože nikdo nikdy nebude 100% „compliant“, je to prostě neustálý proces nalézání slabin a jejich adresace, neustálý proces zlepšování
- Berte to jako příležitost a šanci naadresovat kostlivce (ZKB, GDPR a teď nZKB, ale i interní „nedostatky“)
- **CESNET pomůže**: rámcové smlouvy, síťový monitoring, služby, Varování ala DeepSeek, tyto semináře, základní dokumenty, konzultace ...

Další kroky

- Zpřístupníme Vám vzory a návody:
  - bezpečnostní politiky – role, cíle ...
  - gap analýzy
  - management review – s návodem, co do jednotlivých oblastí dávat
- Další semináře
  - 7. října, 5. listopadu
- Pošleme dotazník
  - možnost vyjádřit se o jaká témata byste měli zájem
  - jestli tento seminář zopakovat a vrátit se ještě o krok zpět





cesnet

Děkujeme za pozornost

... Otázky?