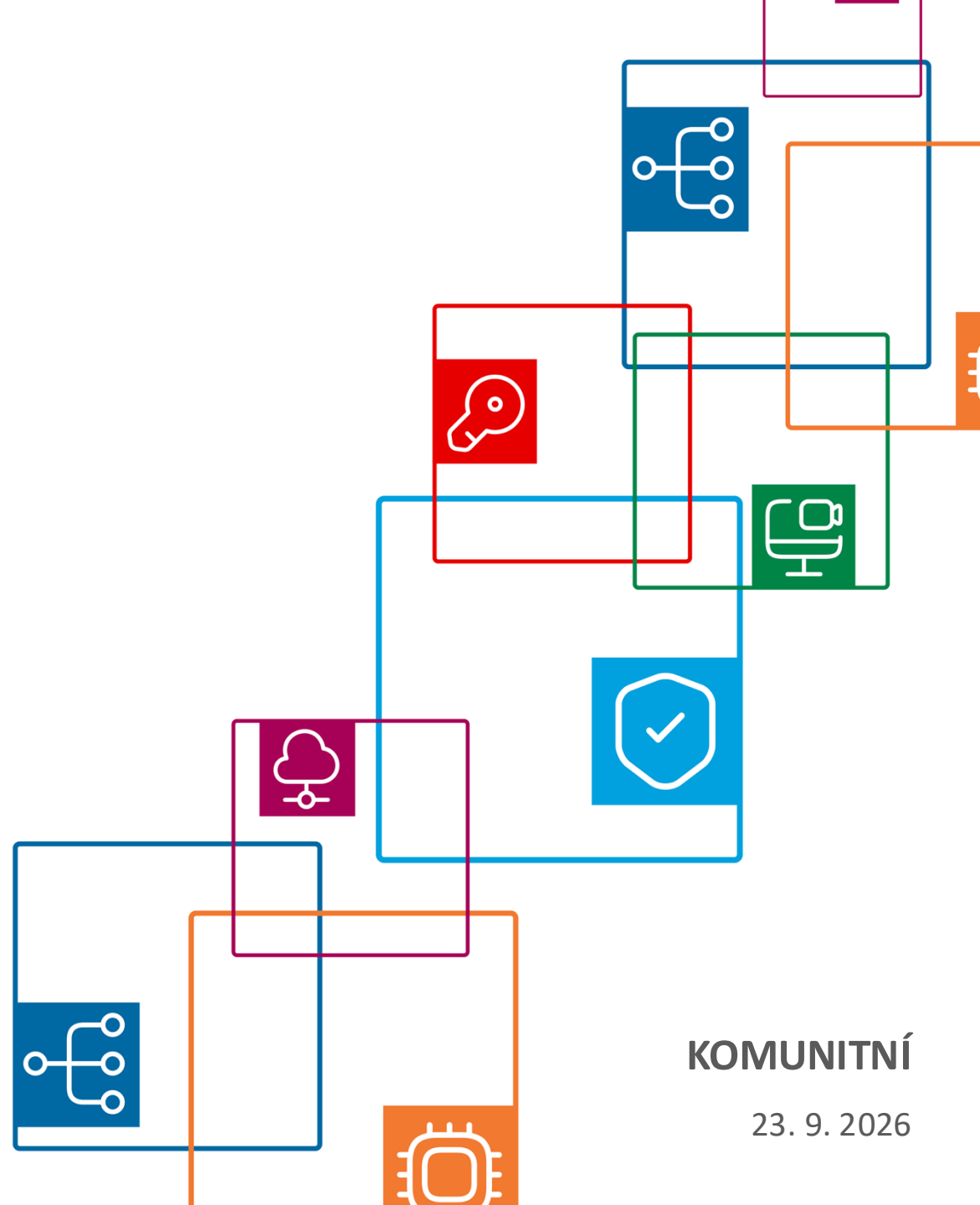




Teorie a praxe nového zákona o kybernetické bezpečnosti:

Řízení dodavatelů

A. Kropáčová, M. Pospíšilová



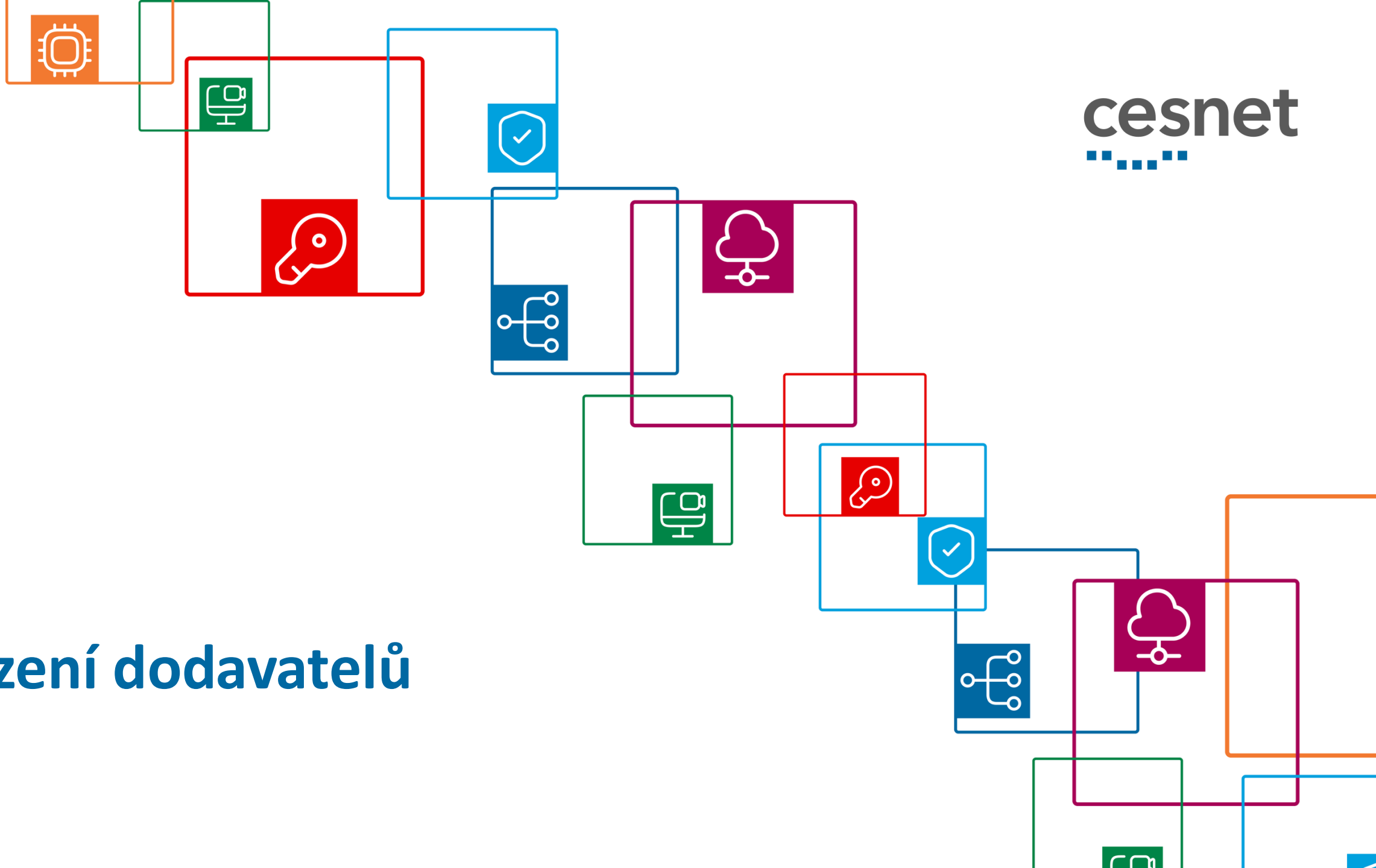
KOMUNITNÍ

23. 9. 2026

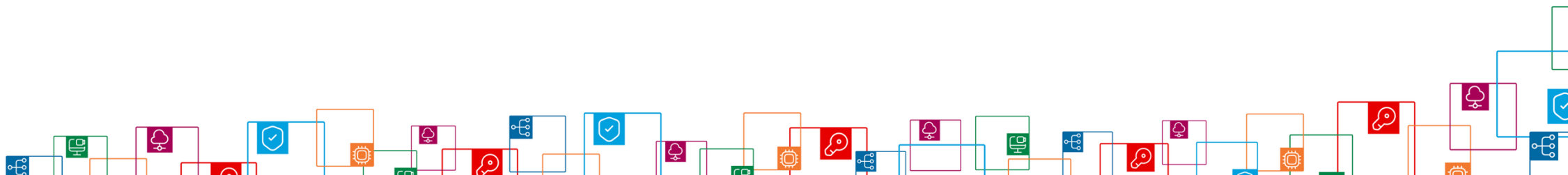
An abstract graphic featuring a series of overlapping, colorful rectangular frames (orange, green, blue, red, purple) arranged in a descending staircase pattern from the top-left to the bottom-right. Each frame contains a white icon: a microchip, a key, a cloud with a network symbol, a shield with a checkmark, and a network diagram. In the top-right corner, the word 'cesnet' is written in a dark grey sans-serif font, with a small blue dotted graphic below it. In the bottom-left corner, the word 'vinky' is written in a red sans-serif font.

Novinky

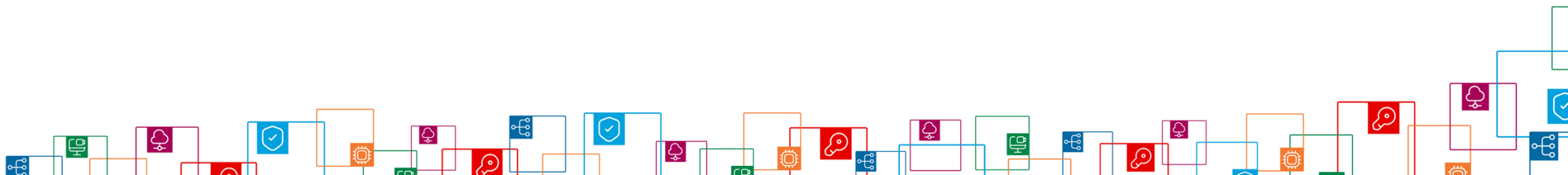
Řízení dodavatelů



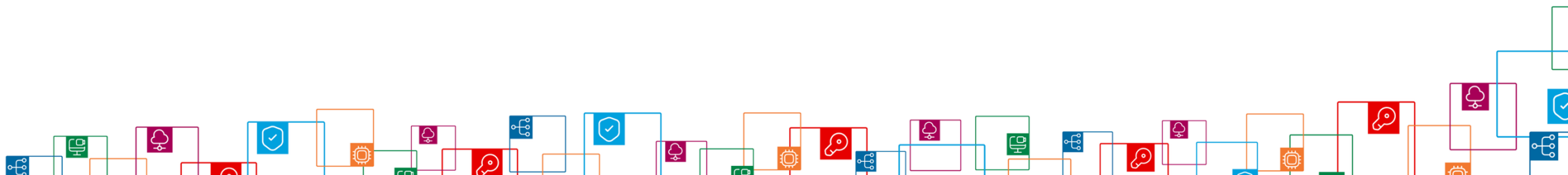
- = organizační bezpečnostní opatření
- = **stanovení pravidel pro řízení bezpečnostních rizik souvisejících s dodávkou zboží a služeb**
- povinnost pro všechny provozovatele regulovaných služeb (režim nižších i vyšších povinností)
 - tak nějak...



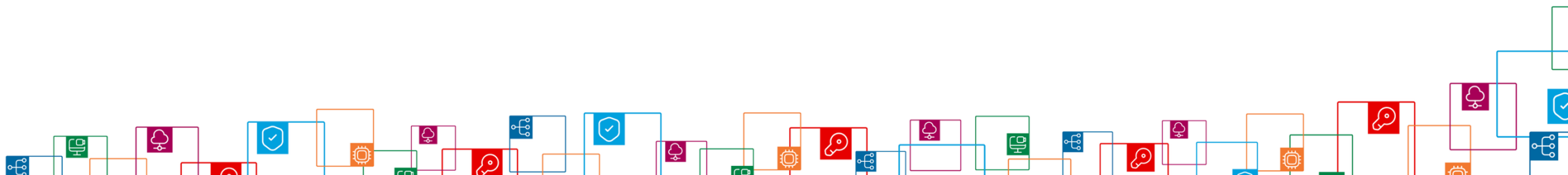
- textace předpisů X praktická zkušenost sdružení CESNET
- jde nám o bezpečnost – jedna pravidla pro všechny?
 - předpisy = minimální standard
 - co je praktické – doporučení, inspirace
 - ZKB X ISMS
 - co je praktické



- účel: ochrana aktiv organizace, tj. ...
 - „... zmírnit rizika spojená s přístupem dodavatele k aktivům organizace,
 - ... zajistit bezpečnost aktiv při spolupráci s dodavateli v souladu s požadavky bezpečnostních politik.“
- dodavatel může být zranitelnost i hrozba
 - zranitelnost: nedostatečné vymezení PaPO dodavatelů, neschopnost včas odhalit pochybení dodavatelů, ...
 - hrozba: porušení bezpečnostní politiky ze strany dodavatele, porušení smluvního závazku dodavatele, závislost na dodavateli

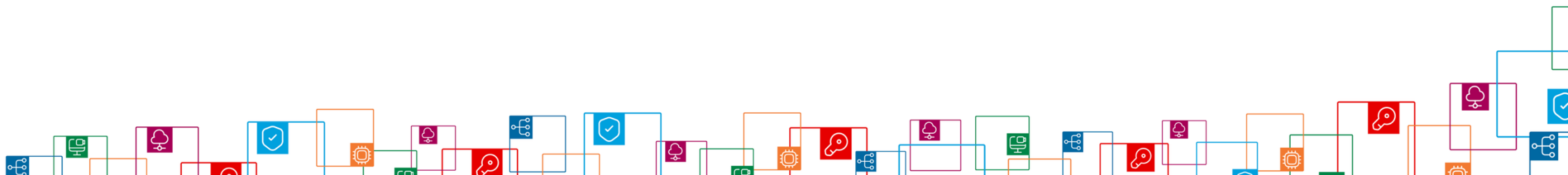


- pozor na definice – „dodavatel“ vs. „dodavatel pro potřeby této politiky“
 - „jakýkoliv právní subjekt, se kterým vstupuje organizace do smluvního vztahu:
 - a) jehož předmětem je dodávka zboží či služeb a zároveň
 - b) v důsledku kterého dojde ke zpřístupnění aktiv organizace tomuto dodavateli.“
- řídíme všechny dodavatele!
 - NTB, externí disk,...

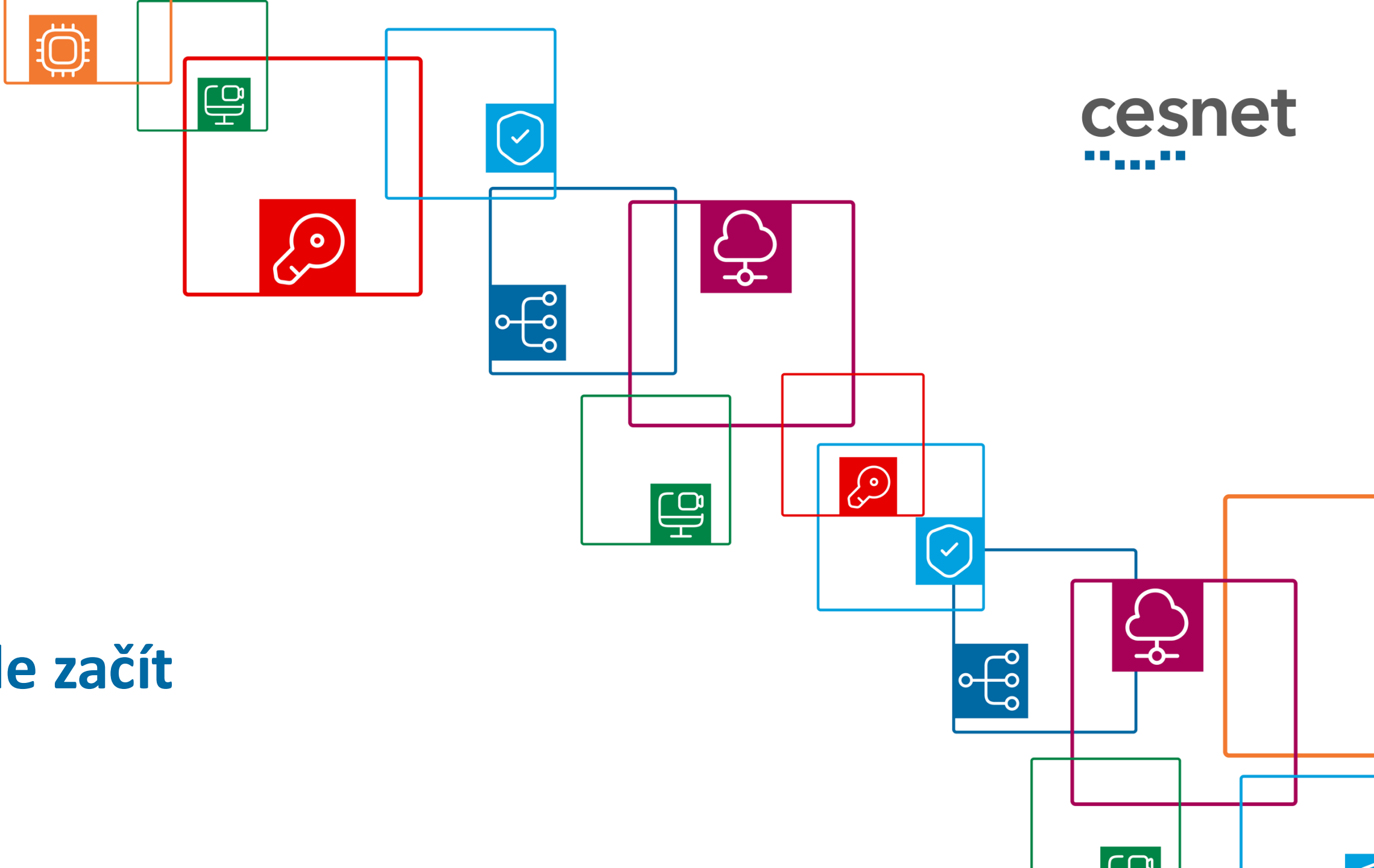


Pro inspiraci: Příloha vyhlášky 82/2018 Sb., o kybernetické bezpečnosti – požadavky na obsah politiky řízení dodavatelů:

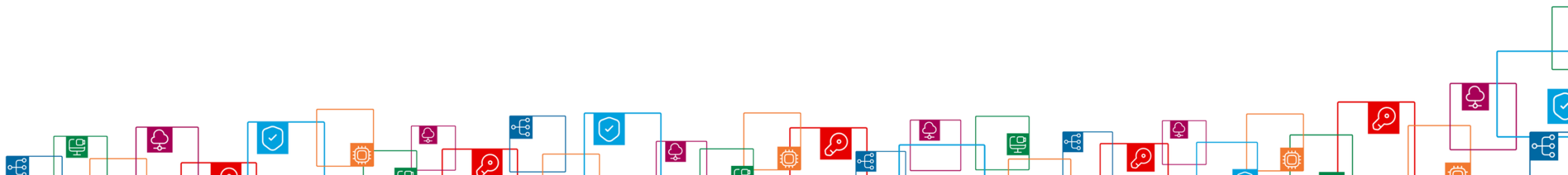
- a) Pravidla a principy pro výběr dodavatelů.
- b) Pravidla pro hodnocení rizik souvisejících s dodavateli.
- c) Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.
- d) Pravidla pro provádění kontroly zavedení bezpečnostních opatření.
- e) Pravidla pro hodnocení dodavatelů.



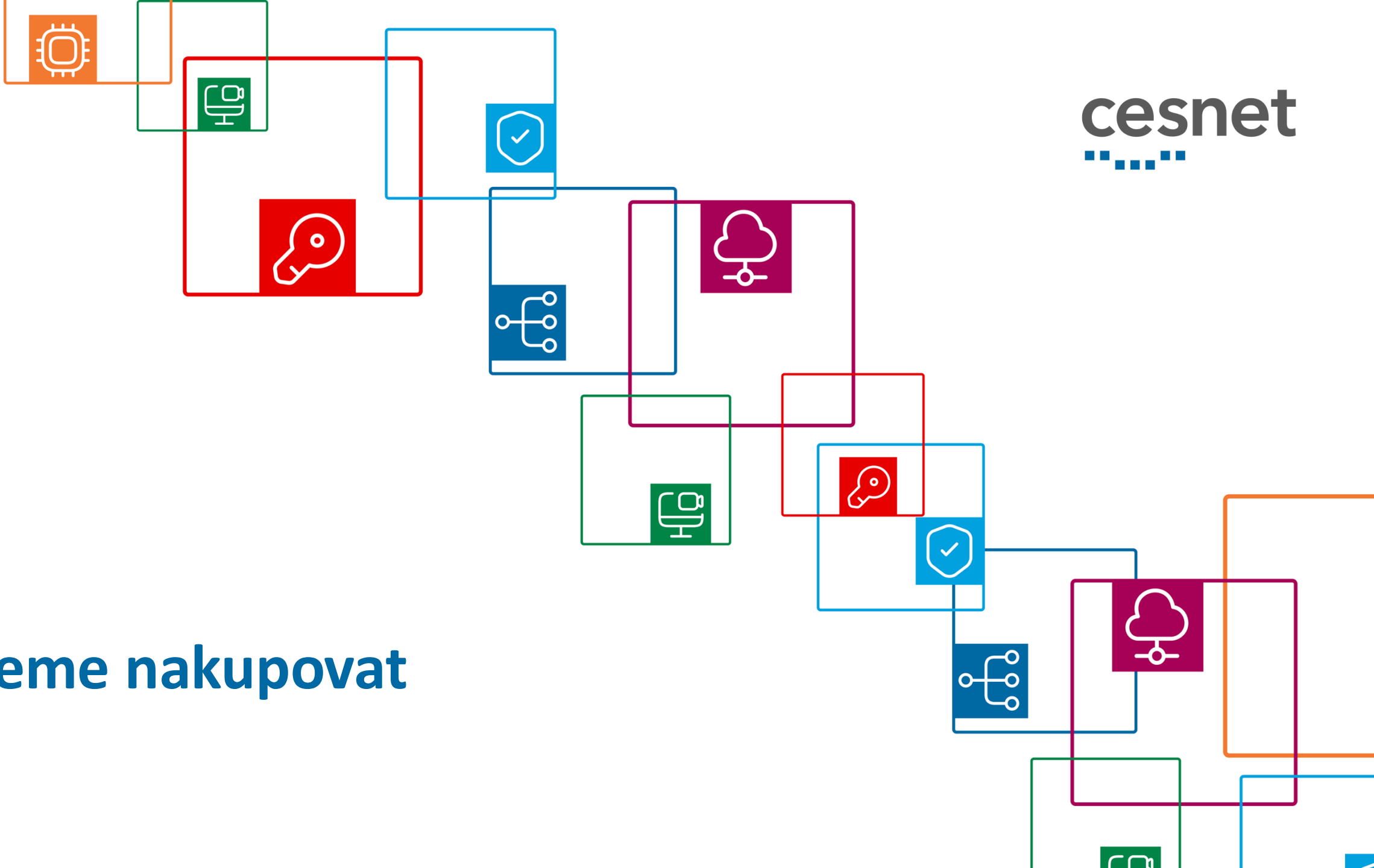
Kde začít

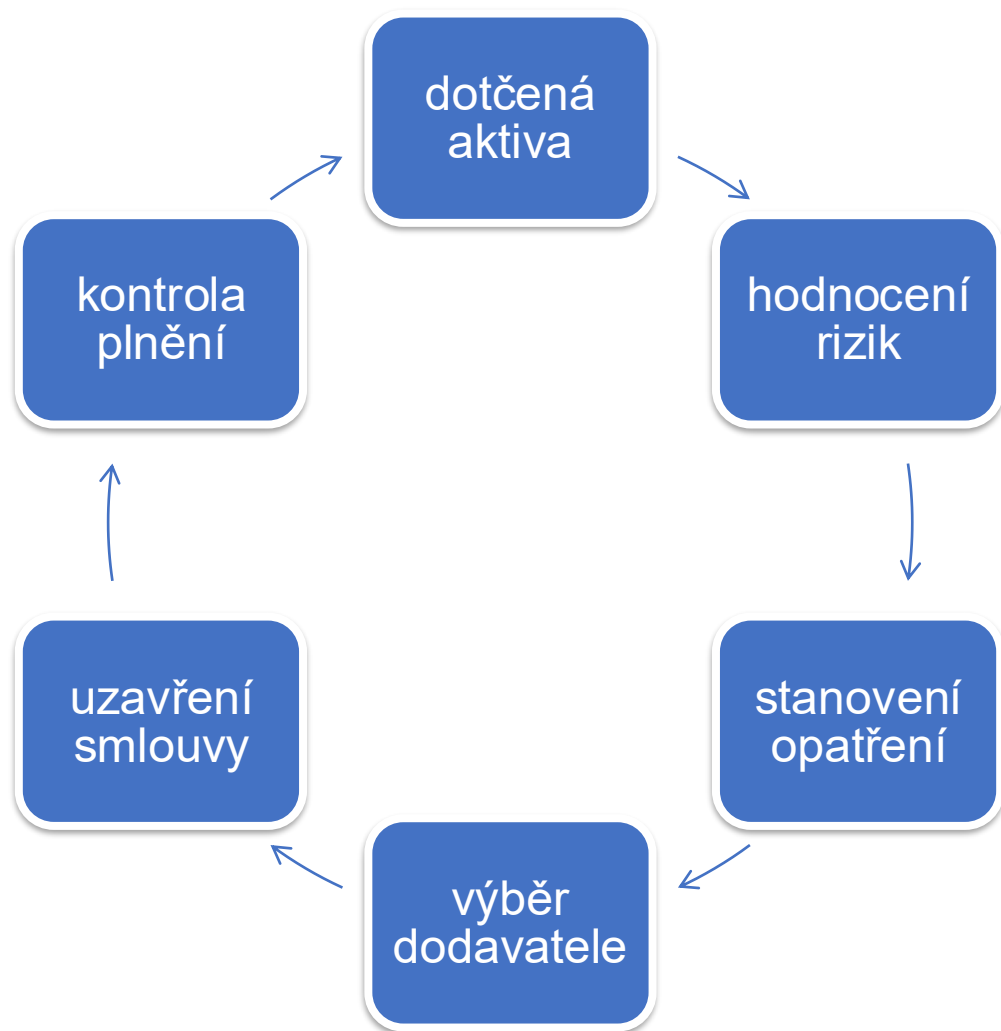


- identifikace regulované služba
- určení aktiv, která tvoří regulovanou službu
- identifikace dodavatelů, kteří mají na aktiva dopad
 - vyhodnotit rizika související s dodavatelem (AR)
 - určit bezpečnostní opatření pro snížení rizik (co potřebujeme od dodavatele, co musíme udělat interně)
 - porovnat požadavky s realitou – dohledat smlouvu
 - v případě potřeby vstoupit do jednání (smlouvu nelze měnit jednostranně!)

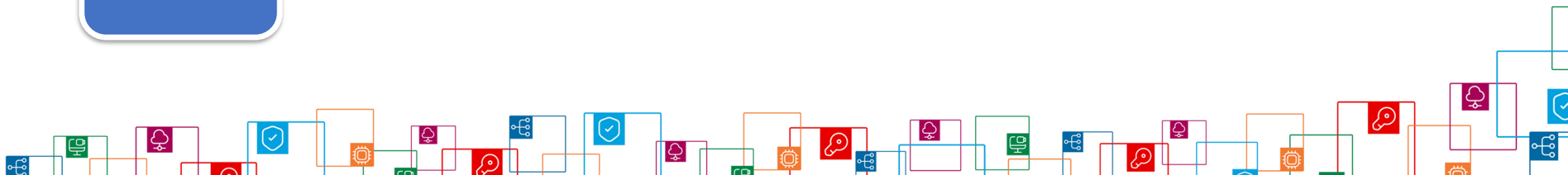


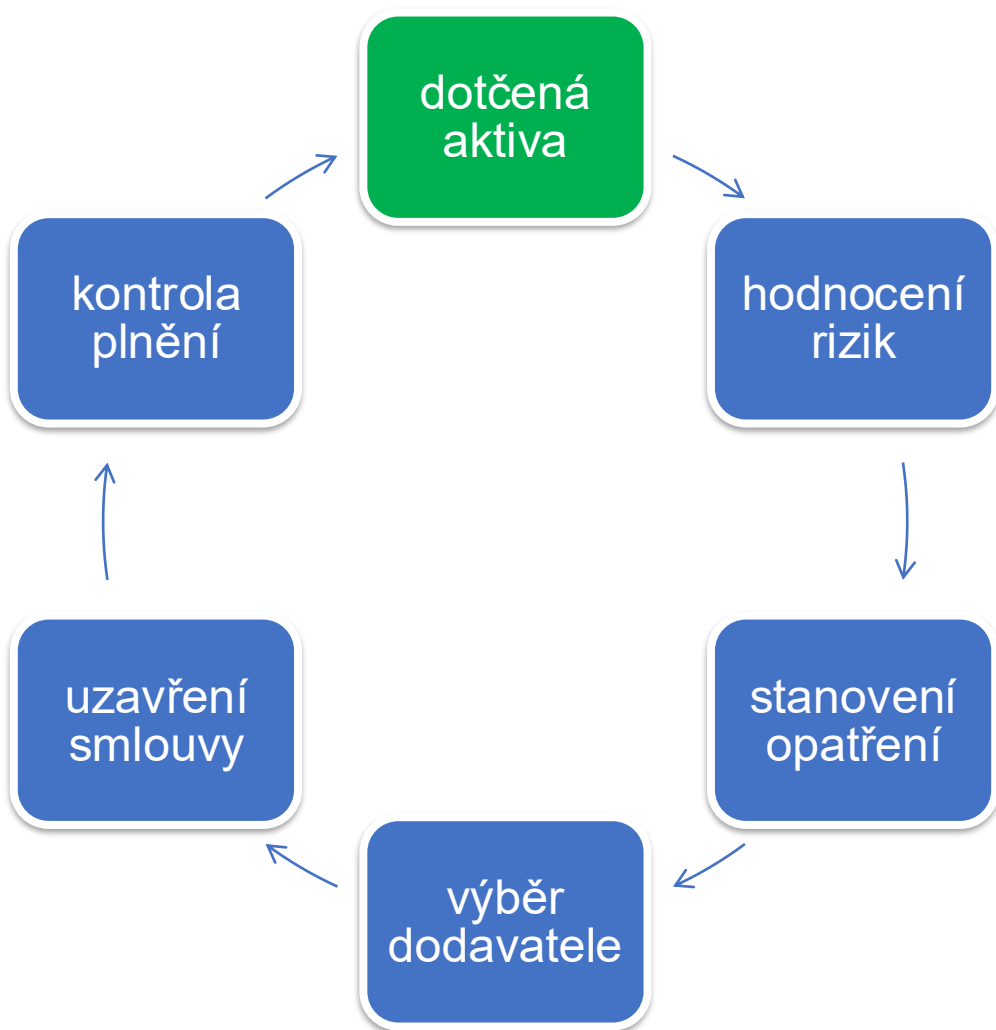
Jdeme nakupovat





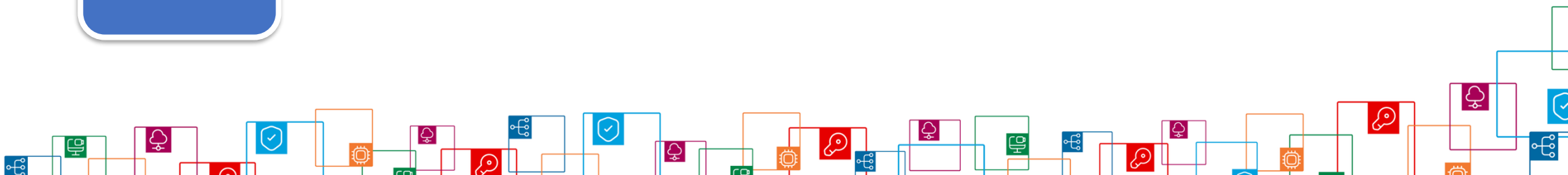
- vhodné vycházet z „životního cyklu dodavatele“
 - od definice předmětu plnění po exit strategii
- povinnost řídit rizika spojená s dodavateli (režim vyšších povinností)

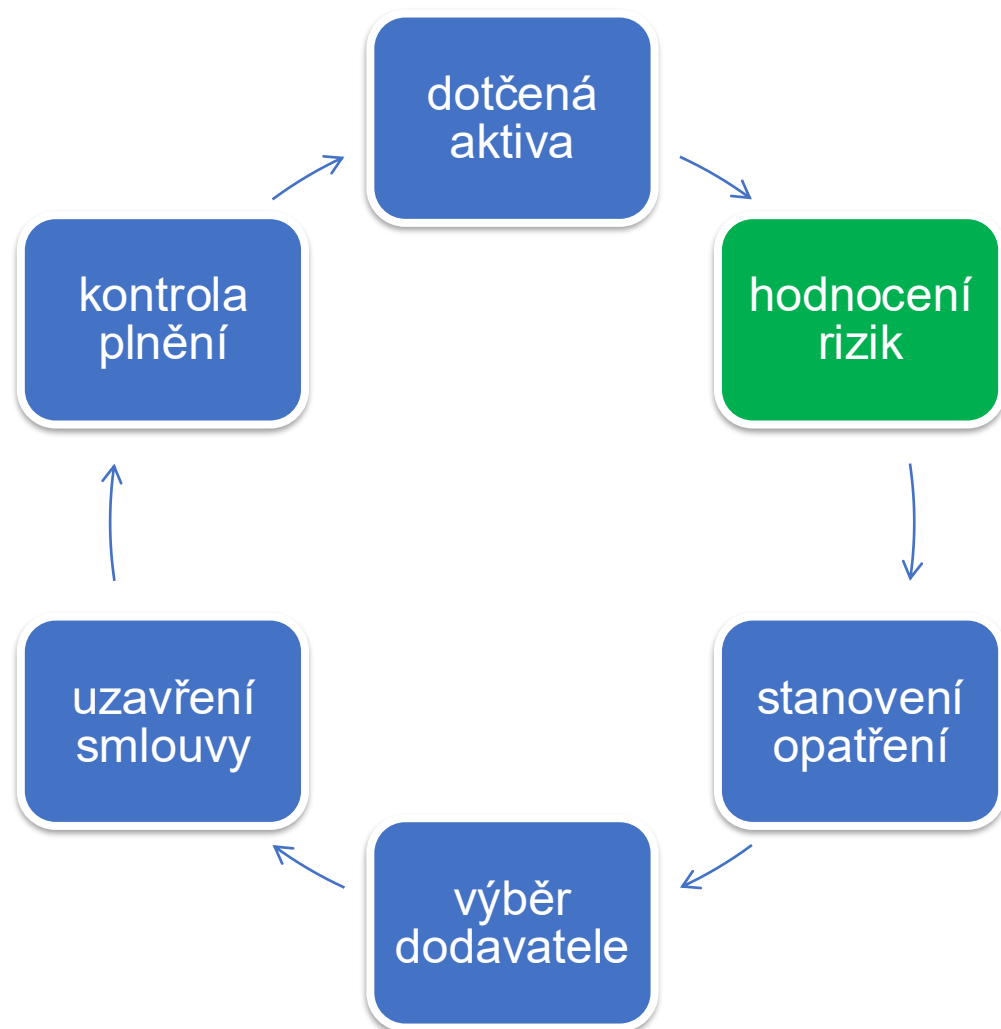




■ identifikace dotčených aktiv

- máme stanovený rozsah řízení kybernetické bezpečnosti – evidence aktiv
- máme udělanou AR ke všem aktivům
- máme stanovená bezpečnostní opatření ke snížení rizik
- máme bezpečnostní politiky





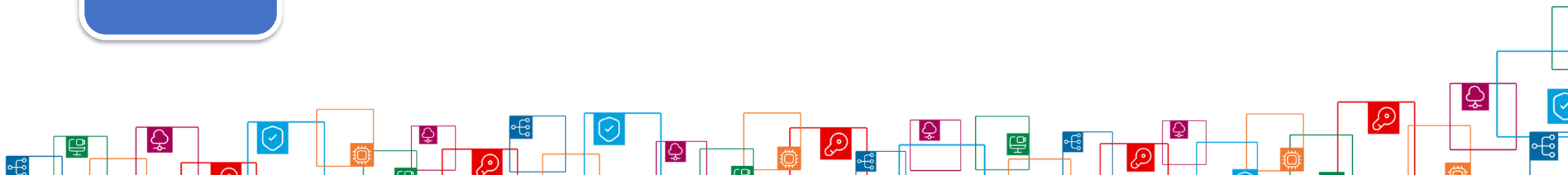
■ hodnocení rizik spojených s dodavatelem

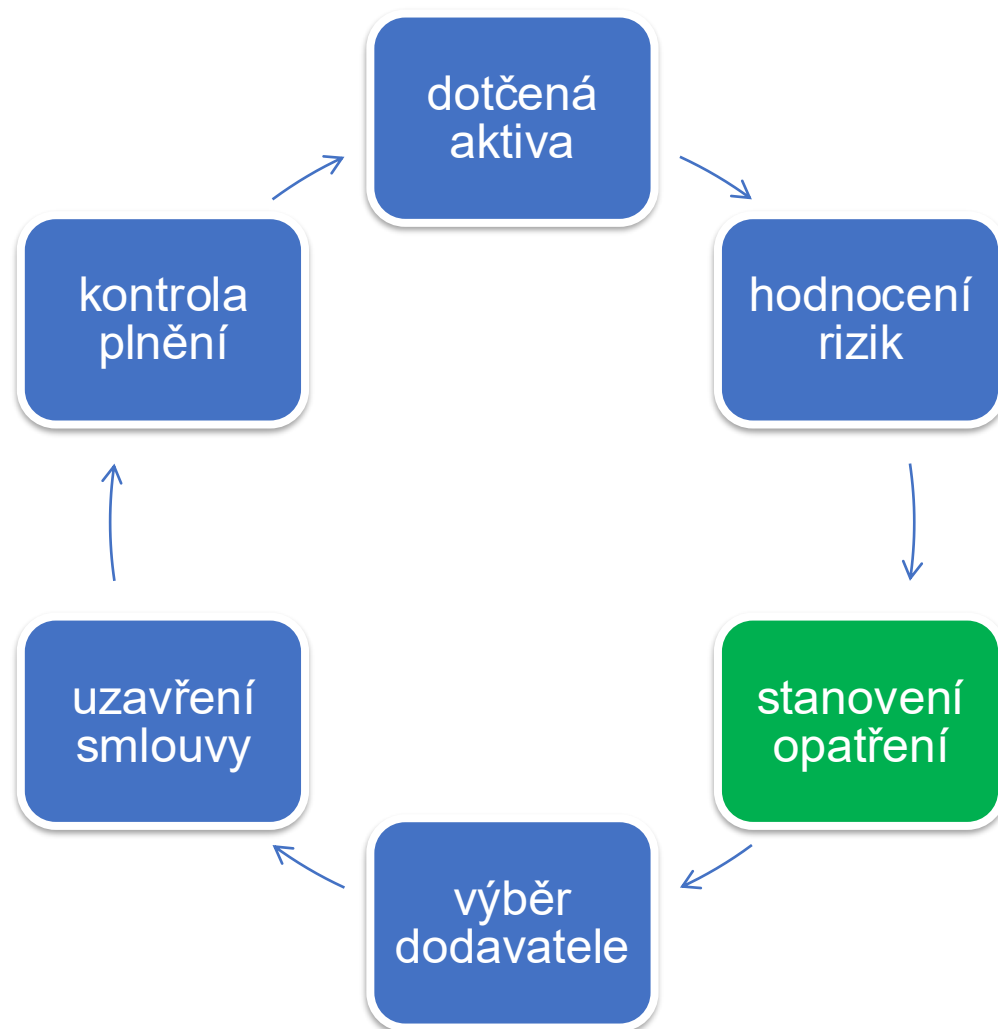
■ revize a doplnění AR

= před čím budu aktiva chránit, jak může dodavatel narušit jejich bezpečnost

- mám identifikovaná všechna relevantní rizika?
- je správně určena jejich hodnota?

■ zohlednit AR k protiopatřením NÚKIB

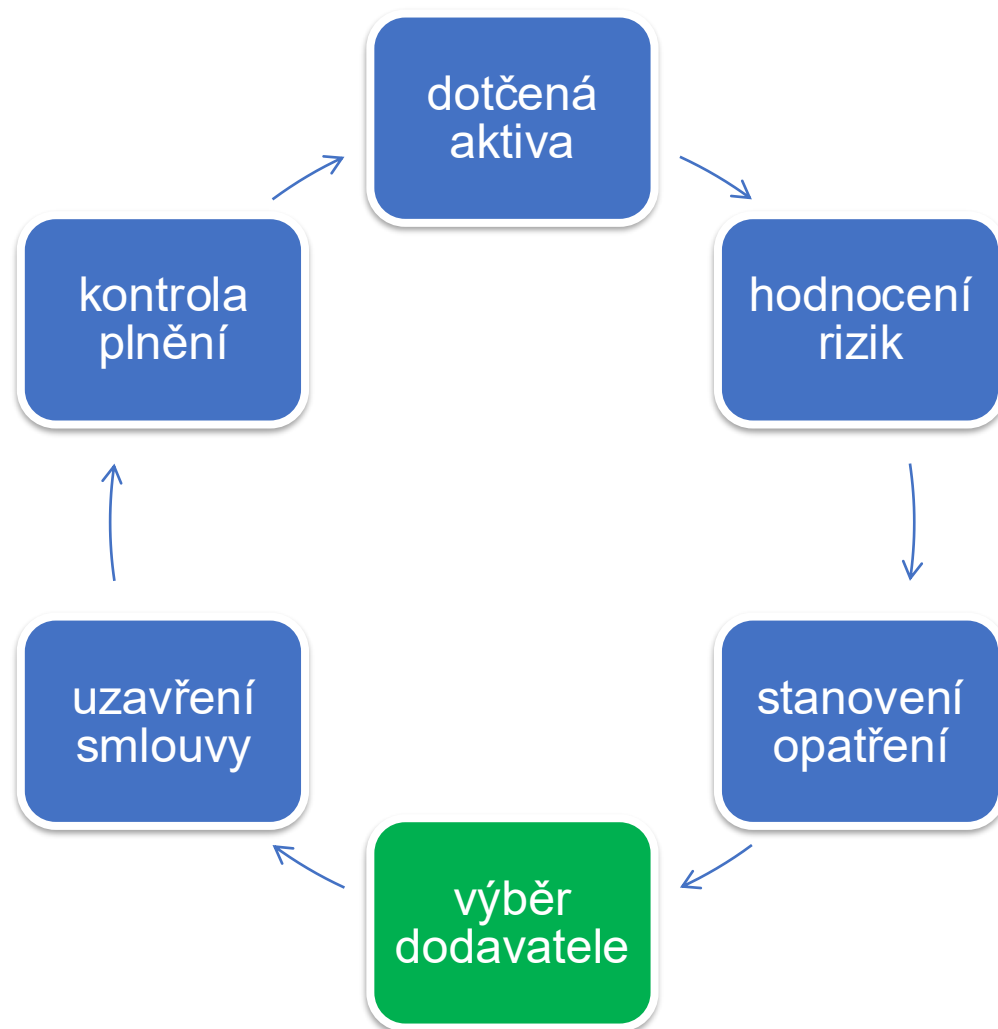




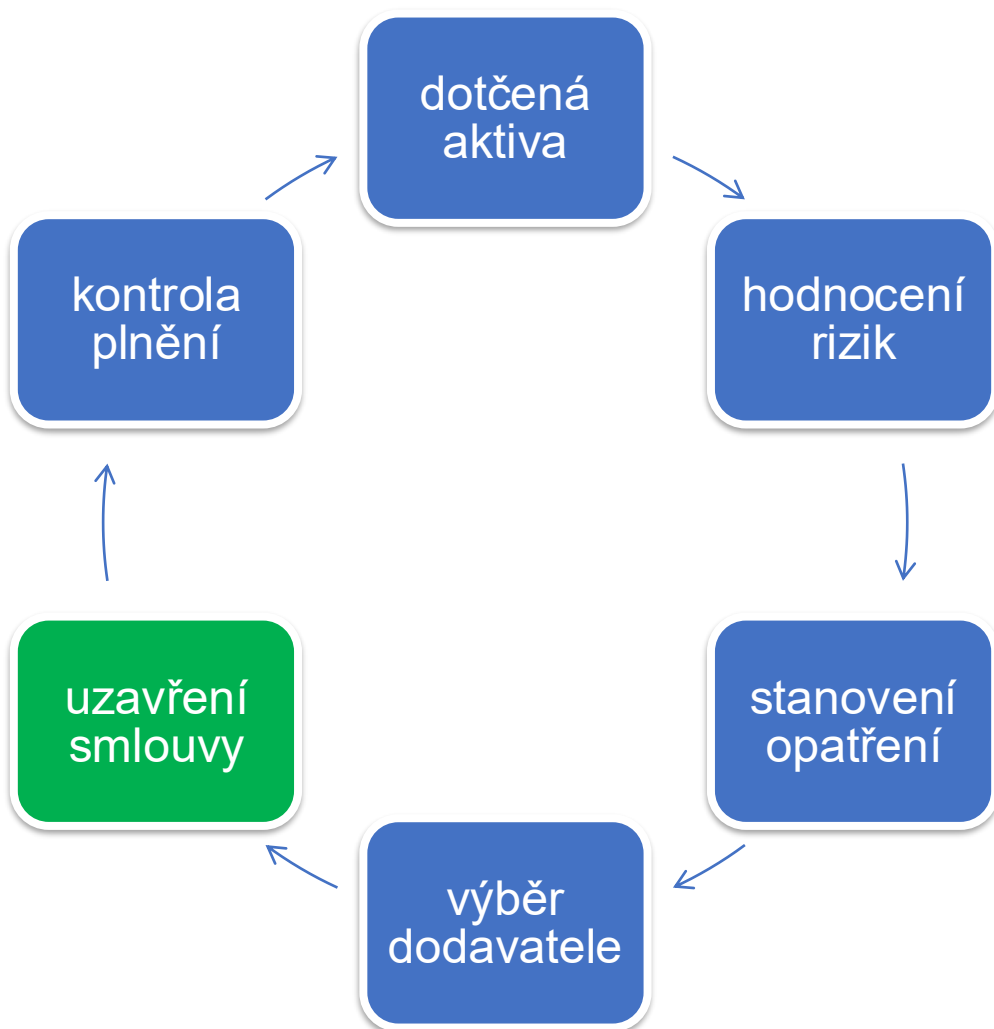
- **stanovení bezpečnostních opatření**
 - **revize a doplnění bezpečnostních opatření**

= jak budu aktiva chránit, co budu chtít po dodavateli a co je potřeba vyřešit interně

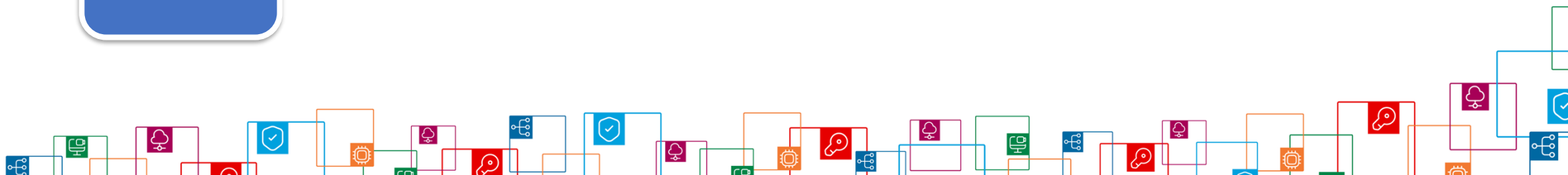
 - není potřeba upravit/přidat nějaké bezpečnostní opatření?
 - jak se projeví ve smlouvě?
 - **zohlednit opatření k protiopatřením NÚKIB**



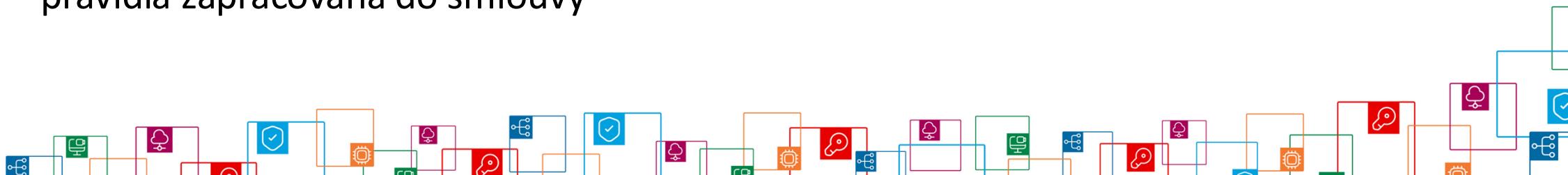
- specifikace pravidel pro výběr dodavatele
 - vycházím ze stanovených bezpečnostních opatření z předchozího kroku
 - podle toho upravit zadání (požadavky na předmět a kvalitu plnění)
 - pozor na veřejné zakázky a bezdůvodné překážky hospodářské soutěže



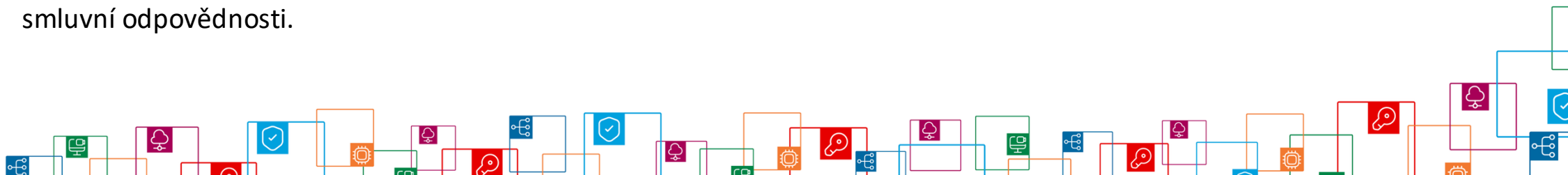
- své požadavky na smluvní podmínky musím zohlednit už při výběru dodavatele
- „pravidla pro dodavatele“
 - požadavek vyhlášky pro vyšší režim
- „povinné náležitosti smlouvy s dodavateli“
 - příloha vyhlášky pro oba režimy

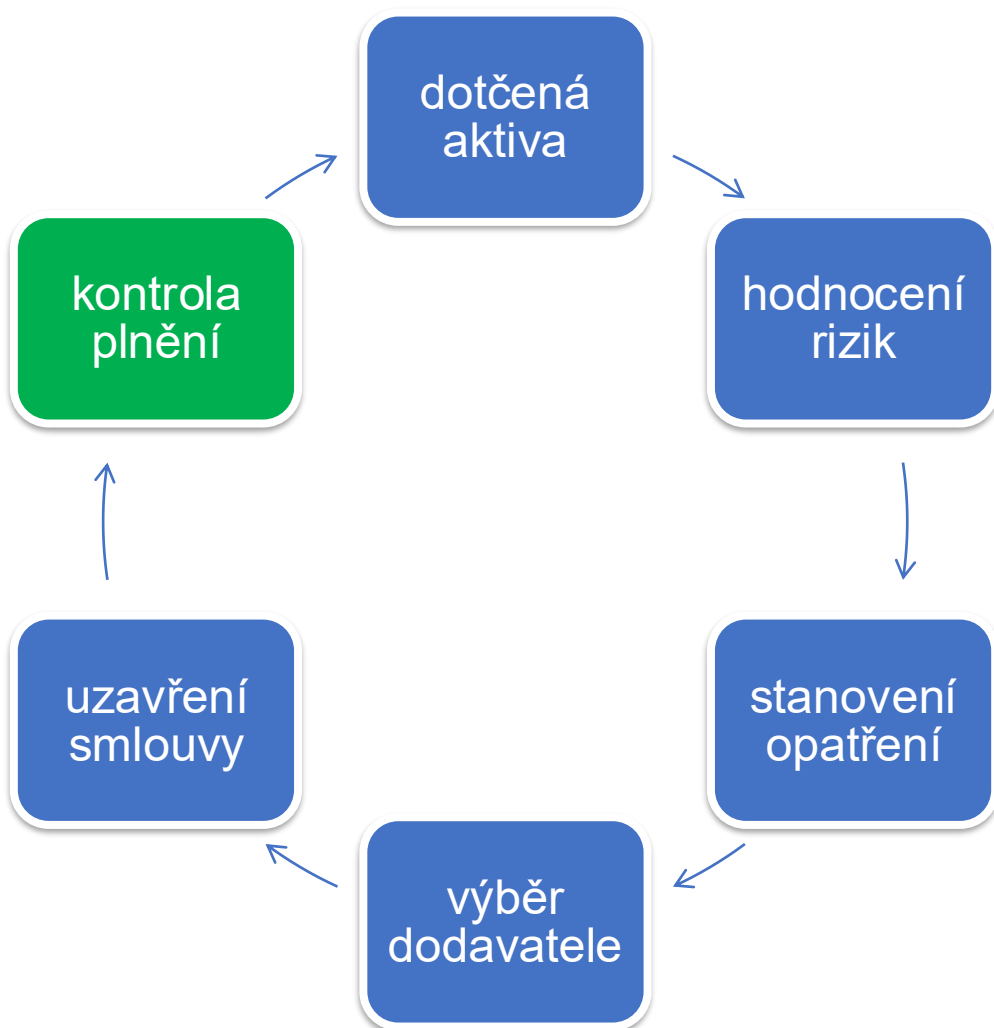


- Povinná osoba při řízení dodavatelů...
 - ... stanoví **pravidla pro dodavatele**, která zohledňují požadavky systému řízení bezpečnosti informací
 - ...prokazatelně **seznamuje** své dodavatele s těmito pravidly
 - ... a **vyžaduje** jejich plnění
- sdružení CESNET:
 - speciální pravidla a školení
 - povinnost dodržovat předložené bezpečnostní politiky
 - pravidla zapracovaná do smlouvy



- Příloha č. 5 Řízení dodavatelů - bezpečnostní opatření pro smluvní vztahy:
 - **RELEVANTNÍ!** S ohledem na předmět plnění a výsledky hodnocení rizik...
- Nezapomenout zejména na:
 - ujednání o mlčenlivosti dodavatele o interních a chráněných informacích sdružení CESNET,
 - ujednání ohledně zpracování osobních údajů,
 - licenční či obdobné ujednání na ochranu duševního vlastnictví sdružení CESNET,
 - povinnost dodavatele oznamovat neobvyklé chování dotčeného informačního či komunikačního systému a podezření na jakékoliv zranitelnosti,
 - opatření přijatá za účelem eliminace konkrétních rizik
 - ujednání pro případ ukončení smlouvy s dodavatelem (tzv. exit strategy)
 - sankce pro dodavatele za porušení smluvních podmínek z oblasti bezpečnosti informací,
 - povinnost dodavatele dodržovat relevantní politiky či absolvovat relevantní školení z oblasti bezpečnosti informací,
 - povinnost podrobit se kontrole či testování (např. pentesty)
 - další potřebná ujednání o úrovni služeb a způsobů a úrovni realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.





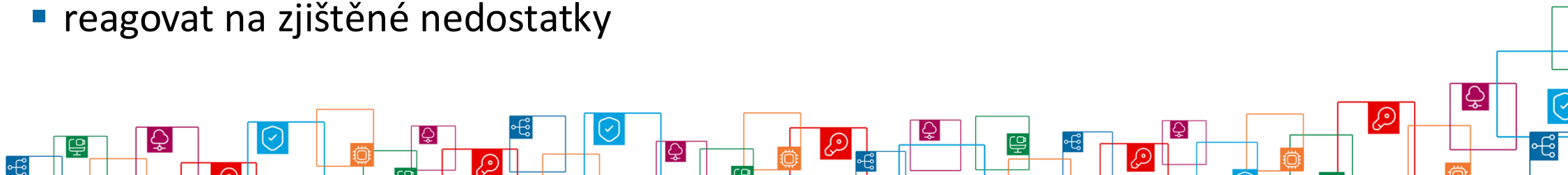
■ hodnocení a kontrola dodavatele

- plní?
- reklamace?
- komunikace?
- nějaké KBU/KBI?
- jiné?

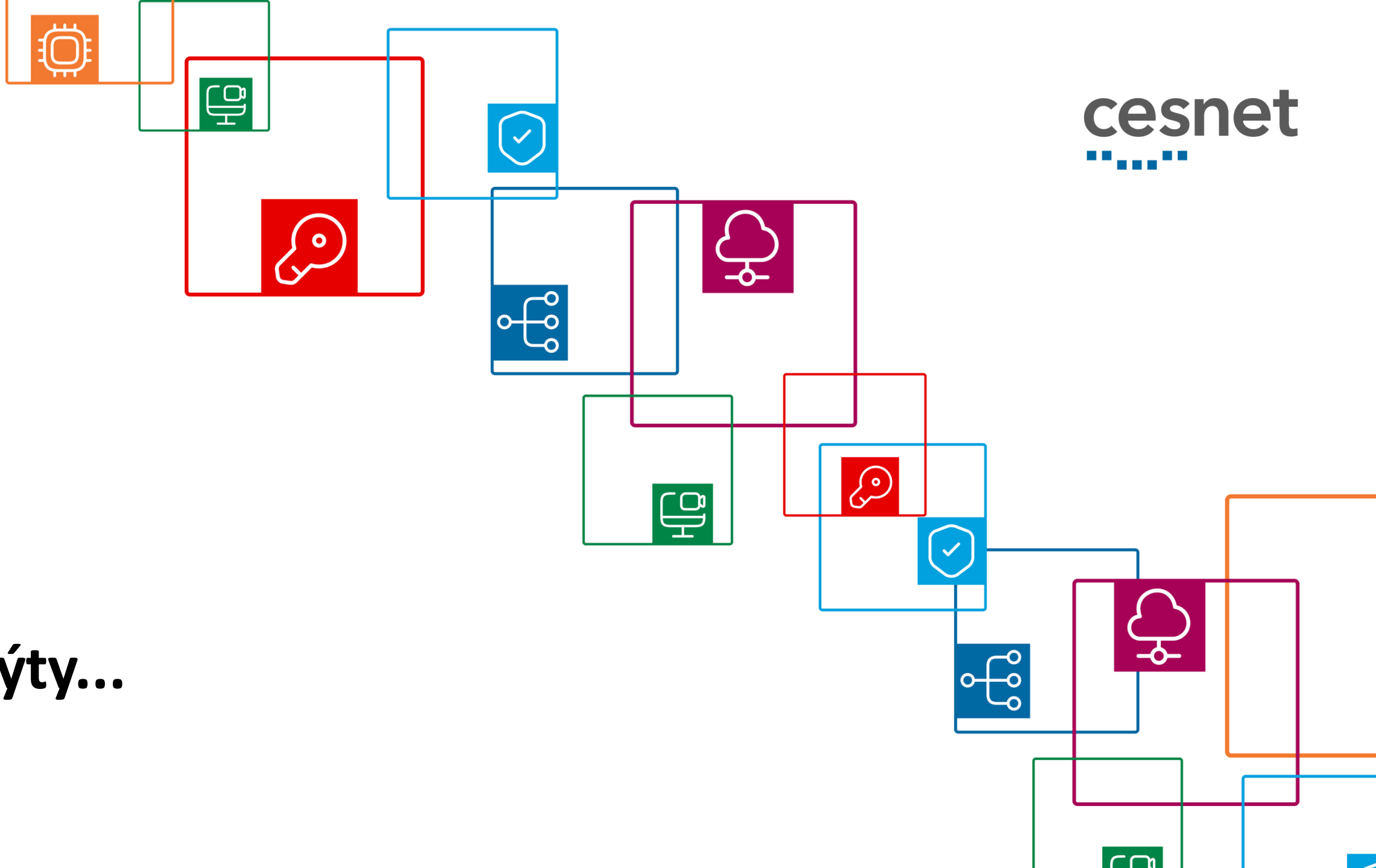
■ opakovaný a soustavný proces!

- v AR zohlednit, že máme dodavatele a výsledky jeho hodnocení
- u bezpečnostních opatření přehodnocovat dle výsledků hodnocení = **vyvození důsledků**
- ve sdružení CESNET:
garant průběžně, MKB při AR

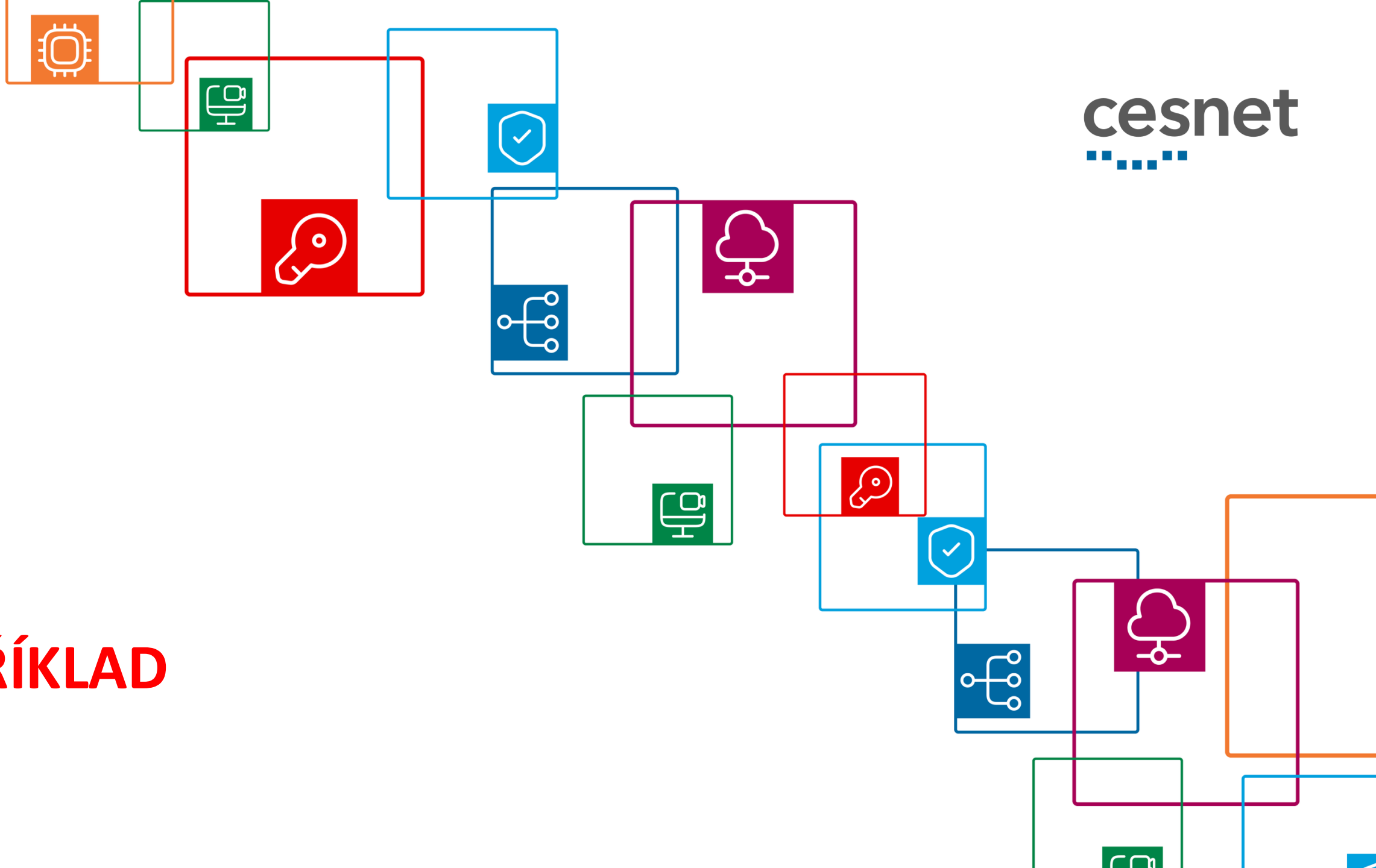
- u režimu vyšších povinností
- ten, kdo poskytuje plnění, které je **významné z hlediska zajištění kybernetické bezpečnosti** regulované služby
 - tj. nejde o velikost zakázky
- **výslovné povinnosti:**
 - identifikovat a evidovat významné dodavatele
 - informovat významné dodavatele o zařazení do evidence
 - zařadit do smlouvy přílohu č. 5 vyhlášky
 - přezkoumávat
 - provádět AR a stanovovat bezpečnostní opatření
 - pravidelně kontrolovat AR a bezpečnostní opatření
 - reagovat na zjištěné nedostatky



Mýty...



PŘÍKLAD



- ZZVZ a nZKB stojí vedle sebe, je nutné dodržet oba
- výstupy z AR musím zohlednit v zadávacích podmínkách
- bezpečnostní opatření mohou fakticky omezit hospodářskou soutěž
X není to nedůvodné
- podkladem musí být kvalitně zpracovaná AR, kterou je potřeba na vyžádání předložit ÚOHS
- zohledňovat i protiopatření NÚKIB (všechna, nejen varování)

MATERIÁL NÚKIB:

https://portal.nukib.gov.cz/storage/uploads/2026/06/09/zadavani-verejnych-zakazek-v-ict_v1_uid_6a2810b138c8d.pdf



Děkujeme za pozornost
... Otázky?

