SPCSS

Státní pokladna
Centrum sdílených služeb

Poskytovatel služeb datových center

a služeb kybernetické bezpečnosti

pro státní správu

Analýza rizik předmětu veřejné zakázky
BEST PRACTICE

SPCSS – Ondřej Nekovář, Arnošt Sarvaš

CyberCon 2022, Brno

14. 09. 2022

Státní pokladna Centrum sdílených služeb, s. p.

Intro

Státní pokladna Centrum sdílených služeb, s. p.

Intro

About Us

- **Ondřej Nekovář**
- **Arnošt Sarvaš**

Státní pokladna Centrum sdílených služeb, s. p.

Intro

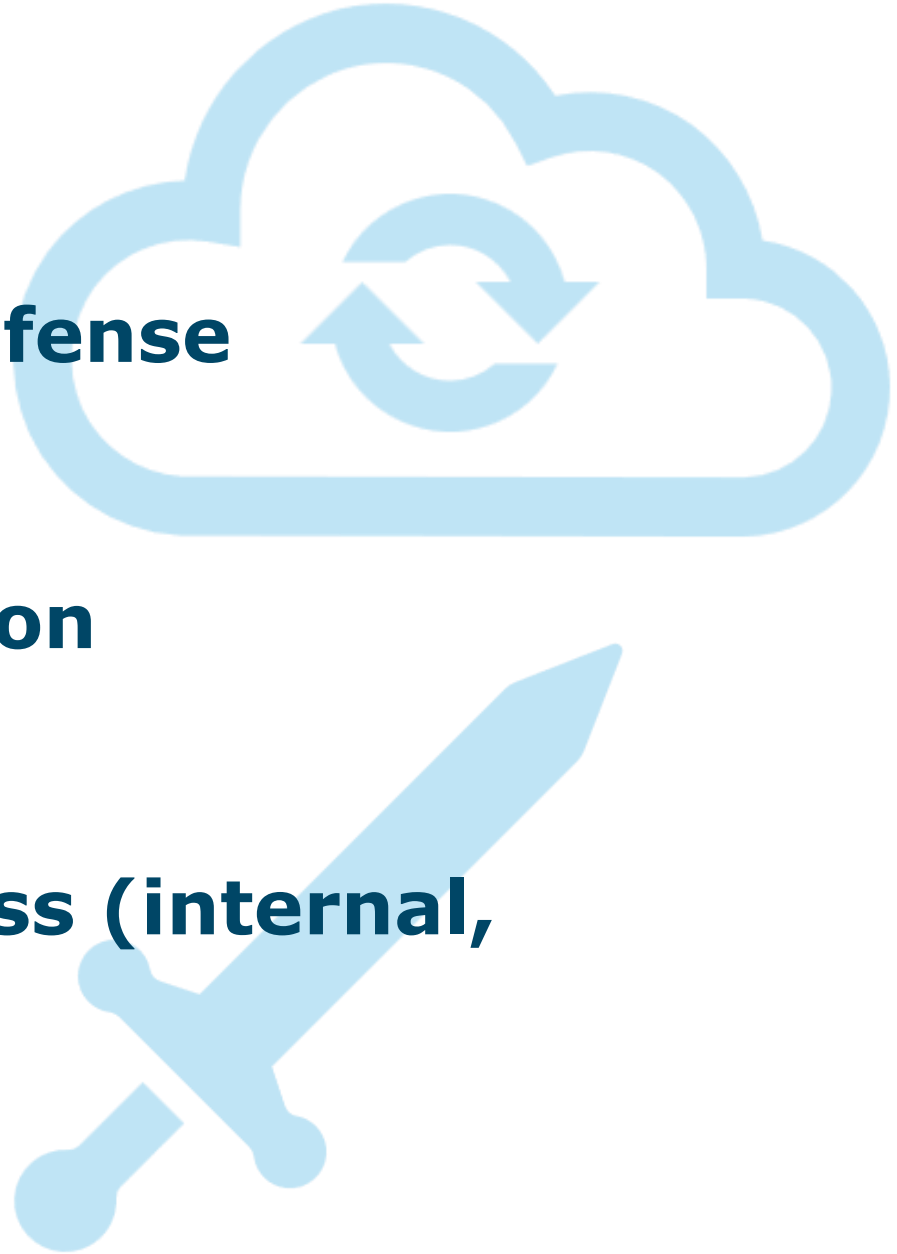
Our topics

- **DC, Cloud, Hybrid-cloud bezpečnost**
- **Resort MF**
- **Rizika Aktivní kybernetické obrany**

Intro

Our business

- **SOC**
- **Threat-intel**
- **Incident response**
- **Vulnerability**
- **Threat hunting**
- **Adversary emulation**
- **Active defense**
- **Identity**
- **Integration**
- **Risk**
- **Awareness (internal, external)**
- **Policy**



Intro

Our goals

- **Resortní centrum kybernetických operací MF**
- ***Dohledové centrum státní části eGC***
- **NPO Program - Vybudování eGovernment cloudu**

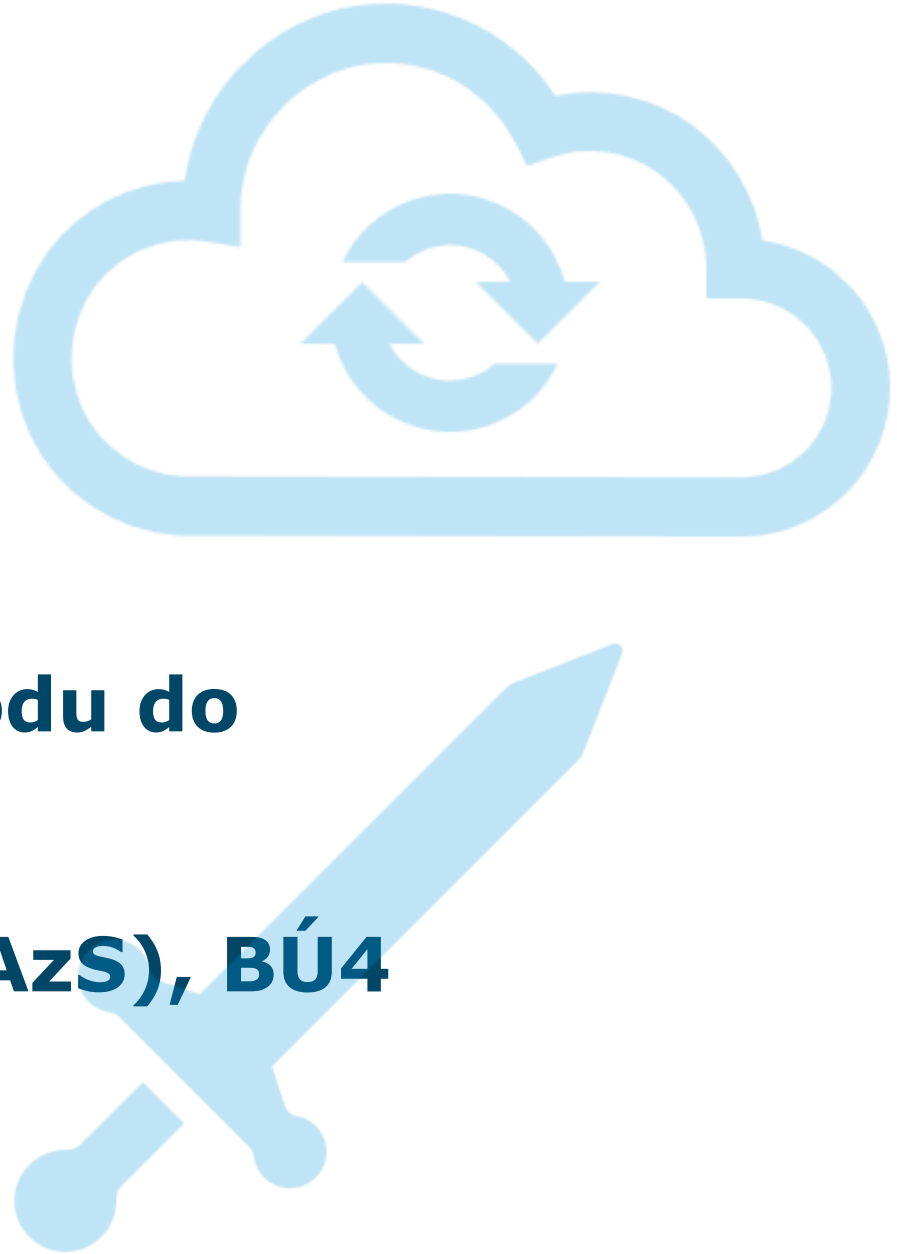
Intro

Our „Resort“ projects

- **Deception platform**
- **Threat-intel platform**
- **Incident response platform**
- **Passwordless**
- **SOCCRATES**

Intro

Our „eGC“ projects

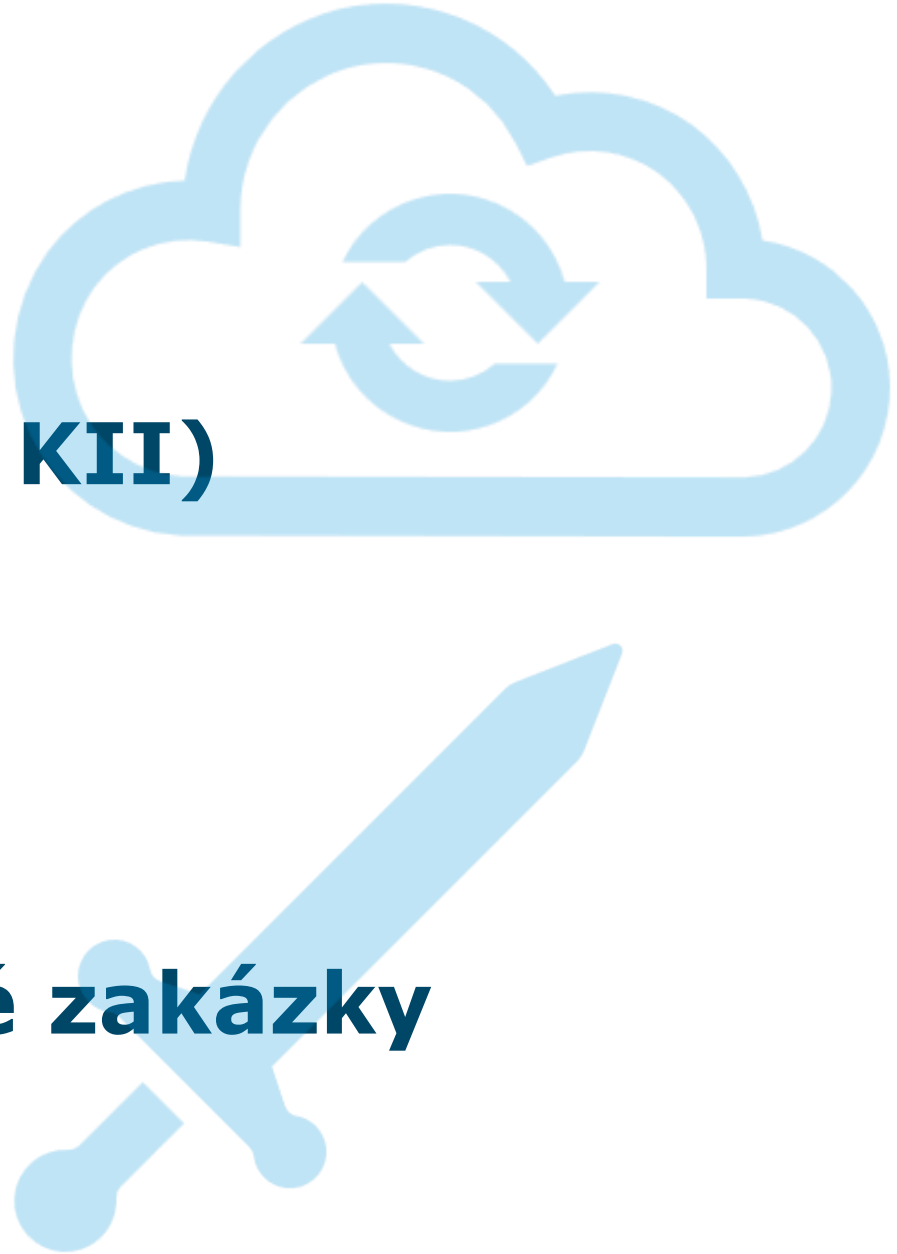


- **Příprava na provozování státní části eGC**
- **Assessment pro IS BÚ4 k přechodu do státní části eGC**
- **Realizace SOC2® - BÚ3 (Azure, AzS), BÚ4**

Risk business

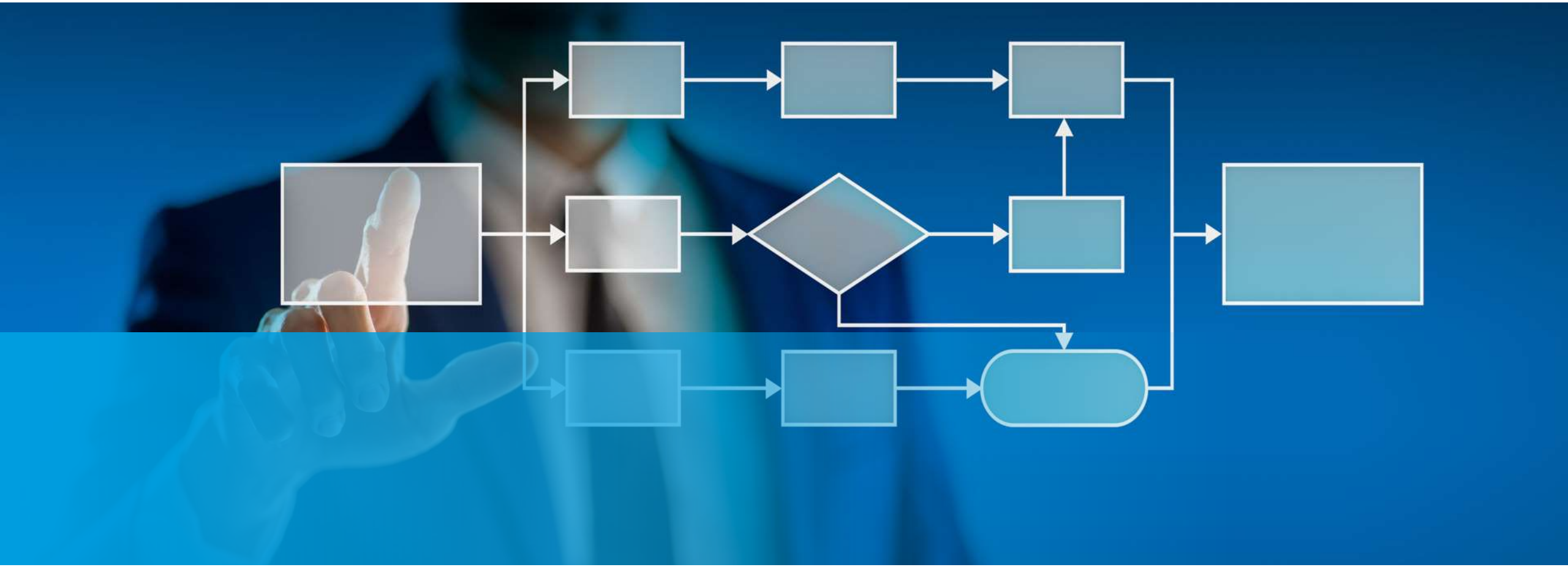
Intro

Risk business



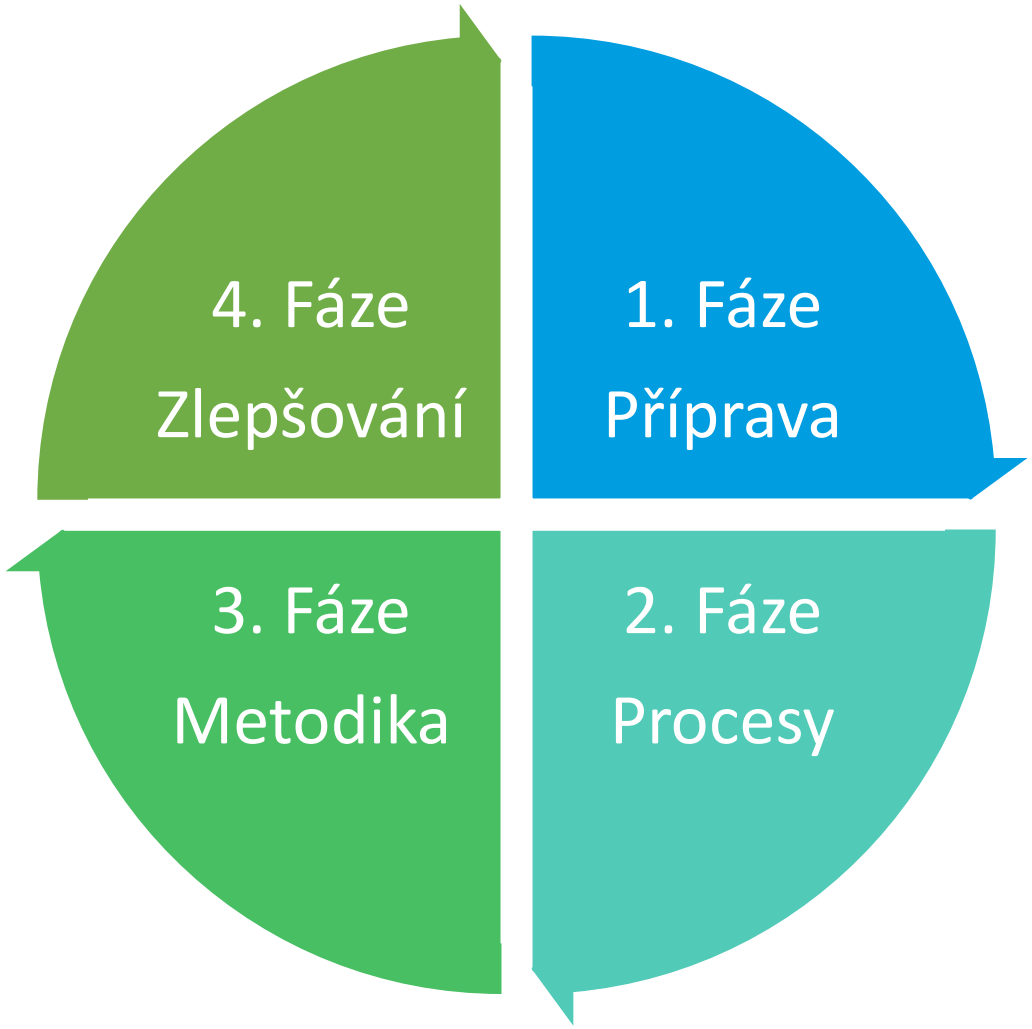
- **Analýza rizik dle VoKB (VIS, KII)**
  - **Vstupní**
  - **Pravidelné**
  - **Významné změny**
- **Analýza rizik předmětu veřejné zakázky**

Zavedení



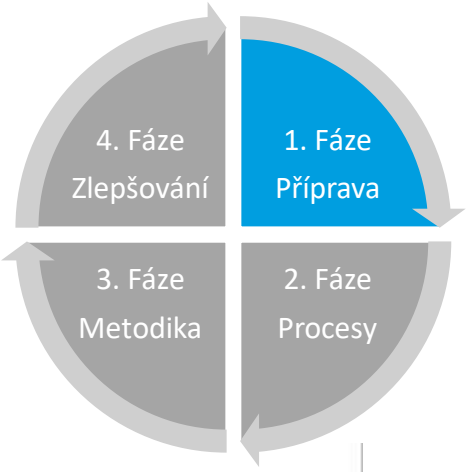
Best practice

Soulad s VoKB



Best practice

1. Fáze - Příprava



- **§ 8 VoKB**

(2) Povinná osoba u významných dodavatelů dále

a) v rámci výběrového řízení a před uzavřením smlouvy provádí hodnocení rizik souvisejících s plněním předmětu výběrového řízení přiměřeně podle přílohy č. 2 k této vyhlášce,

b) v rámci uzavíraných smluvních vztahů stanoví způsoby a úrovně realizace bezpečnostních opatření a určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření,

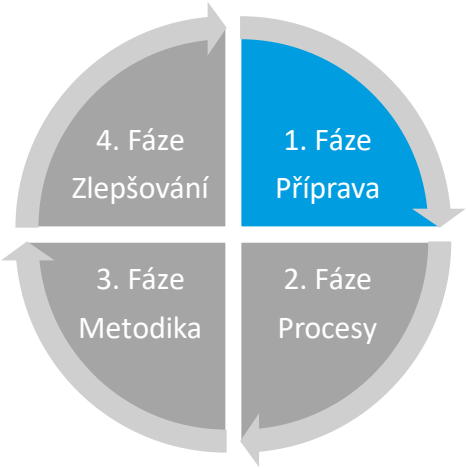
c) provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a

d) v reakci na rizika a zjištěné nedostatky zajistí jejich řešení.

- **Významný dodavatel**
- **Analýza související s plněním předmětu VZ**

Use-case

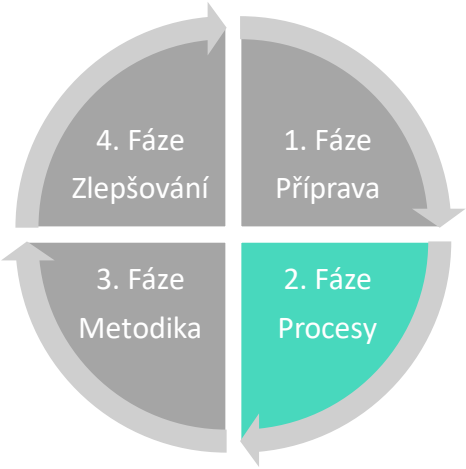
1. Fáze - Příprava



- **Varování ze dne 17. 12. 2018**
  - **Podpůrné materiály k varování**
  - **Soulad se Zákonem č. 134/2016 (ZZVZ)**

Use-case

2. Fáze - Procesy



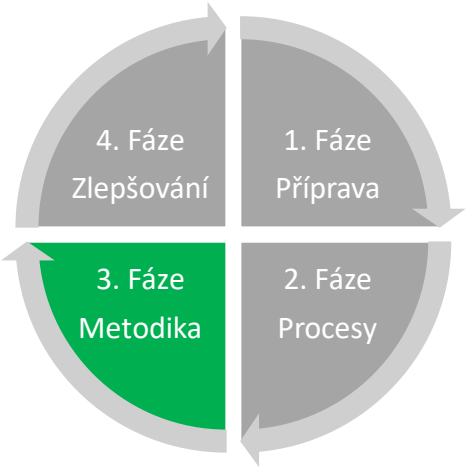
- **Domluva mezi úseky**
- **Změna v dokumentaci**
  - **Interní postupy**
  - **Směrnice**
  - **Formuláře**
- **Proces posouzení veřejných zakázek**
  - **Odpovědnosti**
  - **Lhůty**

Metodika

Státní pokladna Centrum sdílených služeb, s. p.

Use-case

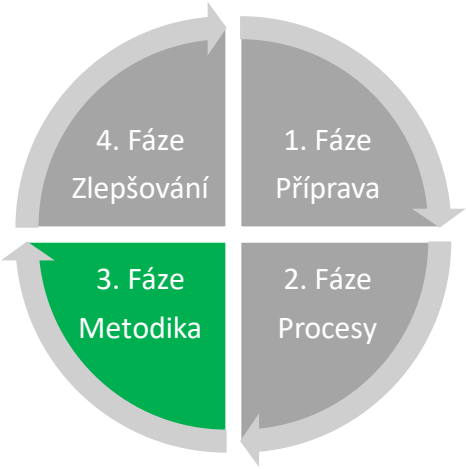
3. Fáze - Metodika



- **Tvorba metodiky ARVZ**
  - **Vychází z metodiky AR kybernetické bezpečnosti**
  - **Je zjednodušena dle požadavků VoKB**
  - **Konzultováno s NÚKIB**
  - **Praktický test**
  - **Vydání**

Use-case

3. Fáze - Metodika



- **Kvalitní metodika**
  - **Je použitelná a dokážeme ji vysvětlit!**
  - **ÚOHS – kvalitní metodika je základ**

ČÍSLO JEDNACÍ: **S0358/2019/VZ-01269/2020/512/KMO**

Instance	I.
Věc	Obnova páteřní a přístupové infrastruktury
Účastníci	1. Metropolnet, a.s. 2. Huawei Technologies (Czech) s.r.o.

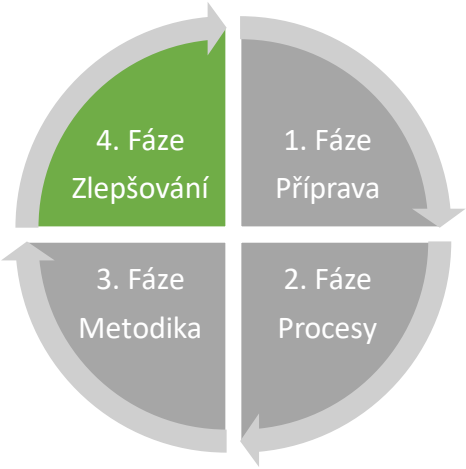
105. NÚKIB dále uvádí, že *„[p]o prostudování poskytnutých dokumentů NÚKIB konstatuje, že hodnocení rizik zadavatelem, jak bylo v předložených dokumentech prezentováno, ve vztahu ke konkrétní veřejné zakázce neodpovídá požadavkům obsaženým v ZKB a VKB.“*. Jako nedostatečnou NÚKIB shledává zejména *„identifikaci primárních a podpůrných aktiv a vazeb mezi nimi, výběr konkrétních podpůrných aktiv, na základě jejichž hodnocení došlo k zákazu použití prostředků dotčených obchodních společností v zadávacím řízení, dále lze identifikovat určitou zmatečnost a nejednotnost v popisu stupnic pro hodnocení jednotlivých proměnných vzorce pro výpočet hodnoty rizika a v popisu samotného vzorce a v neposlední řadě též nesprávné zohlednění varování NÚKIB ze dne 17. 12. 2018 při stanovení hodnot jednotlivých proměnných vzorce pro výpočet rizika (zejm. došlo nejen k úpravě hodnoty hrozby, ale na některých místech též k úpravě hodnoty zranitelnosti).“*. NÚKIB dále uvádí, že předložené materiály pak prezentují postupy hodnocení rizik jak podle pravidel normy ISO 27001, tak podle pravidel obsažených v ZKB a VKB a není tak zřejmé, *„zda a z jakého důvodu zadavatel provádí či hodlá provádět dvojí hodnocení rizik. Žádné z těchto hodnocení však samo o sobě ani v souhrnu nevyhovuje kompletním požadavkům ZKB a VKB.“*.

106. Postup zadavatele při hodnocení rizik a při navazujícím výběru bezpečnostního opatření je tedy z pohledu NÚKIB *„nedostatečně zdokumentován a je obecně (pro nezainteresovanou osobu) neopakovatelný a zmatečný. Stejně tak je zmatečný i samotný způsob zpracování varování NÚKIB ze dne 17. 12. 2018 do procesu hodnocení rizik. Z výše uvedených důvodů pak postup zadavatele nelze označit za souladný se ZKB a VKB.“*.

Zlepšování

Use-case

4. Fáze - Zlepšování



- **Máme metodiku, ale tím to nekončí**
  - **Neustále zlepšování díky praxi**
  - **Nová Varování**

Počet posouzení veřejných zakázek	Počet provedených analýz
172	více než **20**

Future


56
24%
67%
9%
945.3454
241
86%
01.52.87.5523
8%
12.06.2017
1350
23.734
25.92.23.734
002345
23.735
85%
145.3
12
32
62%
00.34.12.8522
0%
32%
75%
6%
40%
5.9223
75%
68%
120%
25.92.24.958

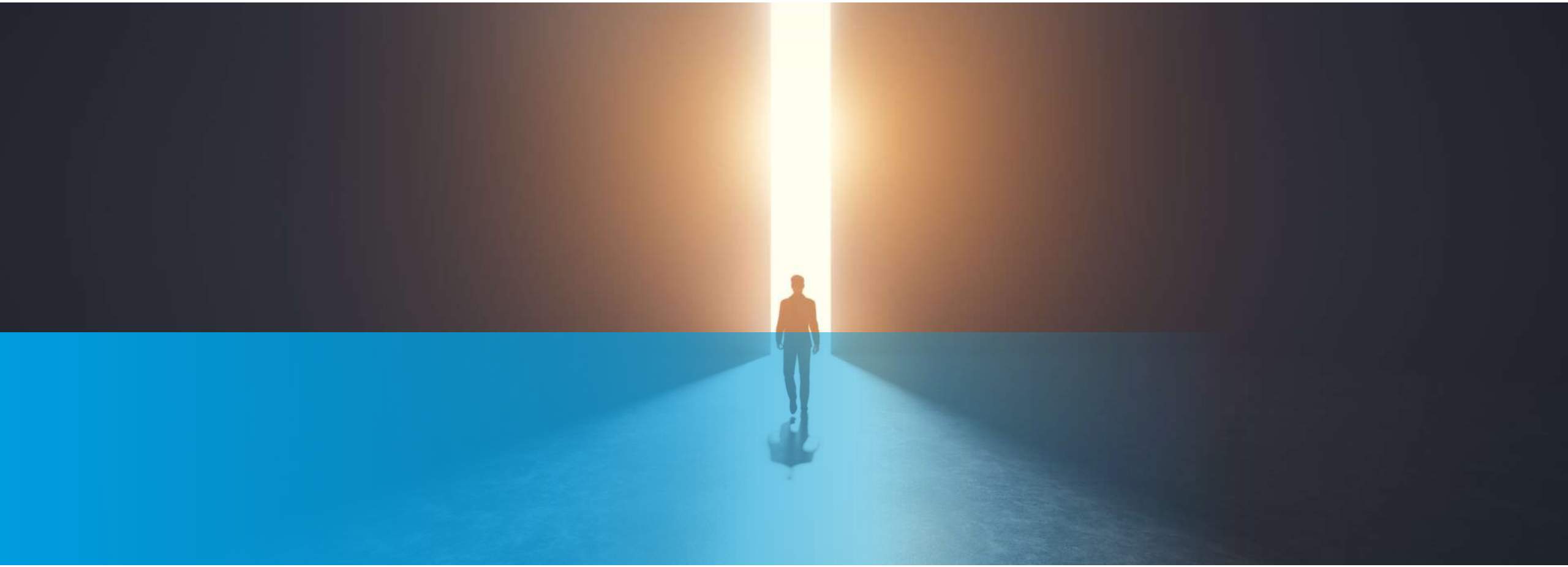
Future
Spolupráce

- **Příprava a vydání dokumentu:**

Analýza rizik předmětu veřejné zakázky

2Q/2023

EoF



Intro

We did

- **FAKO**
- **MISP training**
- **Odborné prezentace**
- **Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti**
- **Metodika AR předmětu veřejné zakázky**
- **Metodika zabezpečení kubernetes**

EoF

Community

Defcon Group 420 Czech republic

- www.DCG420.org

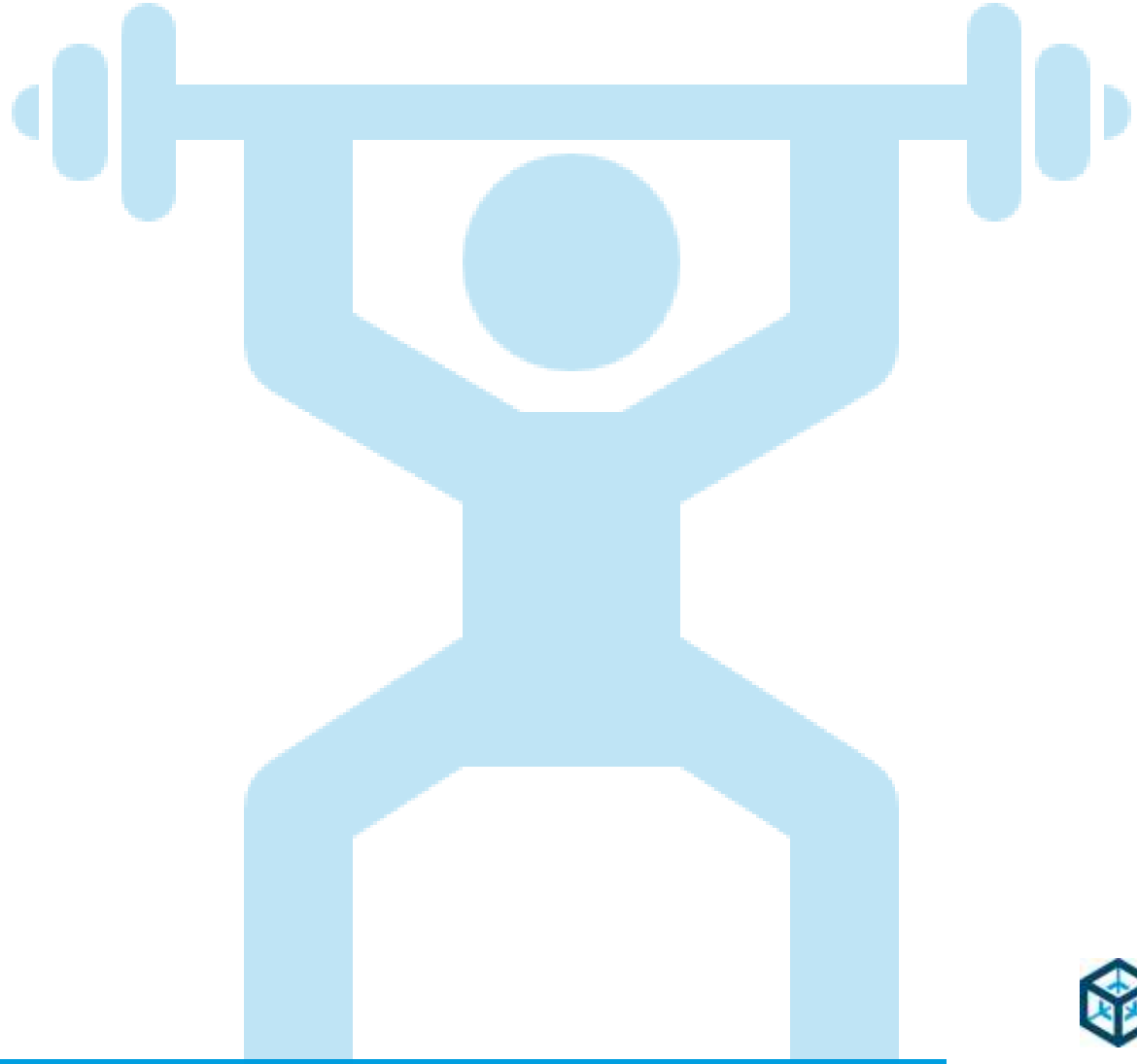
MeetUps

- DCG420.eventbrite.com

SPCSS

EoF

Our Training



MISP Training 2023

- 5. ročník - MISP, AIL, CyCAT
- **New: workflows, corellation**
- Zdarma – On-site/On-line
- Jaro 2023, anglicky

Registrace

- www.spcss.cz/misp

EoF

Our Conference

Fórum aktivní kybernetické obrany 2023

- 3. ročník
- Jaro 2023, česky

Registrace

- www.spcss.cz/fako

EoF

Keep in touch

- **www.spcss.cz/csirt**
- **E-mail csirt@spcss.cz**
- **Twitter @csirtspcss**

Děkujeme za pozornost

Q & A