



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Požiadavky na KB v MU pre CS zapisované do KsVC





MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

INFORMATIZÁCIA

Juraj Pankuch

Sekcia informačných systémov
verejnej správy

juraj.pankuch@vicepremier.gov.sk





MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Úvod



Východiská



Čo je Vládny cloud



Metodika zápisu CS do KsVC



Záver

Základné dokumenty

Zákon 305/2013 Z.z., §10a

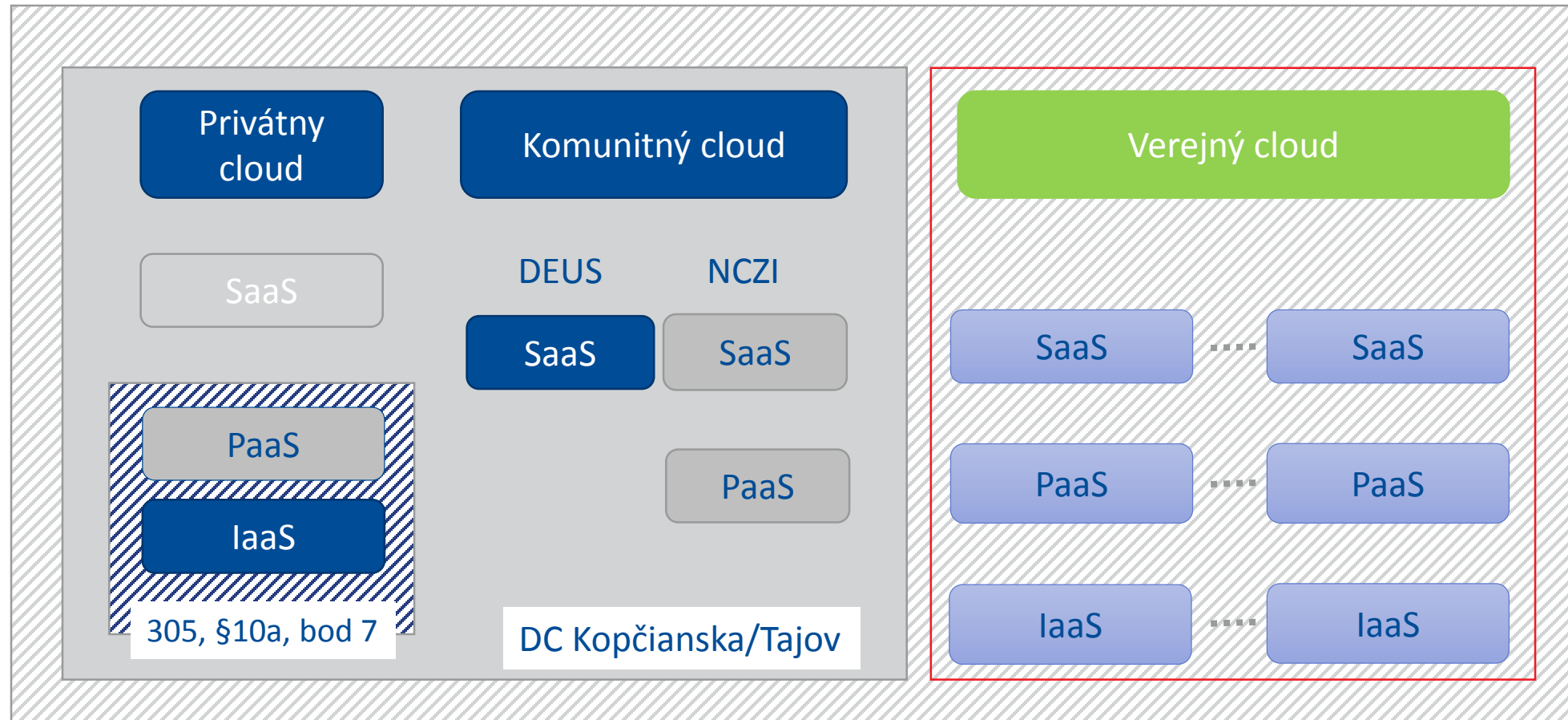
NKIVS, odsek 3.2.4 a SP vládny cloud

Uznesenie vlády 247/2014, bod B.6.

Zákon 95/2019 Z.z., §6



ČO je Vládny cloud



Dôvody pre akreditáciu - overenie zhody

- Zabezpečenie kvalitatívneho štandardu pre CS
- Zvýšiť povedomie a vzdelávať používateľov o kvalite a bezpečnosti cloudových služieb.
- Zlepšiť transparentnosť cloudových služieb:
 - kontinuálne monitorovacie mechanizmy,
 - zaistenie zodpovednosti prostredníctvom certifikácie a iných mechanizmov.
- Posilniť spoluprácu a vymedziť jasné usmernenia pre verejné obstarávanie založené na spolupráci medzi priemyslom a verejným sektorom.



Postupnosť krokov – proces overenia zhody



Základné dokumenty podľa metodiky

1. Metodické usmernenie pre zápis Cloudovej služby do Katalógu
2. 1A – Žiadosť o registráciu Cloudovej služby – U1/U2/U3
3. 1B – Formulár pre samohodnotenie CS – U1
4. 1C – Formulár pre hodnotenie CS – U2/U3
5. 1D – Katalóg vlastností CS
6. 1E – Popis hodnotiteľa CS
7. Mapovanie



Úrovne klasifikácie

U1: Open Data – dáta, ktoré sú verejne dostupné a použiteľné.

V prípade poskytovania infraštruktúry na vývoj IS sa dáta považujú za open data.

Pre U1 - samohodnotenie poskytovateľom cloudovej služby.

Min: C0I0A0 a C0I0A1

U2: Regulované dáta – dáta potrebné pre fungovanie IS VS a nespádajú do žiadnej z regulácií (Neštruktúrované informácie potrebné k vyriešeniu životnej situácie občana, štruktúrované informácie potrebné k vyriešeniu životnej situácie občana).

Pre U2 - posúdenie a ohodnotenie hodnotiteľom.

Min: C1I1A1 až C1I1A2



Úrovne klasifikácie

U3: Dôverné (klasifikované) dáta

– dáta, nakladenie s ktorými je upravené osobitnou právnou normou napr. dáta v zmysle zákona č. 215/2004 Z.z. o ochrane utajovaných skutočností, Konštrukčné údaje, Ekonomické údaje, Štatistické údaje, Oficiálne registre, Geo informácie, Backoffice údaje pracovníkov VS (emaily, osobné a mzdové údaje, ...) a pod.

Pre U3 posúdenie a ohodnotenie minimálne 2 hodnotiteľmi nezávisle.

Min: C2I1A1 až C3I3A3



Kritériá posudzovania pre cloudové služby - overenie zhody

Ekonomika a legislatíva

- Všeobecné informácie o poskytovateľovi cloudovej služby
- Zmluvné náležitosti a oblasť súladu s legislatívou SR a EU

Prevádzka

- Správa a prevádzka dátových centier
- Zákaznícka podpora
- Správa poskytovaných služieb

Bezpečnosť

- Riadenie bezpečnosti
- Technická bezpečnosť
- Technické opatrenia na ochranu osobných údajov

Špecifické

- IaaS,
- PaaS,
- SaaS



Určenie parametrov CIA pre SaaS

Bezpečnostná požiadavka	Žiadna (0)	Nízka (1)	Stredná (2)	Vysoká (3)
Dôvernosť (C)	Neexistuje požiadavka na dôvernosť informácie.	Neautorizovaná zverejnenie informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby.	Neautorizované zverejnenie informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby.	Neautorizované zverejnenie informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby.
Integrita (I)	Neexistuje požiadavka na integritu informácie.	Neautorizovaná modifikácia alebo zničenie informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby.	Neautorizované modifikácia alebo zničenie informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby.	Neautorizovaná modifikácia alebo zničenie informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby.
Dostupnosť (A)	Neexistuje požiadavka na dostupnosť informácie.	Nedostupnosť informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby.	Nedostupnosť informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby.	Nedostupnosť informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby.

Úroveň 1 Úroveň 2 Úroveň 3

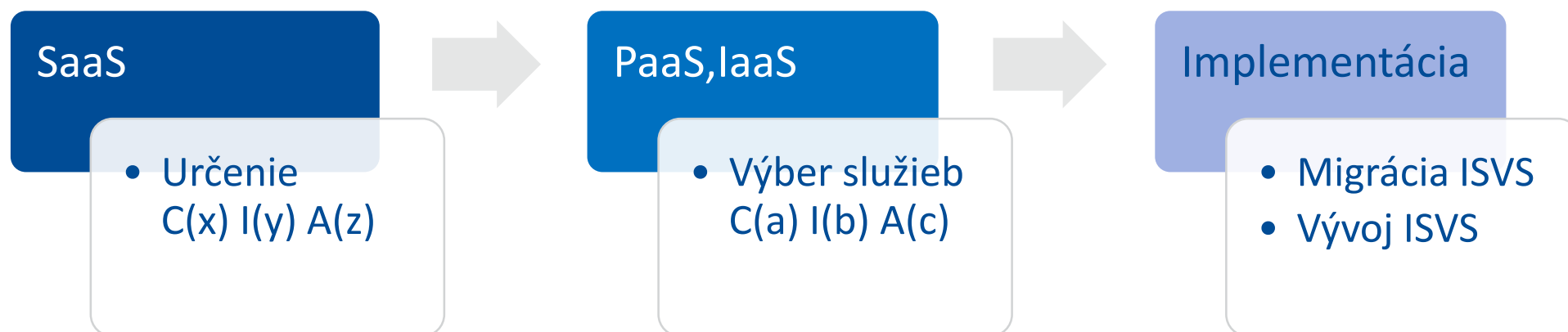


Určenie parametrov CIA pre IaaS a PaaS

Číslo opatrenia	Bezpečnostné opatrenie		Ano-Nie
C	Dôvernosť		
C1	Základná úroveň		
C1F	Fyzické opatrenia		
C1F01	Všetky súčasti systému sú uložené v uzamykateľných priestoroch	PR-C1-01 až PR-C1-04	
C1T	Technické opatrenia		
C1T01	Na perimetri siete je umiestnený sieťový firewall , ktorý filtruje prevádzku smerom do infraštruktúry aj z infraštruktúry na princípe least privilege for most specific	PR-C1-01, SE-C1-01 až SE-C1-04, SE-C2-01 a SE-C2-02	
C1T02	Na všetkých pracovných staniciach je implementovaná ochrana voči škodlivému kódu a prebieha pravidelná kontrola	SE-C1-01 až SE-C1-04, SE-C2-05	
C1T03	Na poštových serveroch je implementovaná ochrana pred spamom a antimalware ochrana	SE-C1-01 až SE-C1-04, SE-C2-05	
C1T04	Pravidelná aktualizácia pracovných staníc (operačných systémov, kancelárskych balíkov, prehliadačov súborov, webových prehliadačov)	SE-C1-01 až SE-C1-04	
C1T05	Všetky heslá musia byť ukladané v nereverzibilnom formáte	PR-C2-01, PR-C3-01, SE-C2-07, SE-C2-08, SS-C3-01	
C1T06	Používatelia pracujú pod používateľskými kontami. Každý používateľ má vlastné konto	PR-C2-01, PR-C3-01, SE-C1-10, SE-C2-07, SE-C2-08, SS-C3-01	
C1OR	Organizačné opatrenia		
C1OR01	Všetci zamestnanci sú poučení o pravidlách používania prostriedkov povinnej osoby z hľadiska informačnej bezpečnosti	SE-C1-10, SE-C1-13	
C1OR02	Je vypracovaná smernica o pravidlách používania IKT prostriedkov povinnej osoby	SE-C1-13, SE-C1-17	
C1OR03	Na pracovných staniciach aj serveroch je inštalovaný len legálny softvér z dôveryhodného zdroja.	SS-C4-01	
C1OR04	Je vypracovaná a pravidelne aktualizovaná sieťová topológia a dokumentácia	SE-C1-21, SS-C3-01, SS-C3-03, SS-C5-01	
C1OR05	Každé aktívum má svojho vlastníka	SE-C1-21, SS-C3-01, SS-C3-03	
C1OR06	Vypracovaná bezpečnostná politika a smernica o bezpečnom používaní.	SE-C1-21, SS-C3-01, SS-C3-03, SS-C5-01	



Vzťah SaaS a PaaS, IaaS – overenie zhody



$$a \geq x \quad b \geq y \quad c \geq z$$



Výhody uvedeného spôsobu – overenia zhody

- Jednotný prístup k overeniu kvality a vyspelosti služby
- Zjednodušenie výberu služieb hybridného cloudu
- Prínos aj pre komerčnú sféru



Katalóg služieb Vládneho cloudu

- **MIRRI – web**

<https://www.mirri.gov.sk/sekcie/informatizacia/egovernment/vladny-cloud/katalog-cloudovych-sluzieb/index.html>

- **Katalóg**

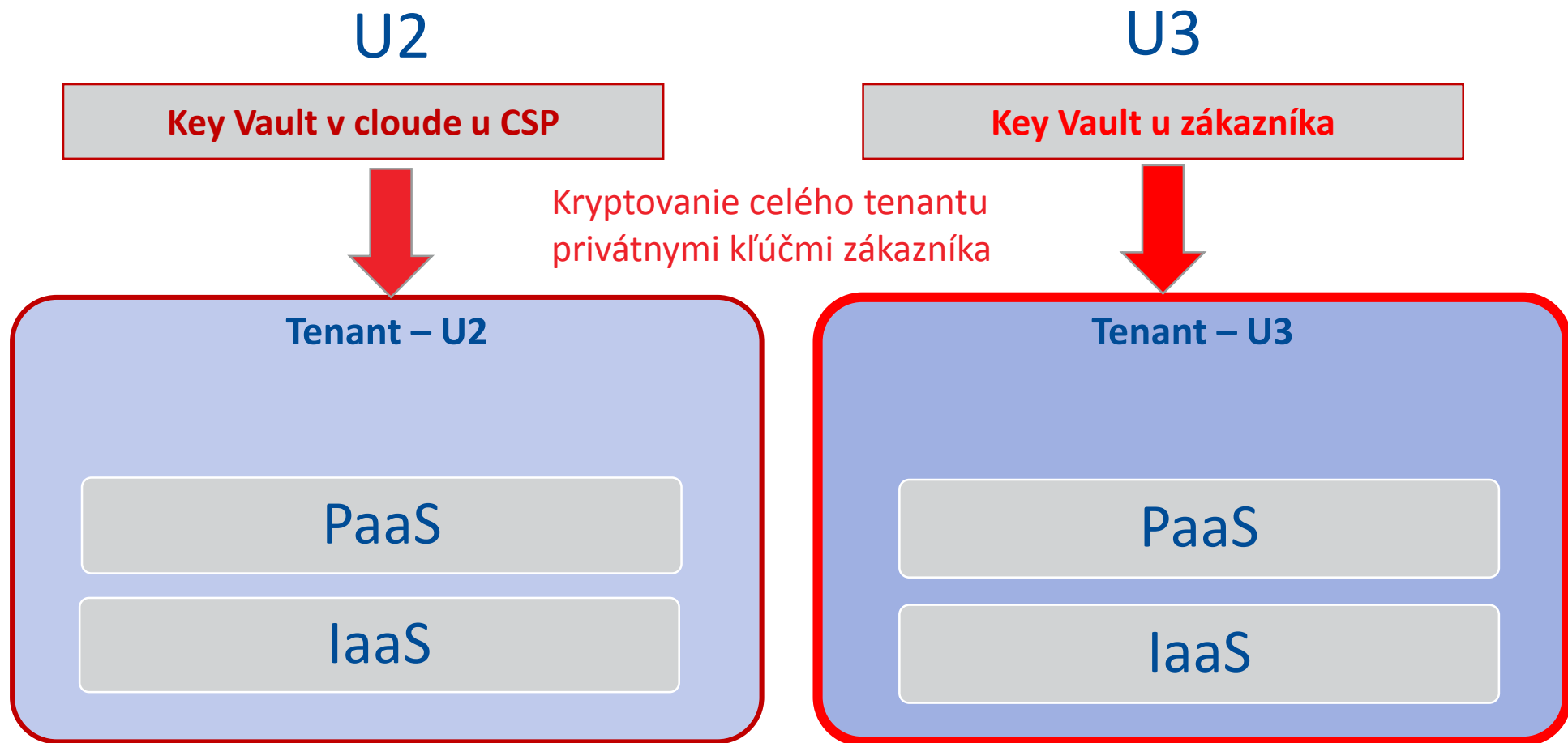
<https://katalog.statneit.sk>

- **Informácie k VC**

<https://cloud.statneit.sk>



Bezpečnosť údajov v cloude pre úrovne U2/U3 a CSP mimo SR



ĎAKUJEME!

www.mirri.gov.sk



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

