Slovakia

Viac istoty.
Viac hodnoty.

Bezpečná cesta v oblakoch: Evolúcia ISO/IEC 27017 a ISO/IEC 27018

Od IT doplnku k horizontálnemu ekosystému zdieľanej zodpovednosti.

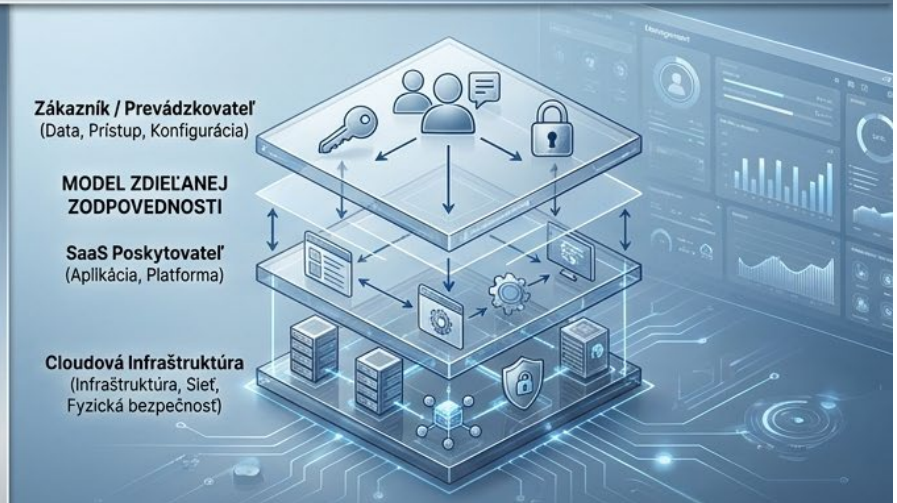
Kto reálne ovláda cloud?

- Bezpečnosť sa v cloudovom prostredí rozdrobuje na tisíce konfigurácií, ktoré ostávajú výlučne našou úlohou.

Považuje váš manažment nákup SaaS riešenia za prenos rizika na dodávateľa?

Ilúzia: Cloud ako Black Box

„Kúpili sme cloud, bezpečnosť kompletne rieši poskytovateľ.“

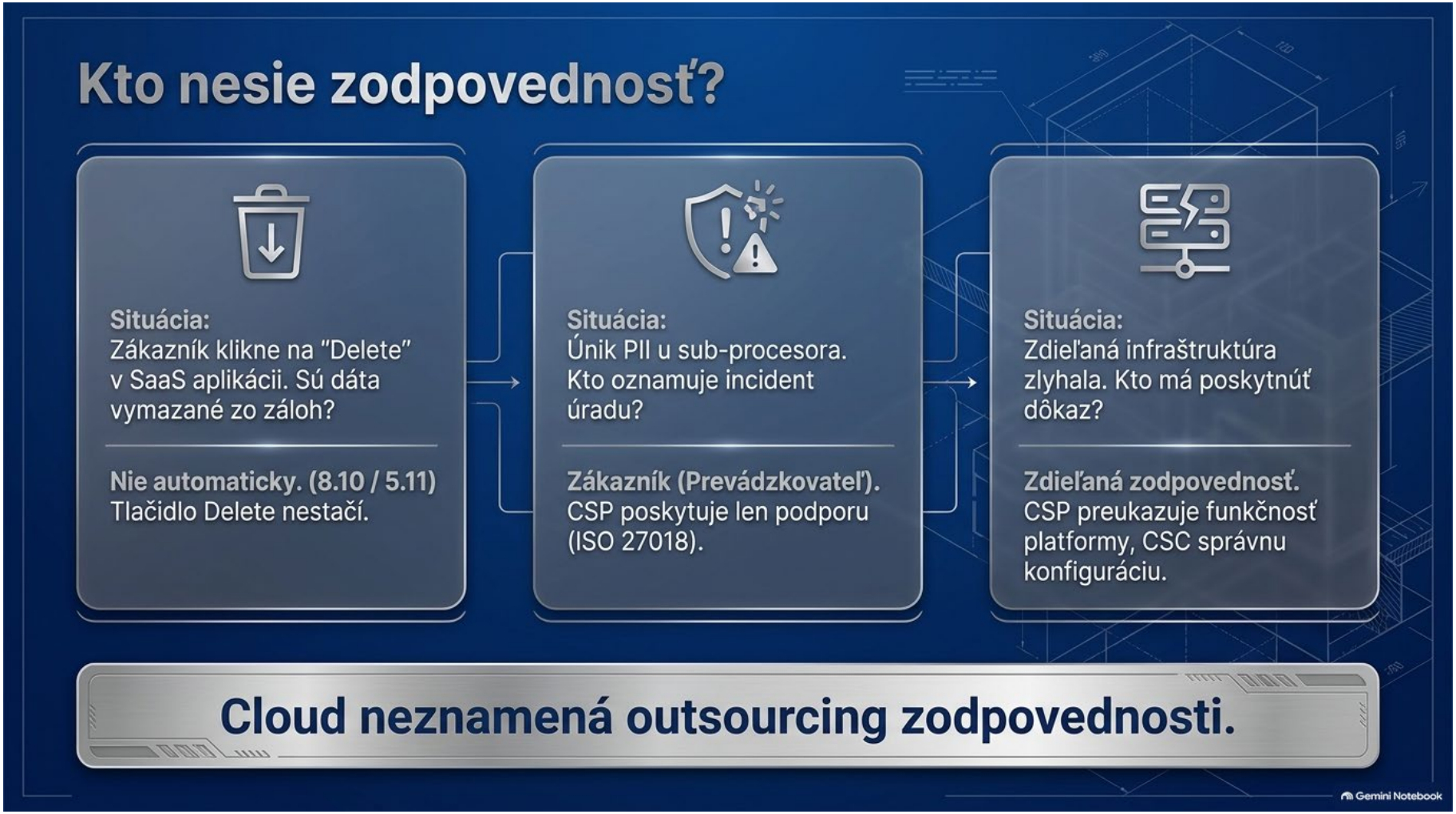


Manažérska realita cloudu: Plná zodpovednosť

- Cloudový model neznamená outsourcing zodpovednosti.
- Podľa GDPR, NIS2 a DORA nesie v prípade zlyhania cloudovej služby právnu, reputačnú a manažérsku zodpovednosť vaša organizácia (Zákazník/Prevádzkovateľ).
- Koniec éry neviditeľného subdodávateľa. Prichádza éra transparentného ekosystému zdieľanej zodpovednosti.

Gemini Notebook

Kto reálne ovláda cloud?



Štruktúra noriem

Slovakia

Nová mapa sveta: Architektonické zosúladenie s ISO/IEC 27002:2022

Prechod zo starého do nového sveta

Transformácia 14 pôvodných domén do 4 moderných tém:

- Organizačné kontroly
- Personálne kontroly
- Fyzické kontroly
- Technologické kontroly

Dopad na ISMS (Dominový efekt)

Toto nie je iba administratívne prečíslovanie! Zmena štruktúry vyžaduje radikálnu aktualizáciu:

- Vyhlásenia o aplikovateľnosti (SoA)
- Registra rizík
- Matice vlastníkov kontrol

Blok 3, Záchranné kolesá noriem (Prílohy)

- **Annex A** (27017 a 27018): Normatívne rozšírené sady kontrol pre cloud a PII. Privacy opatrenia tu nie sú skryté, tvoria samotné jadro noriem.
- **Annex B** (27018): Informatívne spätné mapovanie (z vydania 2019 na 2025) vytvorené výhradne pre zachovanie kontinuity dôkazov pri prechode.

ISO/IEC 27017

Slovakia

Anatómia ISO/IEC 27017: Od kódexu k horizontálnemu štandardu

43 kontrol:
Má špecifické cloudové usmernenia.

54 kontrol:
Preberá sa zo základnej normy v plnom rozsahu bez cloudových úľav! (viac ako 55 %, napr. segregácia fyzických sietí)

Type 1 (Asymetrické usmernenia)

Úplne odlišné povinnosti pre zákazníka (CSC) a poskytovateľa (CSP).

Cloud nie je symetrický vzťah (napr. CSC požiadavky overuje, zatiaľ čo CSP ich definuje a technicky zabezpečuje).

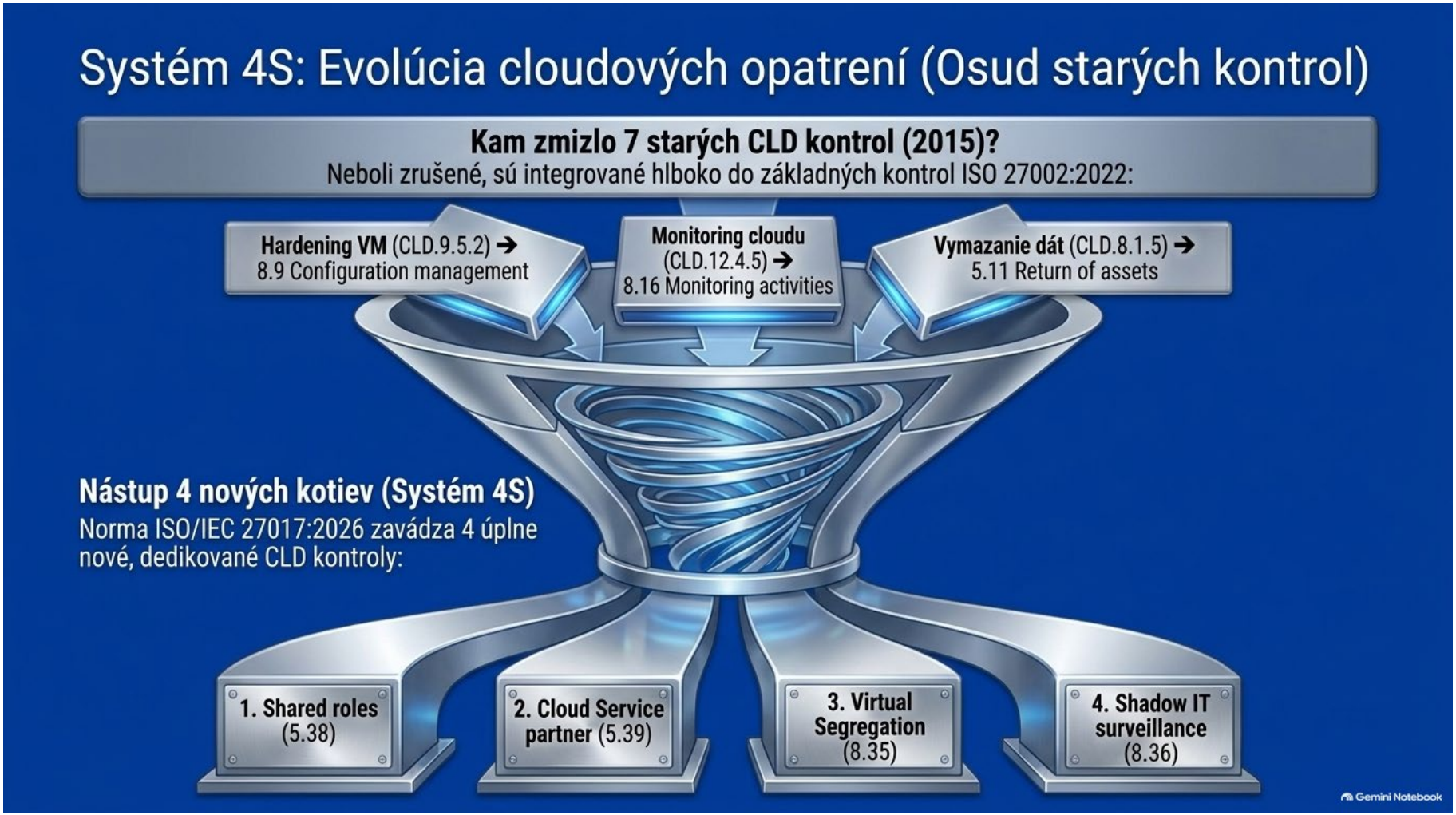
Type 2 (Symetrické usmernenia)

- Spoločné pravidlá a zodpovednosti pre obe strany.
- **Typický príklad:** Zmluvná spolupráca, reakcia na incidenty, digitálne dôkazy a cloudová forenzika.

Gemini Notebook

ISO/IEC 27017 Nové opatrenia

Slovakia



ISO/IEC 27017 Nové opatrenia

Slovakia

CLD Kotvy 1 & 2: Organizácia a Dodávateľský reťazec

5.38 CLD (Shared roles)

Pridelenie, zdokumentovanie a komunikácia zdieľaných rolí medzi Zákazníkom (CSC) a Poskytovateľom (CSP).

Koniec alibizmu. Musí byť explicitne určené: Kto patchuje? Kto zálohuje? Kto rieši bezpečnostný incident? Ak je zodpovednosť zdieľaná, musí byť aj exaktne zdokumentovaná.

5.39 CLD (Cloud service partner - CSN)

Revolúcia v dodávateľskom reťazci: Rozšírenie bezpečnostnej zodpovednosti aj na integrátorov, brokerov a subprocesorov (tzv. CSN).

Typický scenár: CSP poskytuje SaaS službu, ktorá beží na IaaS infraštruktúre iného CSP. Zodpovednosť nesmie vypadnúť medzi dvoma na seba nadväzujúcimi zmluvami!

Gemini Notebook

ISO/IEC 27017 Nové opatrenia

Slovakia

CLD Kotvy 3 & 4: Technológia a Manažérska kontrola

8.35 CLD (Virtual segregation)

Izolácia tenantov v zdieľanej cloudovej architektúre.

Nestačí deklarovať, treba **reálne chrániť**: Hypervízor, API rozhrania, metadáta a všetky vrstvy záloh.

Pravidlo: „Zdieľaná infraštruktúra áno, zdieľané dáta nikdy."

8.36 CLD (Shadow IT / Unauthorized use)

Záchytná sieť pre manažment: Detekcia a prevencia neschváleného používania cloudových služieb samotnými zamestnancami.

Ochrana pred nekontrolovaným únikom dát do voľne dostupných verejných AI nástrojov a súkromných cloudových úložísk. Čo nevidíme, to nevieme chrániť.

Gemini Notebook

ISO/IEC 27018

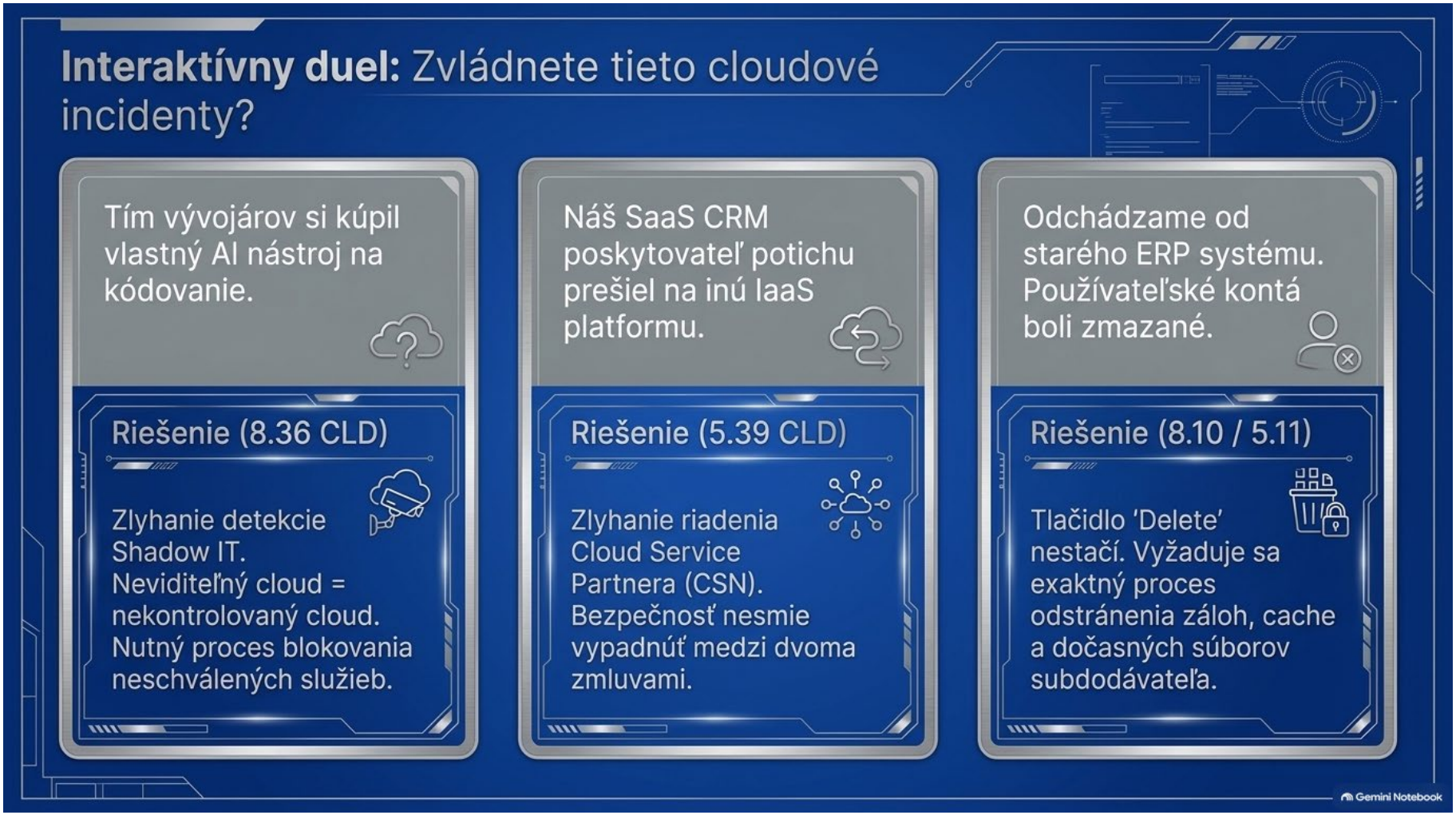
Slovakia

ISO/IEC 27018

Slovakia

?????????

Slovakia


Interaktívny duel: Zvládnete tieto cloudové incidenty?
Tím vývojárov si kúpil vlastný AI nástroj na kódovanie.
Riešenie (8.36 CLD)
Zlyhanie detekcie Shadow IT. Neviditeľný cloud = nekontrolovaný cloud. Nutný proces blokovania neschválených služieb.
Náš SaaS CRM poskytovateľ potichu prešiel na inú IaaS platformu.
Riešenie (5.39 CLD)
Zlyhanie riadenia Cloud Service Partnera (CSN). Bezpečnosť nesmie vypadnúť medzi dvoma zmluvami.
Odchádzame od starého ERP systému. Používateľské kontá boli zmazané.
Riešenie (8.10 / 5.11)
Tlačidlo 'Delete' nestačí. Vyžaduje sa exaktný proces odstránenia záloh, cache a dočasných súborov subdodávateľa.
Gemini Notebook

Skúška pozornosti pri implementácii

Slovakia

Konzultačné a manažérske chytáky: Zlyhania pri prechode na edície 2025/2026

Pasca 1: Ilúzia prechodu 1:1

⚠ **Riziko:** Mechanické prepísanie starých čísel kontrol v SoA bez overenia reálnych zmien v usmerneniach.

Náprava: Detailné preskúmanie nových integrovaných požiadaviek (napr. kontrola 8.9 absorbuje tému hardeningu VM).

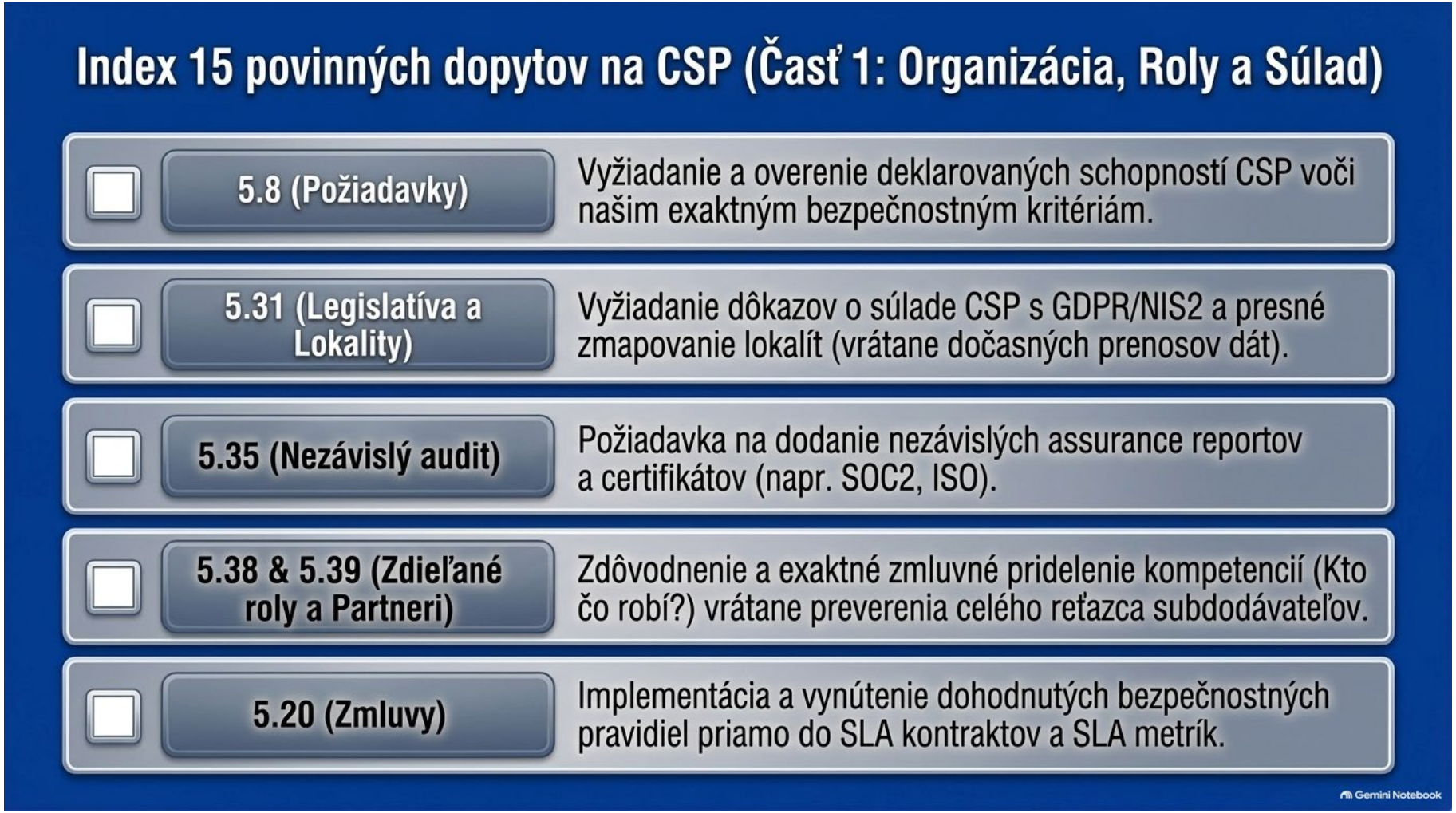
Pasca 2: Slepota voči reťazcu

⚠ **Riziko:** Auditovanie iba primárneho poskytovateľa (SaaS) a ignorovanie jeho subdodávateľskej infraštruktúry (peer CSP).

Náprava: Kontroly 5.21 a 5.39 vyžadujú zmluvný audit celého dodávateľského reťazca.

ISO/IEC 27017

Slovakia

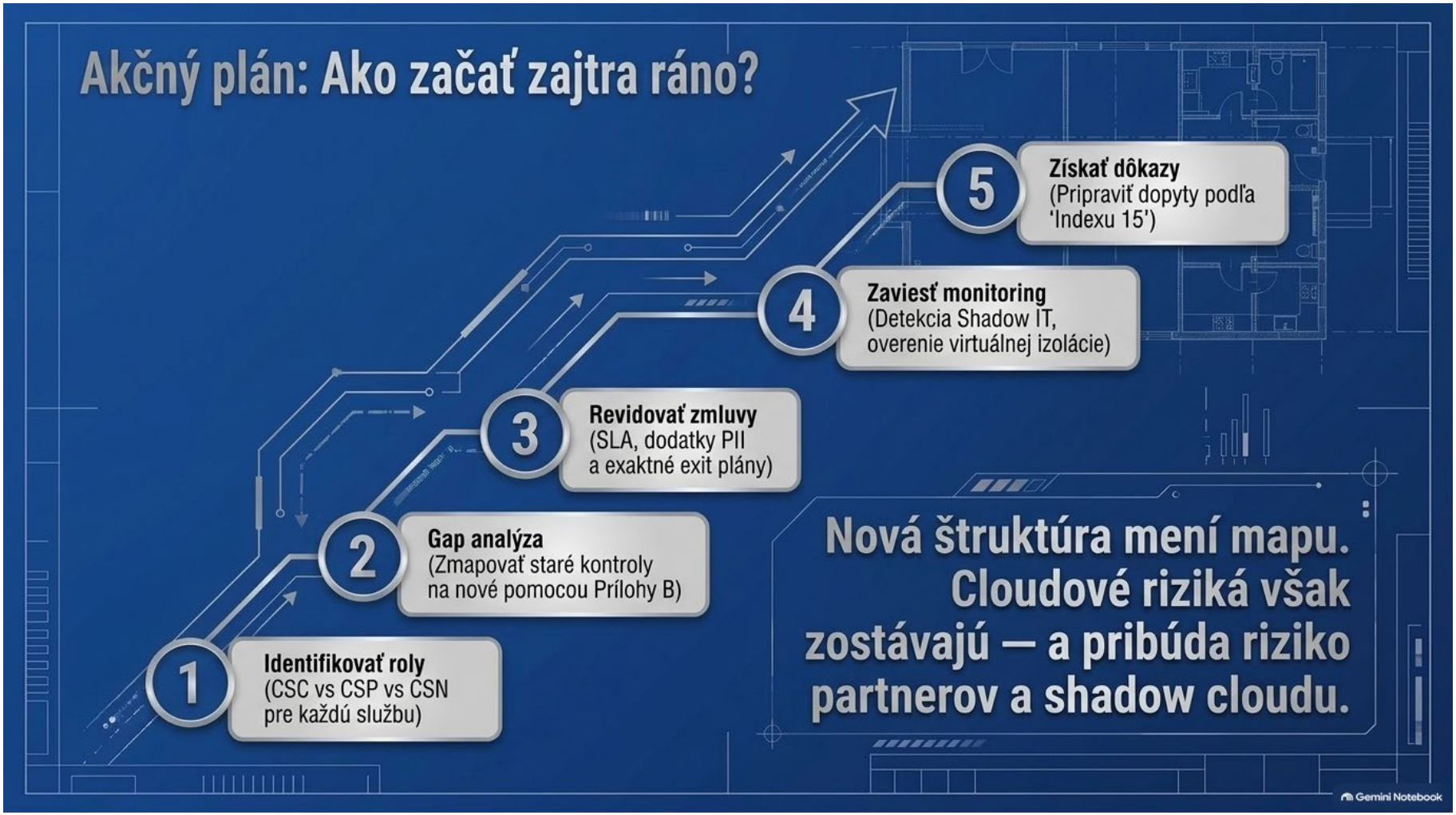


Index 15 povinných dopytov na CSP (Časť 2: Identity, Prevádzka a Monitorovanie)

☐	5.16 – 5.18 (IAM a Prístupy)	Verifikácia robustnosti nástrojov na správu identít a autentifikáciu poskytovaných zo strany CSP.
☐	8.15 & 5.33 (Logovanie a Záznamy)	Verifikácia rozsahu generovaných logov, ich bezpečné uchovávanie, retencia a imunita voči neoprávnenej modifikácii.
☐	8.16 & 8.17 (Monitoring a Čas)	Prístup zákazníka k monitorovacím nástrojom / API rozhraniam a synchronizácia hodín pre bezchybnú forenznú koreláciu logov.
☐	8.35 (Virtuálna izolácia)	Vyžiadanie nezávislých dôkazov (nielen marketingových tvrdení) o skutočnom oddelení sietí, dát a tenantov.
☐	8.8 & 8.25 (Zraniteľnosti a Vývoj)	Preskúmanie postupov CSP pri patchovaní, pravidelnom penetračnom testovaní a bezpečnom vývoji.

Index 15 povinných dopytov na CSP (Časť 1: Organizácia, Roly a Súlad)

☐	**5.8 (Požiadavky)**	Vyžiadanie a overenie deklarovaných schopností CSP voči našim exaktným bezpečnostným kritériám.
☐	**5.31 (Legislatíva a Lokality)**	Vyžiadanie dôkazov o súlade CSP s GDPR/NIS2 a presné zmapovanie lokalít (vrátane dočasných prenosov dát).
☐	**5.35 (Nezávislý audit)**	Požiadavka na dodanie nezávislých assurance reportov a certifikátov (napr. SOC2, ISO).
☐	**5.38 & 5.39 (Zdieľané roly a Partneri)**	Zdôvodnenie a exaktné zmluvné pridelenie kompetencií (Kto čo robí?) vrátane preverenia celého reťazca subdodávateľov.
☐	**5.20 (Zmluvy)**	Implementácia a vynútenie dohodnutých bezpečnostných pravidiel priamo do SLA kontraktov a SLA metrík.


Akčný plán: Ako začať zajtra ráno?
1
Identifikovať roly
(CSC vs CSP vs CSN
pre každú službu)
2
Gap analýza
(Zmapovať staré kontroly
na nové pomocou Prílohy B)
3
Revidovať zmluvy
(SLA, dodatky PII
a exaktné exit plány)
4
Zaviesť monitoring
(Detekcia Shadow IT,
overenie virtuálnej izolácie)
5
Získať dôkazy
(Pripraviť dopyty podľa
'Indexu 15')
Nová štruktúra mení mapu.
Cloudové riziká však
zostávajú — a pribúda riziko
partnerov a shadow cloudu.
Gemini Notebook

Ďakujem za pozornosť