



Desať pravidiel pre tvorbu bezpečnostnej dokumentácie pre právnik

Štefan Pilár



Desať pravidiel pre tvorbu BD

PREHL'AD

- **PREČO** bezpečnostná dokumentácia?
- **AKÁ** bezpečnostná dokumentácia?
- **AKO NA (to)...** bezpečnostná dokumentácia?
 - pravidlá, odporúčania...
- **Bezpečnostná stratégia KB**

Desať pravidiel pre tvorbu BD

PREČO bezpečnostná dokumentácia?

- výslovná požiadavka právnych predpisov
 - zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti („ZoKB“)
(„Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie...“)
 - zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe
 - zákon č. 45/2011 Z. z. o kritickej infraštruktúre

ale aj také

- Nariadenie EP a Rady (EÚ) 2016/679

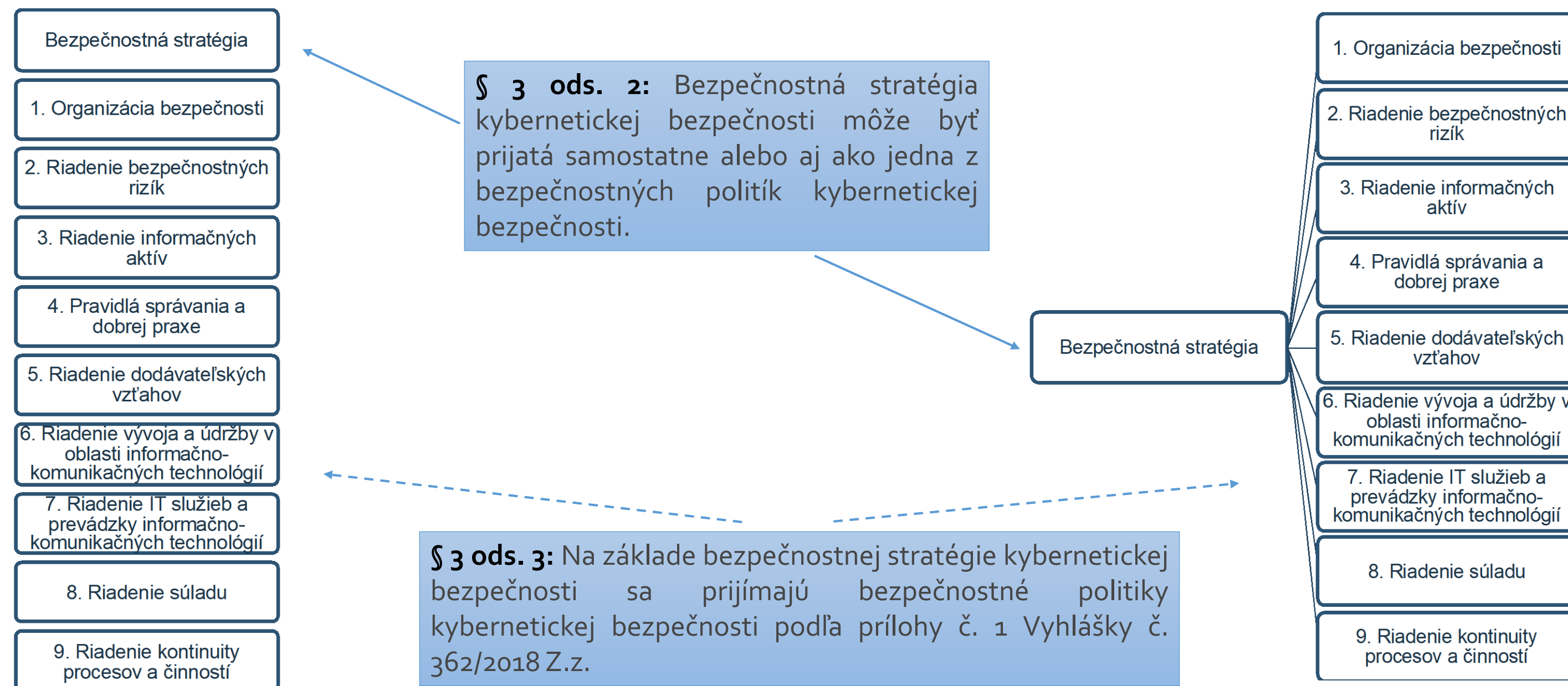
Desať pravidiel pre tvorbu BD

PREČO bezpečnostná dokumentácia?

- „inšpirácia“ (pre iné právne predpisy)
 - stanovenie záväzných pravidiel správania sa
 - prehľadnosť
 - preukaznosť
 - vynútiteľnosť
 - „uchopiteľnosť“
- konkurenčná výhoda

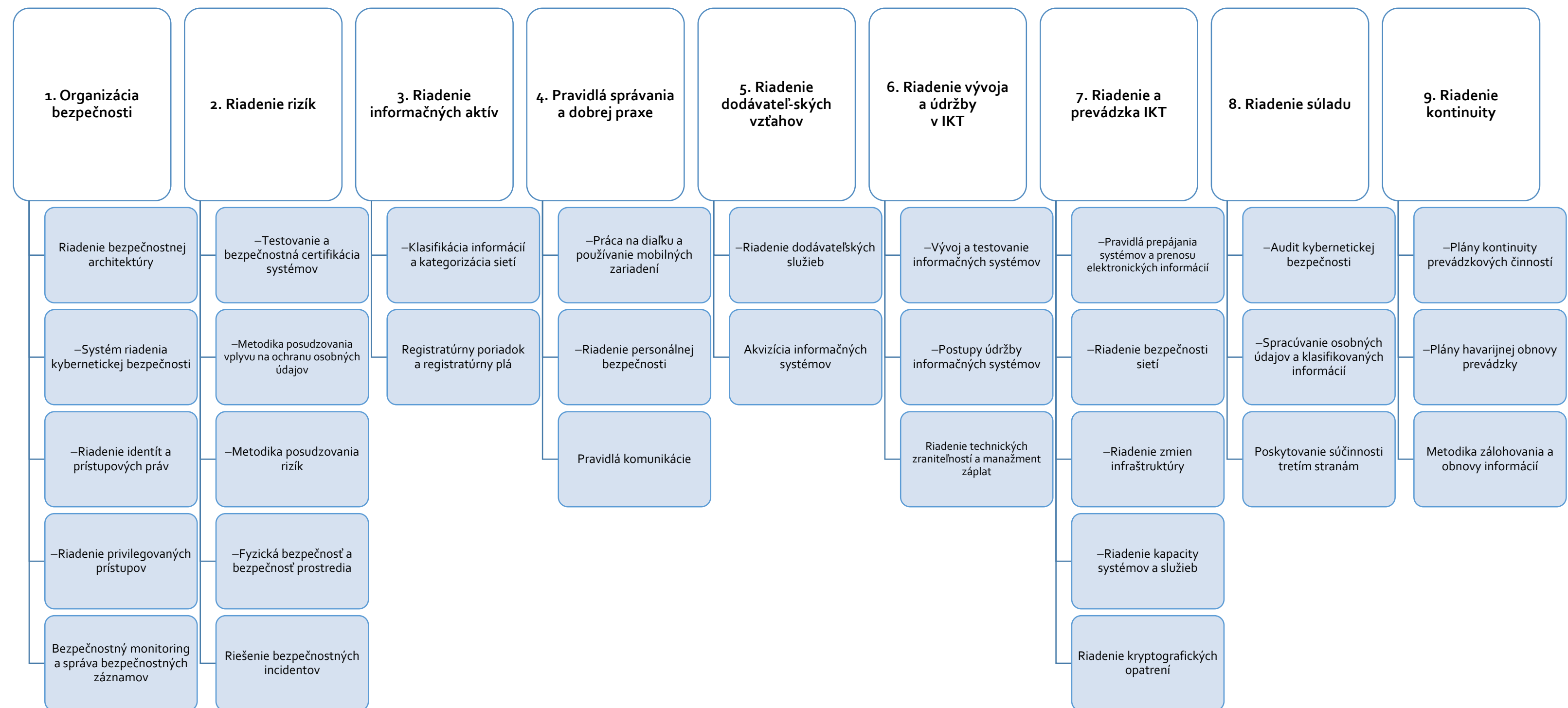
Desať pravidiel pre tvorbu BD

AKÁ bezpečnostná dokumentácia?



Desať pravidiel pre tvorbu BD

AKÁ bezpečnostná dokumentácia?



Desať pravidiel pre tvorbu BD

AKO NA (to).. bezpečnostná dokumentácia?

- **Bezpečnostná dokumentácia sa vypracúva vo vzťahu k poskytovaným službám** (typicky základná služba) a posúdenia s ňou
 - súvisiacej infraštruktúry výrobných a produkčných technológií
 - súvisiacej infraštruktúry informačno-komunikačných technológií
 - súvisiacej aplikačnej architektúry
 - súvisiacej bezpečnostnej architektúry a implementovaných bezpečnostných opatrení
 - súvisiacich organizačných usporiadaní, pracovných rolí, zodpovednosti a delenia právomocí
 - súvisiacich zaužívaných rámcov riadenia operačných rizík
 - súvisiacej organizačnej kultúry a spoločenskej zodpovednosti

Desať pravidiel pre tvorbu BD

AKO NA (to).. bezpečnostná dokumentácia?

- **Bezpečnostná dokumentácia obsahuje**
 - klasifikáciu informácií a kategorizáciu sietí a informačných systémov
 - zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení
 - vykonanú analýzu rizík kybernetickej bezpečnosti
 - záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti

Desať pravidiel pre tvorbu BD

AKO NA (to).. bezpečnostná dokumentácia?

- **Definovanie potrebnej (primeranej) štruktúry dokumentácie**
 - politiky (stratégia a 9 politík, high-level úroveň) – pre všetkých zamestnancov, písané
 - štandardy (konkrétne procesy, napríklad Riadenie zmien) – pre vybrané skupiny zamestnancov
 - pokyny (detailné pokyny, napr. kamerové systémy) – pre vybraných zamestnancov

Desať pravidiel pre tvorbu BD

AKO NA (to).. bezpečnostná dokumentácia?

- **Pravidelná revízia bezpečnostnej dokumentácie**
 - kto
 - kedy
 - čo sa zmenilo
 - verzia
 - ...

Desať pravidiel pre tvorbu BD

AKO NA (to).. bezpečnostná dokumentácia?

- (Každá jednotlivá) **politika má konkrétneho vlastníka**
 - ak nie je vlastník, revízia ani zmeny nefungujú

Desať pravidiel pre tvorbu BD

AKO NA (to).. bezpečnostná dokumentácia?

- **znalosti adresátov sú pravidelne overované a vyhodnocované** (eLearning, školenia, ...)
 - ak bežní zamestnanci nevedia, že existujú nejaké politiky, proces zjavne nefunguje
 - možnosť použitia zábavnejších foriem (gamifikácia, obrázky, videá)

Desať pravidiel pre tvorbu BD

AKO NA (to).. bezpečnostná dokumentácia?

- **dokumentácia je na dostupnom mieste** (shared drive, nástenka, ...)

Desať pravidiel pre tvorbu BD

AKO NA (to).. bezpečnostná dokumentácia?

- **posúdenie dokumentácie tretou stranou** (interná slepota)
 - či spĺňa požiadavky legislatívy
 - či je zrozumiteľná, jasná, odborná

Desať pravidiel pre tvorbu BD

Bezpečnostná stratégia KB

Bezpečnostná stratégia kybernetickej bezpečnosti obsahuje najmenej určenie

1. **bezpečnostných cieľov** z hľadiska kybernetickej bezpečnosti
2. **spôsobu vyhodnocovania bezpečnostných cieľov**, kritérií vyhodnocovania dosahovania bezpečnostných cieľov, spôsobov priebežného hodnotenia ich primeranosti a spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov
3. **úlohy štatutárneho orgánu** pri zabezpečovaní kybernetickej bezpečnosti a vyhlásenie o záväzku o podpore kybernetickej bezpečnosti
4. **všeobecných a špecifických zodpovedností a povinností** v oblasti kybernetickej bezpečnosti a **určenie** príslušných **bezpečnostných rolí** potrebných na riadenie kybernetickej bezpečnosti vrátane **určenia rozsahov činností, kompetencií a úloh; rozdelenie rolí na riadiacu** zložku, **výkonnú** zložku a **kontrolnú** zložku, pričom riadiaca zložka je priamo riadená prevádzkovateľom základnej služby a kontrolná zložka je nezlučiteľná so všetkými ostatnými zložkami
5. **základného rámca na riadenie aktív** podľa § 6, od ktorých závisí činnosť sietí a informačných systémov
6. **základného rámca riadenia rizík** podľa § 6 v súvislosti s aktívami, od ktorých závisí činnosť sietí a informačných systémov a **určenie bezpečnostných opatrení** podľa oblastí v zmysle § 20 ods. 3 ZoKB v závislosti od identifikovaných rizík
7. **rozsahu a periodicity overovania stavu kybernetickej bezpečnosti** prostredníctvom auditu kybernetickej bezpečnosti vrátane zhodnotenia súladu bezpečnostnej stratégie a bezpečnostných politík s požiadavkami ZoKB, iného všeobecne záväzného právneho predpisu, vnútorných predpisov a zmluvnými záväzkami
8. **postupu a zodpovedností pri revízii bezpečnostnej dokumentácie** schvaľovanej prevádzkovateľom základnej služby vrátane periodicity pravidelných revízií a jej aktualizácii po každej zmene majúcej na ňu vplyv, ako aj z dôvodov mimoriadnych revízií



Ďakujem za pozornosť!

Štefan Pilár

spilar@bch.sk

