



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

Riadenie kybernetických bezpečnostných rizík v kontexte vyhlášky o obsahu bezpečnostných opatrení

eFocus:

Riadenie rizík v dynamickom podnikovom prostredí, 8. 9 2020



POŽIADAVKA NA RIADENIE RIZÍK

- Typicky vo všeobecne záväzných právnych predpisoch - väčšinou bez konkretizácie rozsahu a metódy
- Absencia detailu vedie ku rôznym výkladom požiadaviek na riadenie rizika
- Prostredníctvom legislatívy je povinnosť presadzovaná približne posledných 5 rokov
- Metodika riadenia rizika bezpečnosti informácií je bližšie rozpracovaná v technických normách
- Na základe zákona č. 264/1999 Z.z. o technických požiadavkách na výrobky a o posudzovaní zhody slovenské technické normy prestali byť od 01.01.2001 záväzné



ODOLNOSŤ INFORMÁCIÍ VOČI HROZBÁM JE KOMBINÁCIOU VIACERÝCH DISCIPLÍN

Stav kybernetickej odolnosti poskytovanej služby

Riadenie rizík

Riadenie informačnej bezpečnosti

Riadenie
kontinuity
činností

Fyzická
bezpečnosť

Kybernetická
bezpečnosť

Bezpečnosť kritickej
infraštruktúry



Organizácia

Technologické
prostredie

Ochrana údajov

Klasifikácia informácií

Riadenie IT rizík

Manažment
zraniteľností

Havarijné plánovanie

Security Governance

IT architektúra

Riadenie aktív

Riadenie prístupov

Riadenie zmien a
konfigurácií

Riešenie incidentov

Service Level
Management

Vzťahy a komunikácia

Biznis architektúra

Ekosystém partnerov

Vzdelávanie a
povedomie



POŽIADAVKA NA RIADENIE RIZÍK V PRÁVNÝCH A TECHNICKÝCH PREDPISOCH

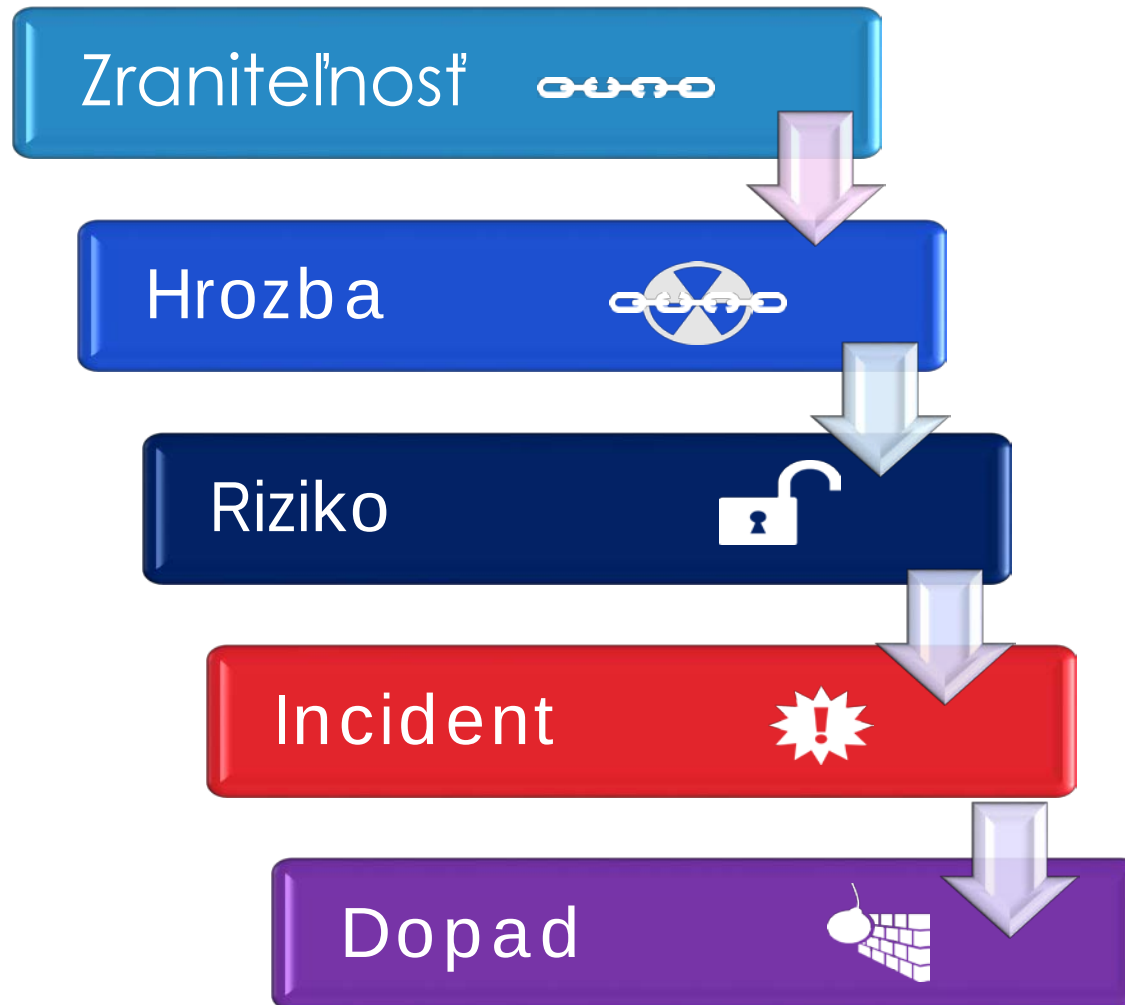
- Zákon č. 483/2001 Z. z. o bankách
- STN ISO 31000 Manažérstvo rizika – Návod
- STN ISO/IEC 27005 Informačné technológie - Bezpečnostné metódy - Riadenie rizík informačnej bezpečnosti
- Nariadenie EÚ 2016/679 všeobecné nariadenie o ochrane údajov (GDPR)
- Zákon č. 18/2018 Z.z. o ochrane osobných údajov
- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
 - Vyhláška NBÚ Č. 362/2018 Z.Z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení



Premostenie medzi generickými - všeobecne záväznými požiadavkami právnych predpisov a detailnými - nezáväznými odporúčaniami technických noriem



BEZPEČNOSTNÉ OPERÁCIE Z POHLĎADU ŽIVOTNÉHO CYKLU INCIDENTU



Hodnotenie zraniteľností

Analýza hrozieb

Ošetrovanie rizík

Aktívny monitoring prostredia

Vyhodnocovanie trendov

Analýza logov

Korelácia udalostí

Eskalácia incidentov

Riešenie incidentov

Riadenie kontinuity činností

Vyhodnotenie incidentov

Korekcia a odporúčania zmien

**Vyhláška NBÚ Č. 362/2018 Z.Z. ktorou sa ustanovuje
obsah bezpečnostných opatrení, obsah a štruktúra
bezpečnostnej dokumentácie a rozsah všeobecných
bezpečnostných opatrení**

Požiadavky v kontexte riadenia rizika



- 1) Bezpečnostná dokumentácia obsahuje:
 - b) klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
 - c) zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení; konkrétny obsah môže byť odvodený z princípov niektorého z rámcov riadenia bezpečnostnej architektúry,
 - d) vykonanú analýzu rizík kybernetickej bezpečnosti
- 2) Bezpečnostná dokumentácia sa vypracúva na základe posúdenia poskytovanej základnej služby a s ňou:
 - f) súvisiacich zaužívaných rámcov riadenia operačných rizík



- 1) Bezpečnostná stratégia kybernetickej bezpečnosti určuje ciele, ktoré je potrebné **na základe výsledkov analýzy rizík kybernetickej bezpečnosti** dosiahnuť, spolu s uvedením základných princípov na ich dosiahnutie a určením právomocí a zodpovedností za riadenie kybernetickej bezpečnosti, **riadenie rizík kybernetickej bezpečnosti** a aktualizáciu bezpečnostnej dokumentácie



§ 5 BEZPEČNOSTNÉ OPATRENIA PRE OBLASŤ ORGANIZÁCIE INFORMAČNEJ BEZPEČNOSTI

- Na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej zásada:
 - d) dodržiavania a vykonávania nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrovanie rizík



§ 6 BEZPEČNOSTNÉ OPATRENIA PRE OBLASŤ RIADENIA AKTÍV, HROZIEB A RIZÍK

- 1) Riadenie aktív, hrozieb a rizík je proces spojený s finančnými, zmluvnými a inventarizačnými funkciami na podporu riadenia životného cyklu informačných technológií a konfiguračných položiek. Účelom riadenia aktív, hrozieb a rizík je zabezpečiť ochranu aktív podľa ich hodnoty.



§ 6 BEZPEČNOSTNÉ OPATRENIA PRE OBLASŤ RIADENIA AKTÍV, HROZIEB A RIZÍK

- 4) Rovnaká ochrana sa neuplatňuje pre všetky druhy aktív. Na tento účel sa aktíva klasifikujú a kategorizujú postupom podľa § 4
- 6) Riadenie rizík pozostáva z:
 - a) identifikácie zraniteľností,
 - b) identifikácie hrozieb,
 - c) identifikácie a analýzy rizík s ohľadom na aktívum,
 - d) určenia vlastníka rizika,
 - e) **implementácie organizačných a technických bezpečnostných opatrení** v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením,
 - f) analýzy funkčného dopadu a
 - g) pravidelného preskúmavania identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.



§ 6 BEZPEČNOSTNÉ OPATRENIA PRE OBLASŤ RIADENIA AKTÍV, HROZIEB A RIZÍK

- 7) Identifikácia rizika sa vykonáva na základe **princípu najhoršieho scenára**, ktorý môže nastať aj pri nízkej pravdepodobnosti. Na určenie úrovne identifikovaného rizika sa vopred nastaví súbor pravidiel, ktoré umožnia na základe štandardných a opakovateľných postupov určiť merateľné a objektívne úrovne rizika pre najhoršie scenáre.
- 8) **Analýzou rizík sa určuje pravdepodobnosť vzniku škodlivej udalosti**, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a **identifikáciou dopadov** pri narušení dôvernosti, integrity alebo dostupnosti aktíva.
- 9) Identifikácia hrozieb je založená na **identifikácii aktív** a ich vlastníkov a **identifikácii zraniteľností** potenciálne pôsobiacich na tieto aktíva

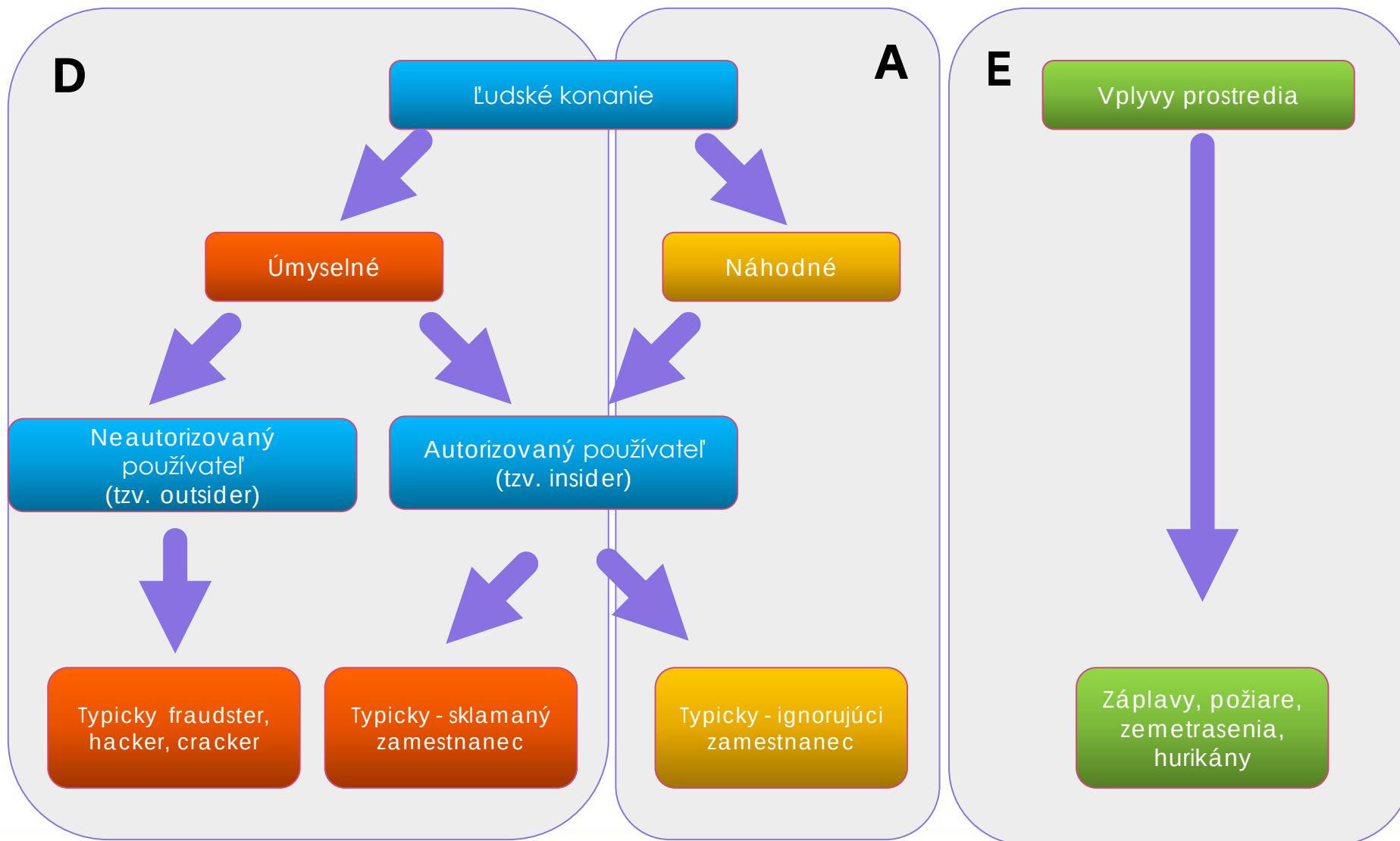


§ 6 BEZPEČNOSTNÉ OPATRENIA PRE OBLASŤ RIADENIA AKTÍV, HROZIEB A RIZÍK

- 10)** Pre potreby analýzy rizík sa **zoznam hrozieb združuje do jednotlivých skupín** tak, že je možné tento zoznam použiť univerzálne pre väčšinu aktív. Pre jednotlivé aktíva sú hodnotené len hrozby relevantné pre konkrétne aktívum. Hrozby sa rozdeľujú podľa ich pôvodu do kategórií najmenej ako
- a) úmyselné hrozby pre všetky úmyselné aktivity zamerané na aktíva,
 - b) náhodné hrozby pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť aktíva,
 - c) hrozby spôsobené vplyvom prostredia pre všetky udalosti, ktoré vznikajú nezávisle od ľudskej činnosti
- Podľa ISO/IEC 27005 je označenie pôvodu hrozieb nasledovné:
- D („**deliberate**“ - úmyselné) – používané pre všetky úmyselné aktivity zamerané na informačné aktíva,
 - A („**accidental**“ - náhodné) - pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť informačné aktíva,
 - E („**environmental**“ - spôsobené vplyvom prostredia) - všetky udalosti, ktoré vznikli nezávisle na ľudskej činnosti



Kategórie hrozieb





§ 6 BEZPEČNOSTNÉ OPATRENIA PRE OBLASŤ RIADENIA DODÁVATEĽSKÝCH SLUŽIEB, AKVIZÍCIE, VÝVOJA A ÚDRŽBY INFORMAČNÝCH SYSTÉMOV

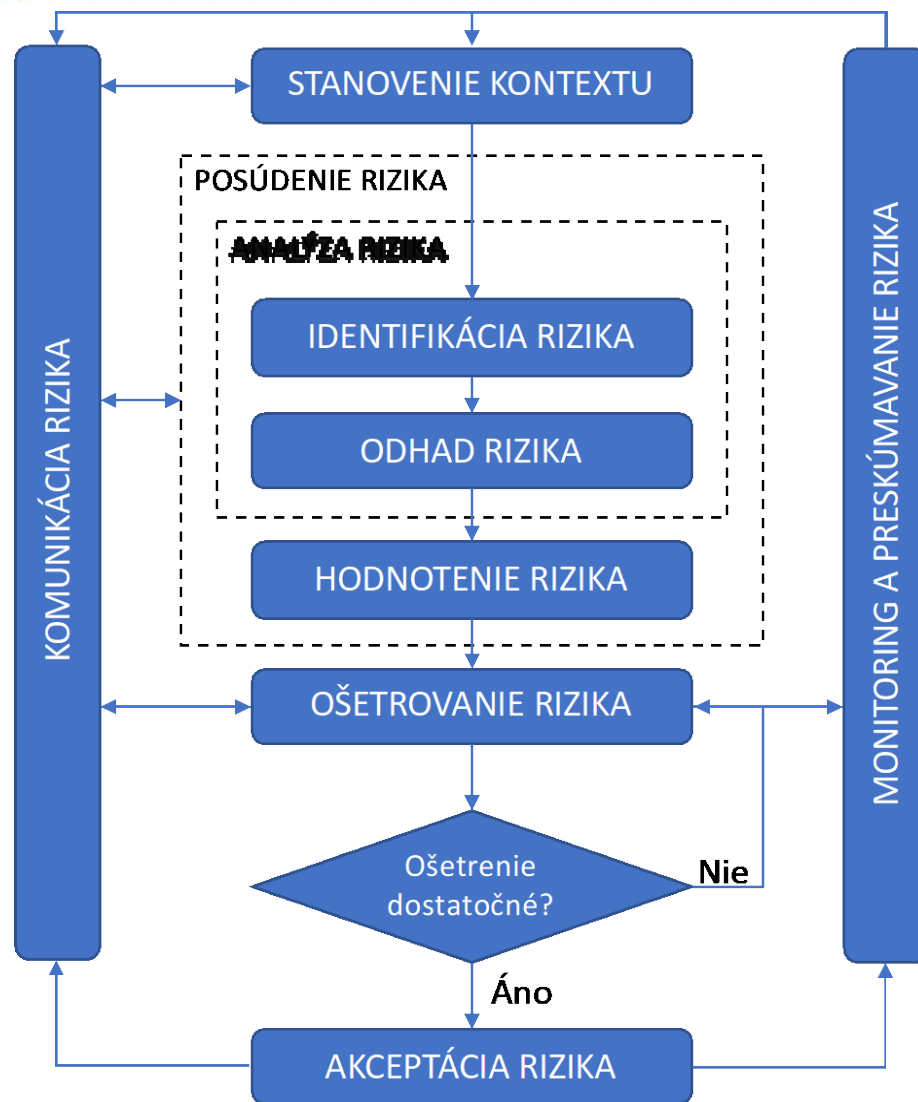
- 1) Na riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov sa pri uzatvorení zmluvy s treťou stranou podľa § 19 ods. 2 zákona **analyzujú riziká dodávateľských služieb, akvizície, vývoja a údržby informačných systémov** spôsobom podľa § 6.



- 2) Riadenie kontinuity procesov pozostáva najmenej z
- a) vypracovania stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu na základe vykonania **analýzy dopadov** kybernetického bezpečnostného incidentu na základnú službu,
 - d) určenia **cieľovej doby obnovy** jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb,
 - e) určenia **cieľového bodu obnovy** jednotlivých procesov, siete a informačných systémov základnej služby a aplikácií, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby



Generický proces riadenia rizík informačnej bezpečnosti (podľa ISO/IEC 27005)



- Vo Vyhláške NBÚ Č. 362/2018 Z.Z. sú obsiahnuté všetky fázy a podprocesy riadenia rizika podľa ISO/IEC 27005
- Podľa § 6 ods. 6 písm e) Riadenie rizík pozostáva z:
 - **implementácie organizačných a technických bezpečnostných opatrení** v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením
- Pokiaľ má vaša organizácia implementované riadenie rizika podľa ISO/IEC 27005, je pravdepodobne v súlade s Vyhláškou NBÚ Č. 362/2018 Z.Z.



ROZSAH BEZPEČNOSTNÝCH OPATRENÍ PODĽA KATEGÓRIE SYSTÉMOV

Bezpečnostné opatrenie podľa § 20 ods. 3 zákona	Kategória I	Kategória II	Kategória III
a) organizácia informačnej bezpečnosti	Odporúčané	Odporúčané	Povinné
b) riadenie aktív, hrozieb a rizík	Odporúčané	Povinné	Povinné
c) personálna bezpečnosť	Odporúčané	Povinné	Povinné
d) riadenie dodávateľských služieb, akvizície, vývoja a údržby IS	Odporúčané	Povinné	Povinné
e) riadenie technických zraniteľností systémov a zariadení	Odporúčané	Povinné	Povinné
f) riadenie bezpečnosti sietí a informačných systémov	Odporúčané	Povinné	Povinné
g) riadenie prevádzky	Odporúčané	Povinné	Povinné
h) riadenie prístupov	Odporúčané	Povinné	Povinné
i) kryptografické opatrenia	Odporúčané	Odporúčané	Povinné
j) riešenie kybernetických bezpečnostných incidentov	Povinné	Povinné	Povinné
k) monitorovanie, testovanie bezpečnosti a bezpečnostné audity	Odporúčané	Povinné	Povinné
l) fyzickej bezpečnosti a bezpečnosti prostredia	Odporúčané	Odporúčané	Povinné
m) riadenia kontinuity procesov	Odporúčané	Povinné	Povinné



Ďakujem za pozornosť

© Copyright Cyber Security Competence and Certification Centre (Hereinafter referred to as "KCCKB"). All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents KCCKB's current intent, is subject to change or withdrawal, and represent only goals and objectives. KCCKB, the KCCKB logo, and other KCCKB products and services are trademarks of the Cyber Security Competence and Certification Centre, in the Slovak republic, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: cybersecurity involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. KCCKB products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. KCCKB does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



www.cybercompetence.sk



www.linkedin.com/company/cybercompetence



[@CybercenterSk](https://twitter.com/CybercenterSk)