Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Organizácia a riadenie informačnej a kybernetickej bezpečnosti, personálna bezpečnosť, ľudské zdroje a vzdelávanie

Pavol Dovičovič

2. apríl 2025

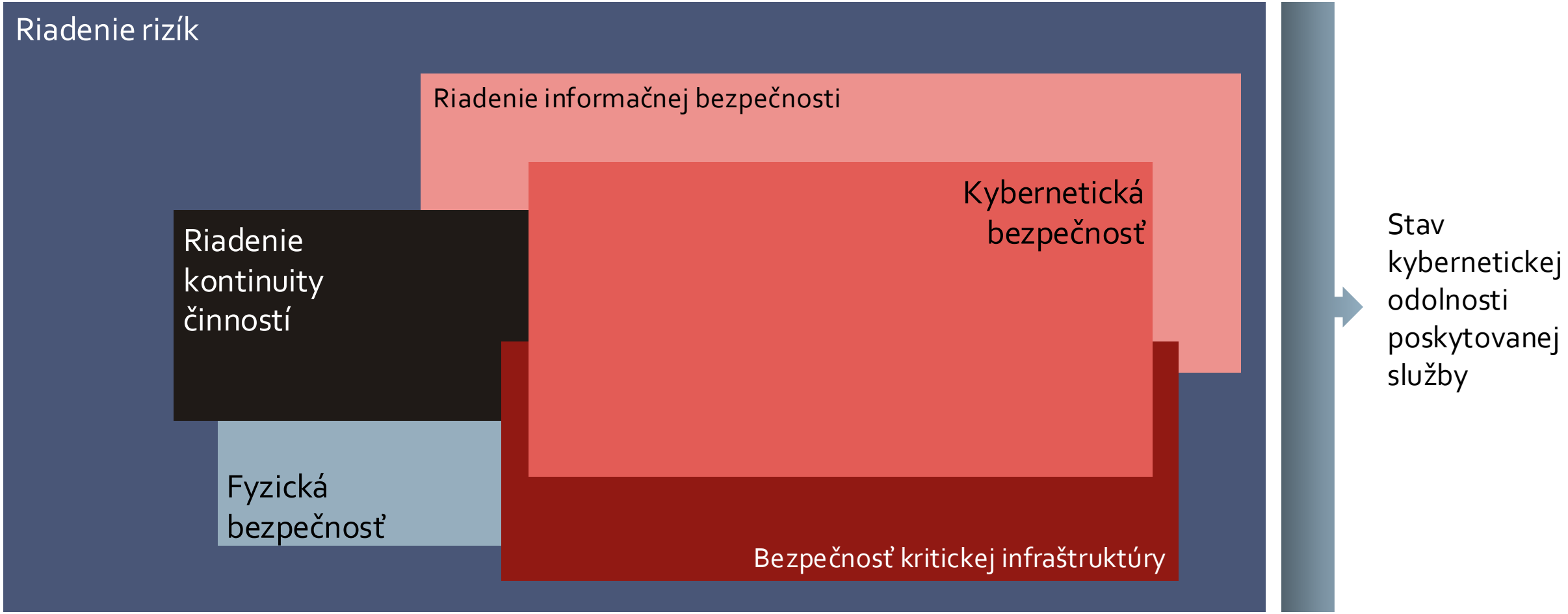
KĽÚČOVÉ ROLY A VZŤAHY V RIADENÍ A VÝKONE BEZPEČNOSTI

„Bezpečnosť nie je len otázkou technológií, ale predovšetkým ľudí – efektívna organizácia, systematické riadenie, dôsledná personálna bezpečnosť a neustále vzdelávanie sú kľúčom k ochrane informácií aj kybernetického priestoru.“

ChatGPT

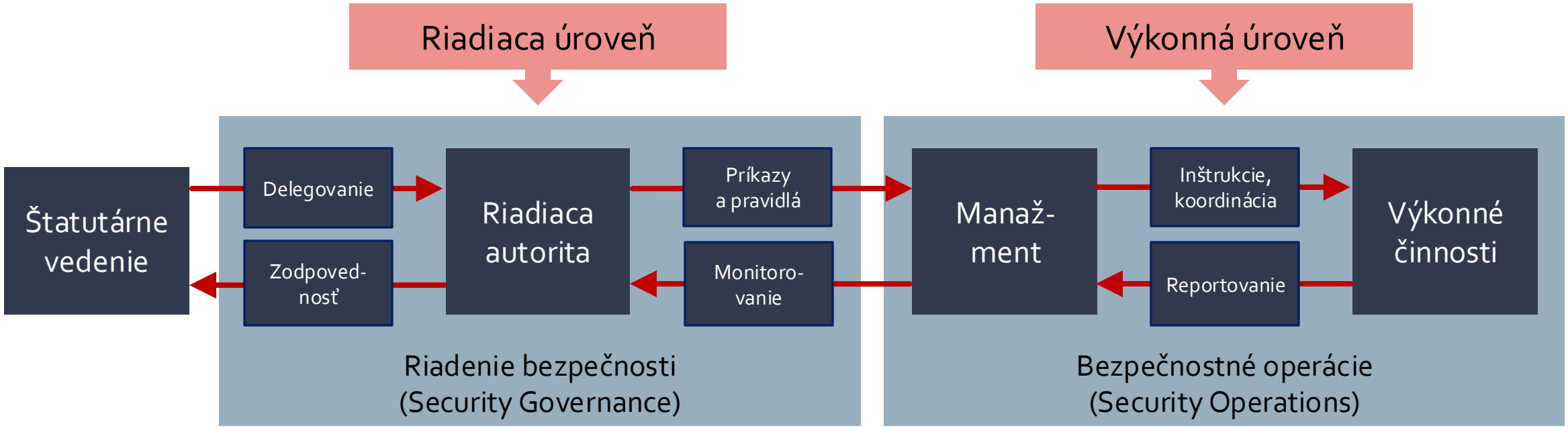
Organizácia a riadenie informačnej a kybernetickej bezpečnosti

BEZPEČNOSTNÉ DOMÉNY



Spolufinancovaný Európskou úniou

KĽÚČOVÉ ROLY A VZŤAHY V RIADENÍ A VÝKONE BEZPEČNOSTI



Zdroj: ISACA, isaca.org/cobit5

VŠEOBECNÝ RÁMEC BEZPEČNOSTNÝCH POLITÍK

Úroveň riadenia		Dokument	Obsah
GOV	1. Strategická	Politiky	Určujú celkové smerovanie organizácie. Stanovujú všeobecné požiadavky, zákazy a zásady správania sa v príslušnej oblasti.
MGMT	2. Taktická	Štandardy	Interpretujú príslušnú politiku v konkrétnych situáciách. Stanovujú povinné aktivity, explicitné pravidlá, ktoré sú navrhnuté na podporu a dodržiavanie politík. Štandardy prenášajú politiku do praxe.
	3. Operatívna	Procedúry	Uvádzajú podrobnosti o tom, ako dodržiavať politiky a štandardy. Procedúry sú súhrnom predpísaných krokov na vykonanie politík prostredníctvom konkrétnych akcií.
		Návody	Dodatočné dokumenty na podporu politík, štandardov a procedúr - všeobecné usmernenie k otázkam typu: "čo robiť za konkrétnych okolností".
		Baseline	Platformovo závislé pravidlá akceptované naprieč odvetvím, poskytujúce najefektívnejšie prístupy ku špecifickej implementácii politík, návrhy riešení, architektonické koncepty, konfiguračné pravidlá, atď.

Zdroj: ISACA, isaca.org/cobit5

Spolufinancovaný Európskou úniou

RÁMEC BEZPEČNOSTNÝCH POLITÍK PODĽA VYHLÁŠKY 362/2018 Z.z.

1. Organizácia bezpečnosti	2. Riadenie rizík	3. Riadenie informačných aktív	4. Pravidlá správania a dobrej praxe	5. Riadenie dodávateľ-ských vzťahov	6. Riadenie vývoja a údržby v IKT	7. Riadenie a prevádzka IKT	8. Riadenie súladu	9. Riadenie kontinuity
Riadenie bezpečnostnej architektúry	Testovanie a bezpečnostná certifikácia systémov	Klasifikácia informácií a kategorizácia sietí	Práca na diaľku a používanie mobilných zariadení	Riadenie dodávateľských služieb	Vývoj a testovanie informačných systémov	Pravidlá prepájania systémov a prenosu elektronických informácií	Audit kybernetickej bezpečnosti	Plány kontinuity prevádzkových činností
Systém riadenia kybernetickej bezpečnosti	Metodika posudzovania vplyvu na ochranu osobných údajov	Registratúrny poriadok a registratúrny plá	Riadenie personálnej bezpečnosti	Akvizícia informačných systémov	Postupy údržby informačných systémov	Riadenie bezpečnosti sietí	Spracúvanie osobných údajov a klasifikovaných informácií	Plány havarijnej obnovy prevádzky
Riadenie identít a prístupových práv	Metodika posudzovania rizík		Pravidlá komunikácie		Riadenie technických zraniteľností a manažment záplat	Riadenie zmien infraštruktúry	Poskytovanie súčinnosti tretím stranám	Metodika zálohovania a obnovy informácií
Riadenie privilegovaných prístupov	Fyzická bezpečnosť a bezpečnosť prostredia					Riadenie kapacity systémov a služieb		
Bezpečnostný monitoring a správa bezpečnostných záznamov	Riešenie bezpečnostných incidentov					Riadenie kryptografických opatrení		

Personálna bezpečnosť

POŽIADAVKY NA PERSONÁLNU BEZPEČNOSŤ

Personálna bezpečnosť pozostáva najmenej:

a) Z postupov pri **zaradení osoby** do niektorých z bezpečnostných rolí, **presunu práv**, povinností a zodpovedností vo vzťahu ku kybernetickej bezpečnosti na inú osobu,

b) Zo zavedenia plánu **rozvoja bezpečnostného povedomia** a vzdelávania spočívajúceho v oboznámení používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov s bezpečnostnými politikami a v pravidelnom zvyšovaní ich bezpečnostného povedomia počas trvania pracovnoprávneho vzťahu, alebo iného obdobného pracovného alebo zmluvného vzťahu,

c) Z **kontroly dodržiavania bezpečnostných politík** zo strany zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov,

POŽIADAVKY NA PERSONÁLNU BEZPEČNOSŤ

d) Z **hodnotenia účinnosti plánu rozvoja** bezpečnostného povedomia zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov,

e) Z určenia pravidiel a postupov na **riešenie prípadov porušenia bezpečnostnej politiky** zo strany používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov,

f) Z postupov pri **skončení pracovnoprávneho vzťahu** alebo iného obdobného pracovného alebo zmluvného vzťahu s používateľom, administrátorom, s osobou zastávajúcou niektorú z bezpečnostných rolí umožňujúcich **presun práv, povinností a zodpovedností** na inú novú osobu,

g) Z postupov pri porušení bezpečnostných politík spočívajúcich v **oprávnení obmedziť alebo odňať prístupové oprávnenia** a privilégiá,

h) Z vykonania poučenia o manipulácii s informáciami pre osoby, ktoré vykonávajú činnosť alebo sa oboznamujú s informáciami podľa osobitného predpisu (zákona č. 198/1994 z. Z. o vojenskom spravodajstve).

ZÁSADY ORGANIZÁCIE KYBERNETICKEJ BEZPEČNOSTI

Zásady uplatňované na účely organizácie kybernetickej bezpečnosti:

a) Určenie manažéra kybernetickej bezpečnosti, ktorý:

   1. Má možnosť **predkladať návrhy** a oznamovať informácie v oblasti kybernetickej bezpečnosti **priamo štatutárnemu orgánu** prevádzkovateľa základnej služby,
   2. Zabezpečuje aplikáciu bezpečnostných opatrení v systéme riadenia kybernetickej bezpečnosti,
   3. Je **nezávislý od riadenia prevádzky a vývoja** služieb informačných technológií a
   4. **Spĺňa znalostné štandardy** na funkciu manažéra kybernetickej bezpečnosti podľa osobitného predpisu,

b) **Najnižšie privilégiá** (least privilege) - každému používateľovi sú obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh,

c) **Oddeľovanie zodpovedností** (segregation of duties) - žiaden používateľ nemá oprávnenie pristupovať, upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity,

d) **Vykonávanie nezávislého hodnotenia,** merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrenie rizík,

e) **Jasné vymedzenie právomoci,** povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností.

Spolufinancovaný Európskou úniou

Ľudské zdroje a vzdelávanie

ROLY V KYBERNETICKEJ BEZPEČNOSTI PODĽA ECSF A SLOVENSKEJ PRÁVNEJ ÚPRAVY

ENISA European Cybersecurity Skills Framework (ECSF)

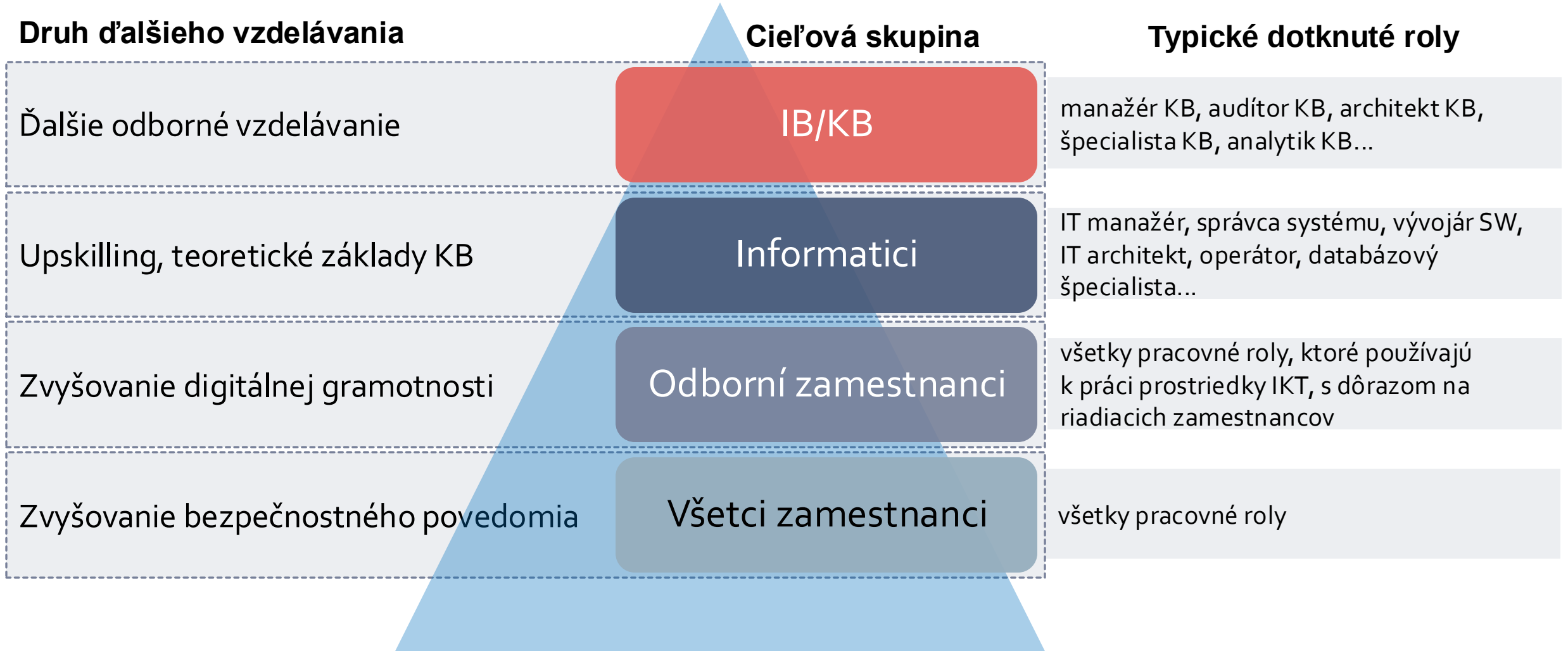


Vyhláška NBÚ č. 492/2022 o znalostných štandardoch v KB



Source: ENISA European Cybersecurity Skills Framework (ECSF)

RÁMEC A CIEĽOVÉ SKUPINY VZDELÁVANIA V KB



Zdroj: NIST Special Publication 800-16: Information Technology Security Training Requirements

Spolufinancovaný Európskou úniou

TYPICKÁ DISTRIBÚCIA KVALIFIKÁCIÍ

ÚROVEŇ ZNALOSTÍ	Laici	Odborní zamestnanci	Manažéri	IT manažéri	Informatici	Špecialisti KB	Manažéri KB	Audítori KB
Znalosť vybraných základných pojmov a ich významu	✓	✓	✓	✓	✓	✓	✓	✓
Použitie mechanizmov a procesov v bezpečnostných riešeniach		✓	✓	✓	✓	✓	✓	✓
Legislatíva, súlad a etika ochrany údajov				✓			✓	✓
Implementácia a uplatňovanie bezpečnostných mechanizmov a riešení				✓	✓	✓	✓	✓
Návrh bezpečnostných mechanizmov a riešení					✓	✓	✓	✓
Návrh stratégií a analýza bezpečnostných mechanizmov a riešení							✓	✓
Posudzovanie zhody a efektivity procesov, bezpečnostných mechanizmov a riešení								✓
PRÍSLUŠNÝ KURZ	Prehľad KB		Základy KB			Manažér KB		Audítor KB

CYBERGAME 2025

CYBERGAME je kyberbezpečnostná súťaž štýlu Capture The Flag (CTF)

CyberGame je cvičenie, kde si hráči môžu vyskúšať riešenie incidentov, analýzu škodlivého kódu či informačných zdrojov a tak zistiť, čo všetko obnáša práca bezpečnostných špecialistov.

- Organizovaná Národným bezpečnostným úradom – https://cybergame.sk/sk
- Rôzne obtiažnosti, otvorená pre širokú verejnosť

- 15 scenárov, 79 úloh
- V roku 2024 bola 2312 registrovaných hráčov, 874 aktívnych hráčov z toho až 606 študentov

ZÁVER

- Ďakujeme za Váš čas.
- Nasledujúci webinár na tému „Riadenie aktív, identifikácia hrozieb a riadenie rizík.“ - 24.4.2025



NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE



Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.