



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti



NCC-SK
SLOVAKIA CYBERSECURITY
COORDINATION CENTRE
 

ROLY, ZNALOSTNÉ ŠTANDARDY A CERTIFIKÁCIA V KYBERNETICKEJ BEZPEČNOSTI

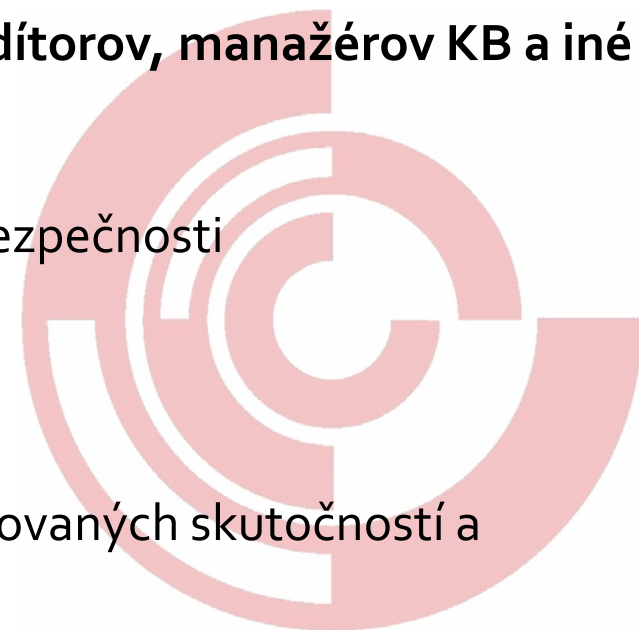
Miroslav Havelka

eFOCUS, Bratislava, 20.09.2023



KOMPETENČNÉ CENTRUM KB (KCCCKB)

- Pôsobnosť **Národného koordinačného centra KB** v zmysle Nariadenia EÚ č. 2021/887
- **Výkon činností orgánu posudzovania zhody, t.j. certifikácia audítorov, manažérov KB a iné**
- **Vzdelávanie dospelých** v kybernetickej bezpečnosti
- Organizácia kampaní na zvyšovanie povedomia v kybernetickej bezpečnosti
- Publikačná činnosť
- **Audit kybernetickej bezpečnosti** podľa zákona č. 69/2018 Z.z.
- Poskytovanie konzultácií v oblasti kybernetickej bezpečnosti, utajovaných skutočností a dôveryhodných služieb
- **Znalecká a expertízna činnosť** podľa zákona č. 382/2004 Z. z.. o znalcoch
- Činnosti autorizovanej osoby podľa Zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností
- Zónové merania a merania nežiadúceho elektromagnetického vyžarovania





NIEKOĽKO ZÁKLADNÝCH POJMOV

- **Vedomosti** (resp. znalosti) - poznatky nadobudnuté v priebehu vzdelávania, učenia sa alebo skúsenosťou; sústavy predstáv a pojmov
- **Zručnosti** - schopnosti jednotlivca uplatňovať vedomosti v praxi a využívať ich na plnenie úloh a riešenie problémov
- **Kompetencie** - preukázané schopnosti jednotlivca použiť vedomosti, zručnosti a osobné, sociálne a/alebo metodologické schopnosti v pracovných alebo študijných situáciách a v odbornom a osobnom rozvoji
- **Certifikácia** - Atestácia nezávislým akreditovaným orgánom posudzovania zhody, týkajúca sa charakteristík objektu posudzovania





PRÁVNÁ ÚPRAVA ZNALOSTNÝCH ŠTANDARDOV V KB NA SLOVENSKU A EÚ

Európska legislatíva

Directive (EU) No. 2016/1148
concerning measures for a high common level
of security of network and information
systems across the Union

NIS

Directive (EU) No. 2022/2555
on measures for a high common level of
cybersecurity across the Union, amending
Regulation (EU) No 910/2014 and Directive
(EU) 2018/1972, and repealing Directive (EU)
2016/1148 (NIS 2 Directive)

NIS2

Národná právna úprava

Zákon o kybernetickej bezpečnosti
č. 69/2018 Z.z.

Vyhláška NBÚ č. 492/2022
o znalostných štandardoch
v kybernetickej bezpečnosti



ROLY VO VZŤAHU KU ZNALOSTNÝM ŠTANDARDOM

- Zodpovednosť osoby v oblasti kybernetickej bezpečnosti v organizácii musí byť jednoznačne zadefinovaná prostredníctvom rolí, v ktorých osoba vystupuje vo vzťahu k informačnému systému
- S rolami je spojená množina povinností a oprávnení pri inicializácii, návrhu, vývoji, používaní a prevádzke informačného systému
- Charakteristika rolí patriacich do danej kategórie podrobnejšie špecifikuje:
 - **klúčové činnosti,**
 - **požadované vedomosti, zručnosti a kompetencie**
 - **a ďalšie podmienky, ktoré musí spĺňať osoba zaradená do danej roly tak,**
aby bola schopná plniť povinnosti v oblasti kybernetickej bezpečnosti vyplývajúce z roly, v ktorej je zaradená
- **Znalostné štandardy musia vychádzať zo špecifikácie jednotlivých rolí**





EURÓPSKY VS. SLOVENSKÝ RÁMEC ROLÍ V KB

ENISA European Cybersecurity Skills Framework (ECSF)



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





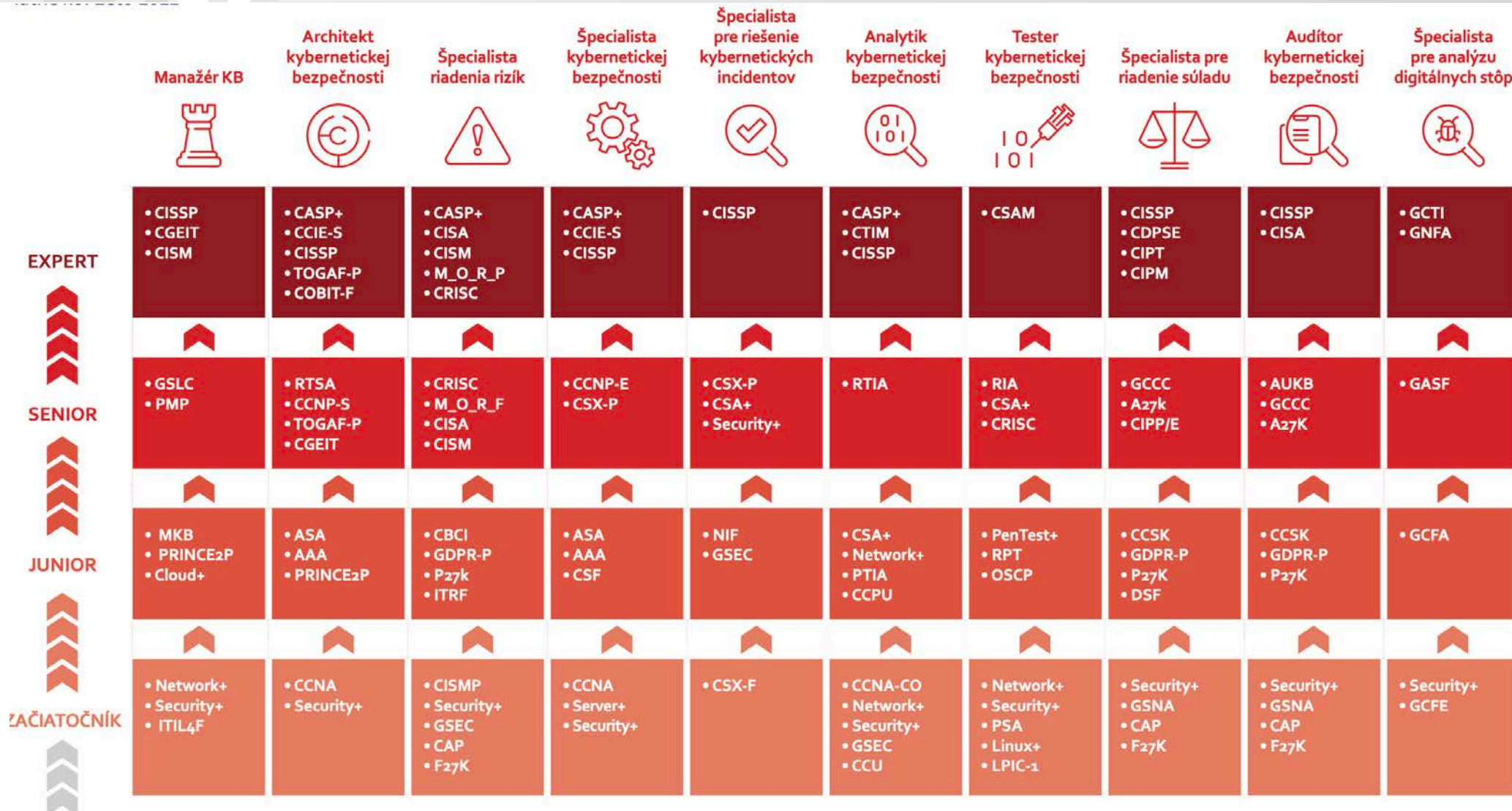
MAPOVANIE ROLÍ V KB: ECSF .vs VYHLÁŠKA NBÚ Č. 492/2022

VYHLÁŠKA NBÚ č. 492/2022		ECSF RÁMEC ROLÍ
Špecialista kybernetickej bezpečnosti		CS implementer
Manažér KB		Chief information security officer (CISO)
Audítor KB	Iba tieto roly sú vyžadované ZoKB (2023)	CS auditor
Tester KB		Penetration tester
Architekt KB		CS architect
Špecialista riadenia rizík KB		CS risk manager
Špecialista pre analýzu digitálnych stôp		Digital forensic investigator
Špecialista pre riadenie súladu		Cyber legal, policy & compliance officer
Špecialista pre riešenie kybernetických incidentov		Cyber incident responder
Výskumník KB		Cyber threat intelligence specialist / Cybersecurity researcher
Lektor		CS Educator

Source: ENISA European Cybersecurity Skills Framework (ECSF)



MAPOVANIE KOMERČNÝCH CERTIFIKÁTOV NA ROLY V KYBERNETICKEJ BEZPEČNOSTI





OBSAH VYHLÁŠKY NBÚ č.492 – PRÍLOHA č.5 – MANAŽÉR KB

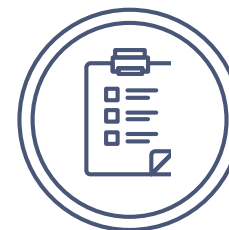
■ Špecifikuje potrebné:

- Vedomosti
- Zručnosti
- Stupeň vzdelania
- Odborná prax
- Špecifické kľúčové kompetencie



■ V oblastiach:

- Riadenie bezpečnosti
- Riadenie hrozieb a rizík
- Aplikácia bezpečnostných opatrení
- Výkon operatívnych bezpečnostných činností
- Riadenie súladu





POŽIADAVKY NA ROLU MANAŽÉRA KB V ZMYSLE VYHLÁŠKY NBÚ č.492 – VEDOMOSTI (PRÍKLAD)

Rola:	Manažér kybernetickej bezpečnosti
Vedomosti:	Riadenie bezpečnosti • Procesy, systémy a zásady riadenia kybernetickej bezpečnosti, vrátane zásad riadenia fyzickej a objektovej bezpečnosti BL5 • Organizácia kybernetickej bezpečnosti BL6 • Terminológia a skratky v oblasti kybernetickej bezpečnosti BL6 • Princípy riadenia IT služieb, správy systémov a správy počítačových sietí BL5



ZÁVER: AKO NÁM MÔŽU POMÔČŤ ZNALOSTNÉ ŠTANDARDY V SPRÁVNOM NASTAVENÍ SYSTÉMU KYBERNETICKEJ BEZPEČNOSTI?

Znalostné štandardy v kybernetickej bezpečnosti sú nutné a potrebné najmä na:

- akreditáciu existujúcich ale aj nových študijných programov, odborov a predmetov
- definície štandardov zamestnaní v Národnej sústave povolání (v zmysle zákona č. 5/2004 Z. z. o službách zamestnanosti)
- opis nárokov trhu práce na jednotlivé pracovné miesta
- určenie požiadaviek na odborné zručnosti a praktické skúsenosti potrebné na vykonávanie pracovných činností na trhu práce
- určenie zodpovedností osôb v oblasti kybernetickej bezpečnosti v organizáciách
- zvýšenie spôsobilostí osôb pri práci v kybernetickom priestore
- skrátenie doby detekcie hrozieb a reakčnej doby pri riešení incidentov



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.



www.cybercompetence.sk



www.linkedin.com/company/cybercompetence



@CybercenterSk



TAXONÓMIA VZDELÁVACÍCH CIEĽOV

Úroveň	Vzdelávací cieľ	Popis vzdelávacieho cieľa
BL ₁	ZAPAMÄTANIE	Schopnosť zapamätať si potrebné informácie. Skúšobné otázky spojené s touto úrovňou testujú pamäť uchádzača a zahŕňajú úlohy ako: definícia, výber zo zoznamu, rozpoznanie, popis a pomenovanie.
BL ₂	POCHOPENIE	Schopnosť porozumieť alebo pochopiť význam toho, čo bolo komunikované a využiť získanú informáciu bez toho, aby ju uchádzač spájal s inými informáciami, interpretáciami alebo materiálmi. Otázky na preskúmanie vedomostí na tejto úrovni zahŕňajú scenáre, ktoré uvádzajú príklady, ilustrácie, odvodenia, sumarizáciu a interpretáciu. Úroveň zahŕňa vedomosti získané na predchádzajúcej úrovni.
BL ₃	APLIKÁCIA	Uchádzač by mal byť schopný používať myšlienky, princípy a teórie v nových, konkrétnych situáciách. Otázky na preskúmanie na tejto úrovni zahŕňajú vedomosti a pochopenie a môžu zahŕňať úlohy typu: výber vhodných postupov, uplatňovanie zásad, použitie prístupu alebo identifikácia možností. Úroveň zahŕňa vedomosti získané na predchádzajúcich úrovniach.
BL ₄	ANALÝZA	Uchádzač je schopný rozdeliť komunikáciu na základné časti, aby bol jasne uchopený význam informácie. V tejto úrovni sa skúma podstata jednotlivých entít, s cieľom lepšie porozumieť komplexným celkom. Úroveň zahŕňa vedomosti získané na predchádzajúcich úrovniach.
BL ₅	SYNTÉZA	Na tejto úrovni je uchádzač schopný opätovne spojiť rôzne časti alebo prvky konceptu do jednotného systému alebo celku. Toto spojenie a zmysel pre malé časti je rozhodujúcim faktorom v učení. Úroveň vzdelávania BL₅ je pre uchádzača typicky najintenzívnejšia. Otázky na preskúmanie vedomostí na tejto úrovni zahŕňajú scenáre ako: tvorba, návrh, písanie, kombinovanie, skladanie, organizovanie, revízia a plánovanie. Aby sa mohlo prístupíť k tejto úrovni vzdelávacích cieľov, musí zahŕňať prvé štyri úrovne – zapamätanie, pochopenie, aplikáciu a analýzu.
BL ₆	POSÚDENIE	V tejto fáze je uchádzač schopný dospieť k prehľadu a posúdiť hodnotu a relatívny prínos myšlienok alebo postupov pomocou vhodných kritérií. Uchádzač musí byť schopný porovnávať, posudzovať, hodnotiť, odôvodňovať, kritizovať a kontrastovať teórie, postupy, metódy a koncepty. Úroveň zahŕňa vedomosti získané na všetkých predchádzajúcich úrovniach.



POŽIADAVKY NA ROLU MANAŽÉRA KB V ZMYSLE VYHLÁŠKY NBÚ č.492 – VEDOMOSTI (PRÍKLAD)

Zručnosti:

Riadenie bezpečnosti

- 1) strategické riadenie kybernetickej bezpečnosti organizácie
- 2) vypracovanie a prezentácia bezpečnostných stratégií a konceptov
- 3) implementácia a riadenie procesov kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov
- 4) zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie



POŽIADAVKY NA ROLU MANAŽÉRA KB V ZMYSLE VYHLÁŠKY NBÚ č.492 – VZDELANIE A PRAX (PRÍKLAD)

Stupeň vzdelania:	Úplné stredné všeobecné alebo úplné stredné odborné	Vysokoškolské I. stupňa	Vysokoškolské II. a III. stupňa
Odborná prax:	• najmenej 7 rokov praxe v oblasti informačných technológií • z toho najmenej 5 rokov praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok	• najmenej 5 rokov praxe v oblasti informačných technológií • z toho najmenej 3 roky praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok	• najmenej 3 roky praxe v oblasti informačných technológií • z toho najmenej 1 rok praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok



POŽIADAVKY NA ROLU MANAŽÉRA KB V ZMYSLE VYHLÁŠKY NBÚ č.492 – ŠPECIFICKÉ KOMPETENCIE

Špecifické kľúčové kompetencie

- a) schopnosť prijímať rozhodnutia
- b) schopnosť myslieť a konať v súvislostiach
- c) schopnosť riešiť konflikty
- d) schopnosť poskytovať spätnú väzbu
- e) schopnosť delegovať úlohy
- f) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí
- g) schopnosť viesť pracovný tím
- h) schopnosť organizovania a plánovania práce
- i) analytické myslenie
- j) strategické a koncepčné myslenie
- k) tvorivosť (kreativita)
- l) prezentačná zručnosť

Požiadavky označené * sú odvetvovo závislé. Pre príslušnú rolu sú posudzované v kontexte kompetencií, potrebných na vykonávanie určitej pracovnej činnosti v konkrétnom odvetví.

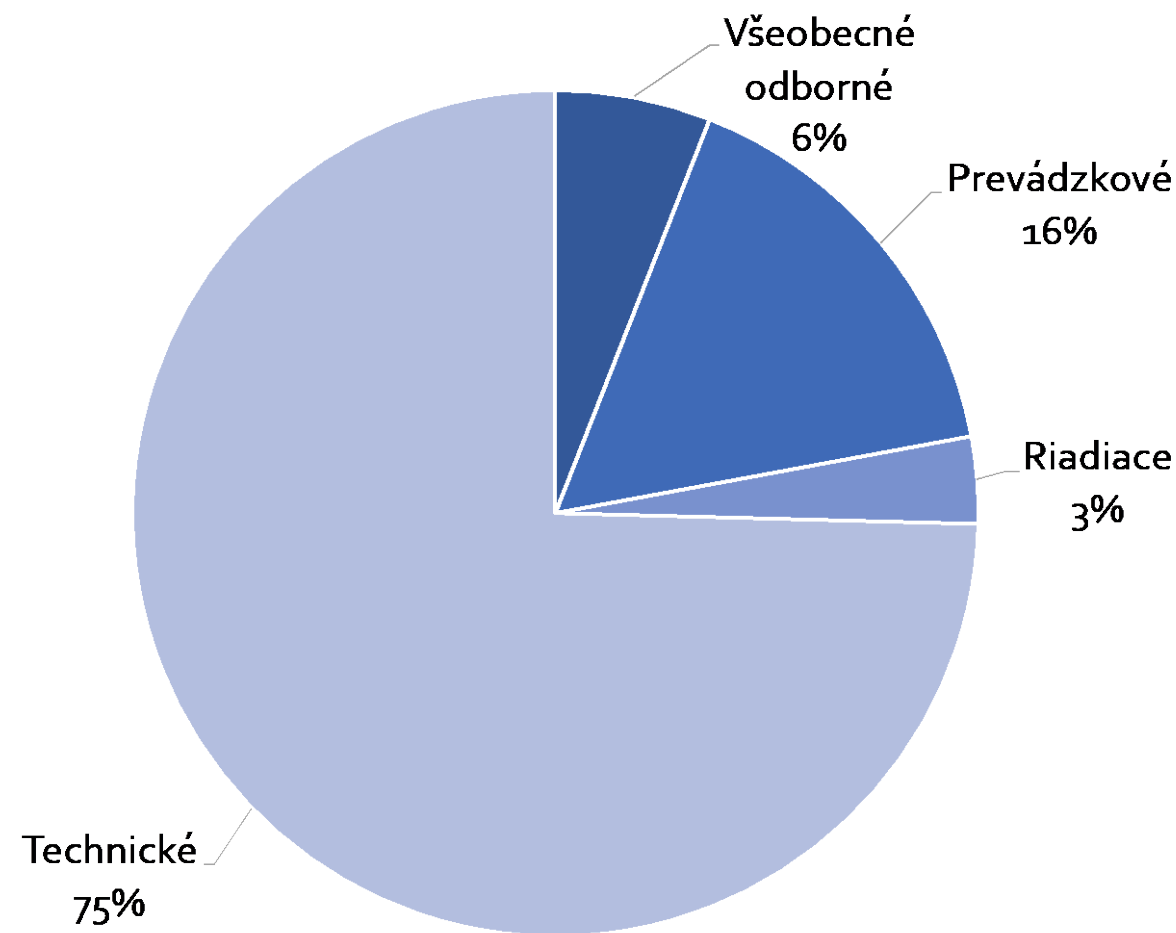


METODIKA PRE STANOVENIE KVALIFIKAČNÉHO RÁMCA ROLÍ

Použiteľná inšpirácia pre kvalifikačný rámec jednotlivých rolí je: [National Initiative for Cybersecurity Education \(NICE\)](#).

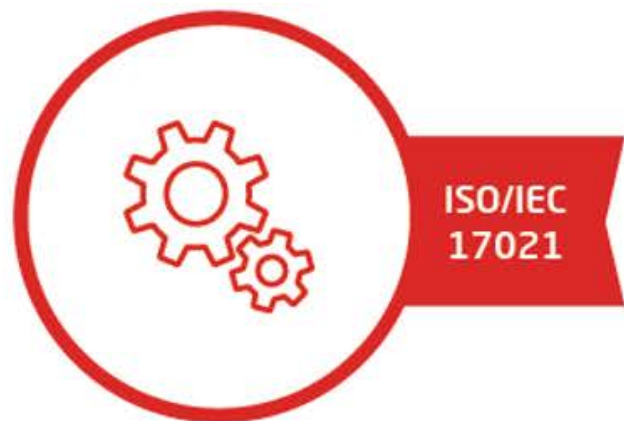
Rámec pozostáva z nasledujúcich komponentov:

- **Kategórie** – Vysokoúrovňové skupiny kvalifikačných komponentov
- **Oblasti špecializácie** – Odlišné oblasti prác
- **Pracovné roly** – množiny špecifických znalostí, zručností a schopností potrebných na vykonávanie činností v konkrétnej pracovnej úlohe





OBJEKTY POSUDZOVANIA ZHODY



SYSTÉMY|MANAŽÉRSTVA



OSOBY



PRODUKTY

STN EN ISO/IEC 17021-1

- Posudzovanie zhody - požiadavky na orgány **vykonávajúce audit a certifikáciu systémov manažérstva**

STN EN ISO/IEC 17024

- Posudzovanie zhody - všeobecné požiadavky na orgány **vykonávajúce certifikáciu osôb**

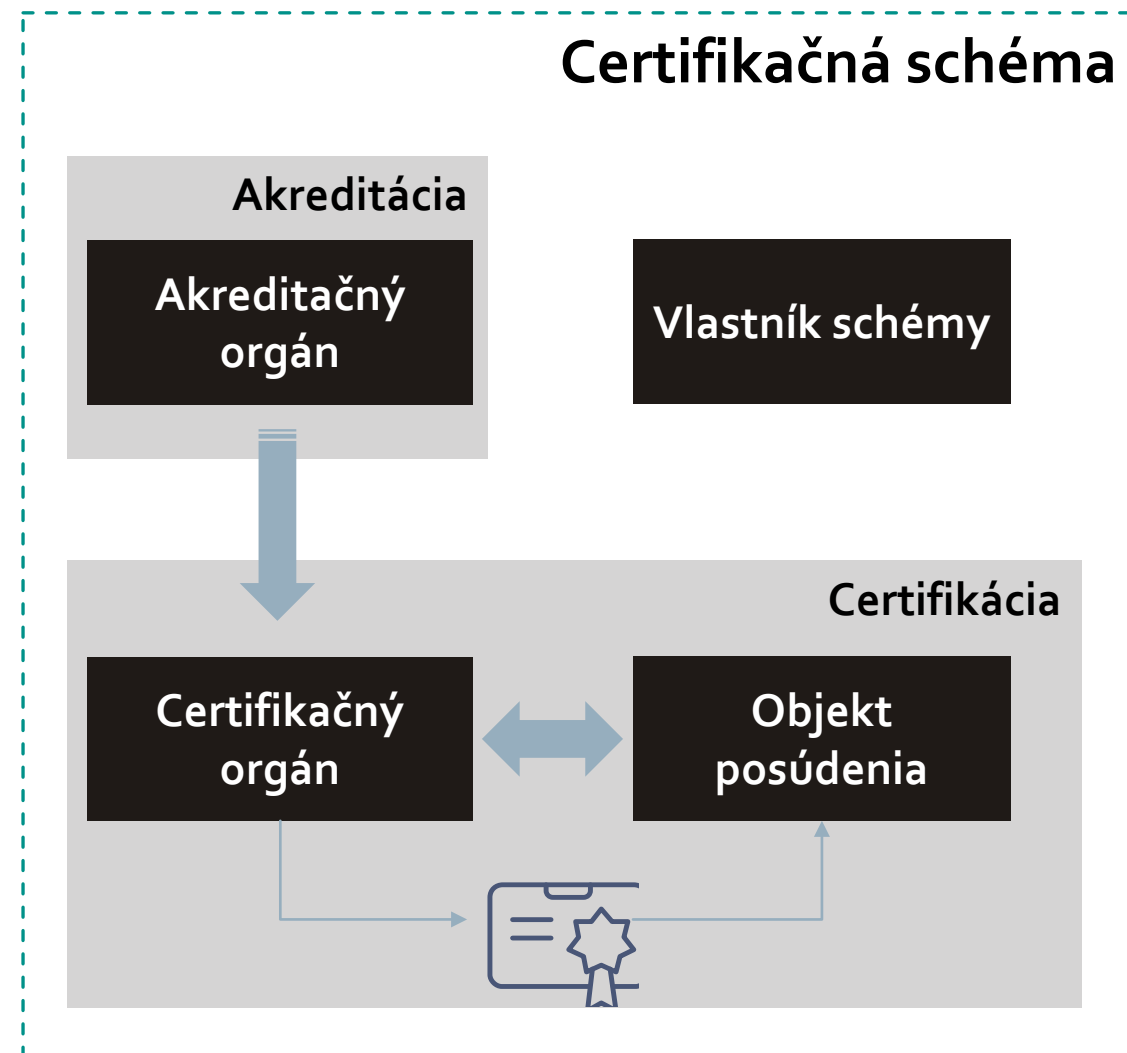
STN EN ISO/IEC 17065

- Posudzovanie zhody - požiadavky na orgány **vykonávajúce certifikáciu výrobkov, procesov a služieb**



PROCES AKREDITÁCIE PRE POSUDZOVANIE ZHODY

- **Akreditačný orgán:** autoritatívny orgán, ktorý vykonáva akreditáciu. (V Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba – SNAS)
(STN EN ISO/IEC 17000: 2005, čl. 2.6)
- **Certifikačný orgán:** orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy
(ISO/IEC 17065: 2012, čl. 3.12)
- **Akreditácia** - atestácia treťou stranou týkajúca sa orgánu posudzovania zhody, ktorá slúži ako oficiálny dôkaz kompetentnosti plniť špecifické úlohy posudzovania zhody
(STN EN ISO/IEC 17000: 2005, čl. 5.6)
- **Certifikácia:** atestácia treťou stranou týkajúca sa produktov, procesov, systémov alebo osôb.
(STN EN ISO/IEC 17000: 2005, čl. 5.5)





CERTIFIKAČNÁ SCHÉMA



- **Certifikačná schéma:** systém certifikácie, ktorý sa vzťahuje na určené objekty, na ktoré sa aplikujú rovnaké určené požiadavky, osobitné pravidlá a postupy. (ISO/IEC 17065: 2012, čl. 3.9)



- **Vlastník schémy:** osoba alebo organizácia zodpovedná za rozvoj a udržiavanie konkrétnej certifikačnej schémy (ISO/IEC 17065: 2005, čl. 3.11)

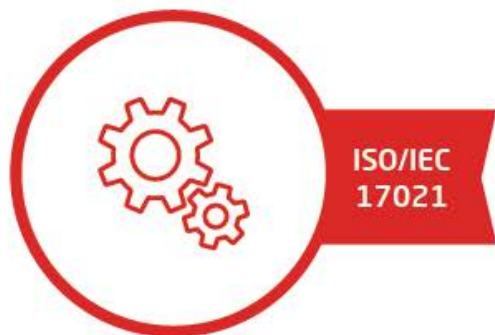
Certifikačné schémy obsahujú dva kľúčové prvky:

1. Kritériá stanovujúce konkrétne certifikačné požiadavky na posúdenie (tieto tvoria špecifikáciu, podľa ktorej sa posudzuje zhoda)
2. Metodiku posudzovania ktorú aplikuje certifikačný orgán na vykonanie posúdenia zhody

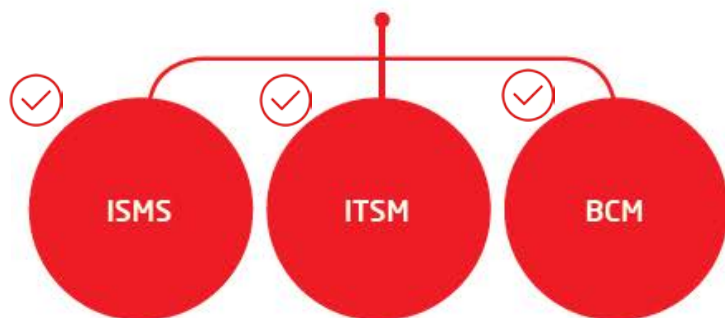




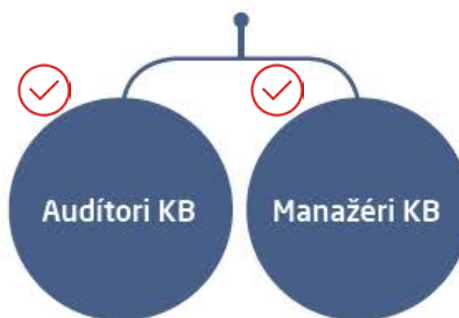
POSUDZOVANIE ZHODY V KB NA SLOVENSKU



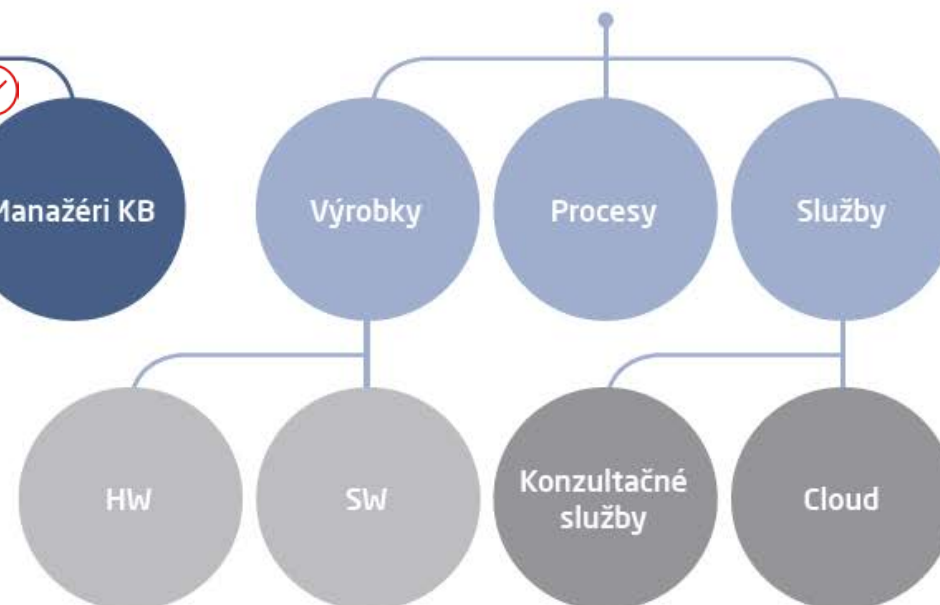
SYSTÉMY|MANAŽÉRSTVA



OSOBY



PRODUKTY





STAV KREDITÁCIE PRE JEDNOTIVÉ OBJEKTY POSUDZOVANIA ZHODY

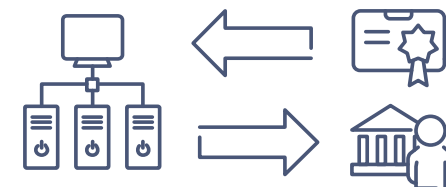
OBLASŤ	SYSTÉMY MANAŽÉRSTVA ISO/IEC 17021	OSOBY ISO/IEC 17024	VÝROBKY, PROCESY A SLUŽBY ISO/IEC 17065/ 17025
Audítori kybernetickej bezpečnosti		✓	
Manažéri kybernetickej bezpečnosti		✓	
Produkty v kybernetickej bezpečnosti – všeobecné IKT – HW			~
Produkty v kybernetickej bezpečnosti – všeobecné IKT – SW			~
Produkty v kybernetickej bezpečnosti– služby v KB			~
Produkty v kybernetickej bezpečnosti – cloudové služby			~
Produkty v kybernetickej bezpečnosti – 5G			~
Ochrana utajovaných skutočností – mechanické zábranné prostriedky			~
Ochrana utajovaných skutočností – Technické prostriedky			✓
Ochrana utajovaných skutočností – TEMPEST/ Nežiaduce elektromagnetické vyžarovanie			~
Ochrana utajovaných skutočností - Šifrovacie prostriedky			
Systém manažérstva informačnej bezpečnosti (ISO/IEC27001)	✓		
Systém manažérstva (IT) služieb (ISO/IEC20000)	✓		
Systém manažérstva kontinuity činností (ISO 22301)	✓		
Systém manažérstva kvality (ISO9001)	✓		
Dôveryhodné služby - služby kvalifikovanej časovej pečiatky			✓



- [STN EN ISO/IEC 17000 Posudzovanie zhody - Slovník a všeobecné zásady]:
 - **dohl'ad**: systematické opakovanie činností posudzovania zhody ako základ udržania platnosti stanoviska o zhode
 - **pozastavenie**: dočasná neplatnosť stanoviska o zhode pre celý určený rozsah atestácie alebo pre jeho časť
 - **zrušenie**: odvolanie stanoviska o zhode
- [Zmluva s certifikovaným audítorom kybernetickej bezpečnosti]:
 - **Certifikačný orgán je oprávnený**:
 - vykonať mimoriadne posudzovanie splnenia certifikačných požiadaviek, ak je to potrebné,
 - pozastaviť, prípadne zrušiť certifikáciu, ak sa preukáže neplnenie certifikačných požiadaviek alebo porušenie certifikačných podmienok, za ktorých bol audítorovi kybernetickej bezpečnosti udelený certifikát



POSUDZOVANIE ZHODY



- Overované entity a prvky sú v procese overovania úrovne bezpečnosti všeobecne nazývané ako „**objekty posúdenia**“ (z angl. „assessment objects“)
- **Certifikácia** (Posudzovanie zhody) - Atestácia nezávislým akreditovaným orgánom posudzovania zhody, týkajúca sa charakteristík objektu posudzovania
- Typickým výstupným dokumentom posudzovania zhody je **certifikát**, vydaný **akreditovaným orgánom posudzovania zhody**

Pre certifikáciu je typická požiadavka na akreditáciu a dohľad