



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

Kybernetické bezpečnostné riziká v kontexte legislatívnych a normatívnych požiadaviek

Konferencia eFocus

Kybernetická bezpečnosť, hrozby a ohrozenia v digitálnom svete



REGULÁCIA: ÁNO ČI NIE?

Konferencia eFocus: Kybernetická bezpečnosť, hrozby a ohrozenia v digitálnom svete



PRAMENE PRÁVA A REGULÁCIA



- Zmysel zákonov určuje konkrétna skutočnosť, ktorá vyvoláva potrebu ich prijatia
 - tento zmysel sa nazýva **prameň práva**
- Materiálne pramene práva - **faktory, ktoré vplývajú na tvorbu práva** (ekonomické, sociálne, technologické, politické, geografické, mravné a ekologické, a iné...)
- Regulácia sa vykonáva prostredníctvom normatívnych právnych aktov, t.j. všeobecne záväzných právnych prepisov
- Pravidlá a ich vynucovanie majú za cieľ **dosiahnuť žiaduce správanie zúčastnených subjektov**
- O právach a povinnostiach dozorovaných subjektov je oprávnená rozhodovať **štátna moc**

[1] Prusák, J. *Teória práva*. 2. vyd. Bratislava : Vydavateľské oddelenie PF UK, 2001. 188 s. ISBN 80 – 7160 – 146 – 2



MÔŽE REGULÁCIA POMÔŤ KYBERNETICKEJ BEZPEČNOSTI?

Cieľ regulácie:

- dosiahnutie primeranej úrovne kybernetickej bezpečnosti, ochrany informácií, ochrany údajov a ochrany súkromia

Čiastkové úlohy:

- návrh jednotných metód ochrany informácií
- návrhy na zlepšenie procesov riadenia hrozieb a rizík
- vynútenie aktivít zameraných na dosiahnutie dostatočnej úrovne ochrany dát a informácií
- tlak na dosiahnutie stavu odolnosti voči zraniteľnostiam

Nástroj dosiahnutia:

- Všeobecne záväzné právne predpisy, ktoré:
 - efektívne stanovujú pravidlá a
 - dosiahnu žiaduce správanie zúčastnených subjektov





LAISSEZ-FAIRE

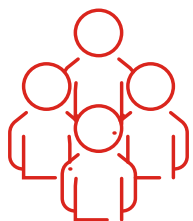
- **Laissez-faire** je francúzska fráza ktorá znamená „**ponechať**“ alebo „**nechať veci tak**“,
- Zároveň názov doktríny ktorá sa používa na označenie prístupu k politike bez pomoci štátu
- Teória laissez-faire presadzuje odolávanie vládnym zásahom pri stanovovaní politík prostredníctvom zákonov, nariadení, dotácií, ciel, daní a iných obmedzení
- Laissez-faire podporuje kapitalizmus a filozofiu voľného obchodu a slobodného správania **bez obmedzovania práv iných ľudí**





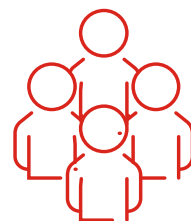
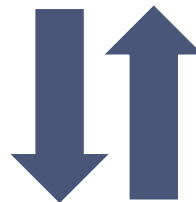
MIERA REGULÁCIE

Laissez-faire



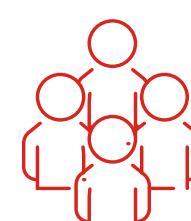
Konajte slobodne,
bez porušenia práv tretích strán

Demokratická



Dohodnime sa všeobecne,
ako by sme mali konať

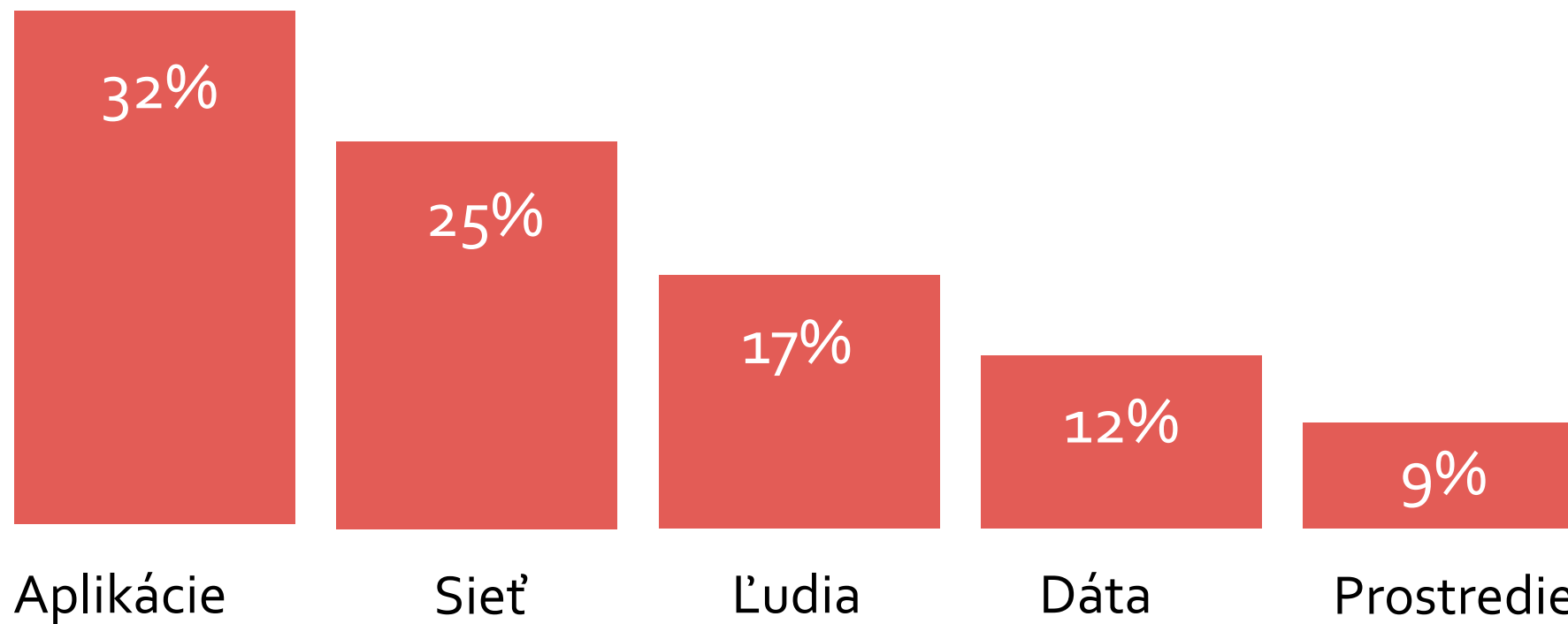
Autokratická



Konajte tak, ako vám je nariadené



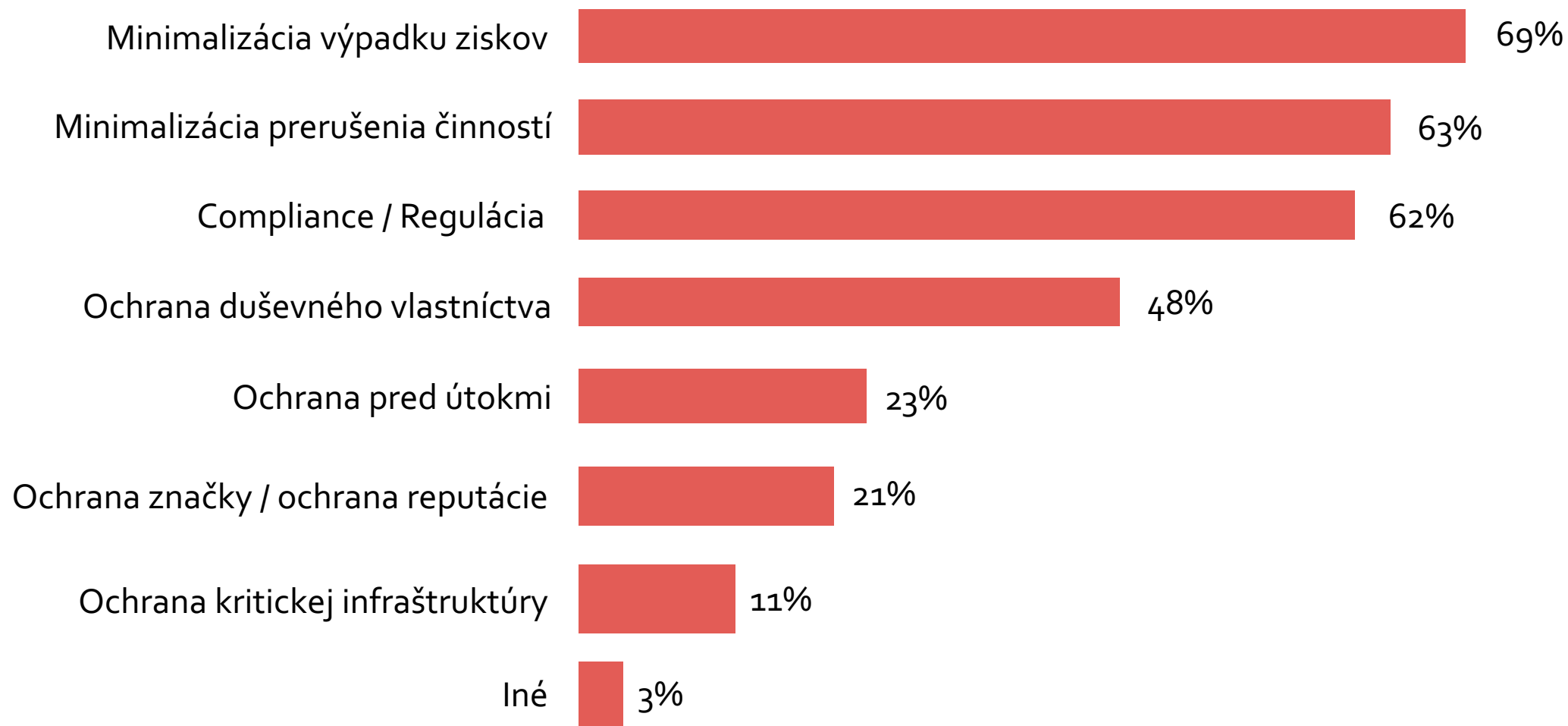
AKÝ JE NAJČASTEJŠÍ VEKTOR INCIDENTOV?



Zdroj: Ponemon's Application Security Risk Study



AKÉ SÚ TYPICKÉ SUBJEKTÍVNE DÔVODY PRE RIADENIE BEZPEČNOSTNÉHO RIZIKA?



Zdroj: Ponemon's Application Security Risk Study



PRÁVNÁ ÚPRAVA KYBERNETICKEJ BEZPEČNOSTI

Konferencia eFocus: Kybernetická bezpečnosť, hrozby a ohrozenia v digitálnom svete



INFORMAČNÁ VS. KYBERNETICKÁ BEZPEČNOSŤ

- **Informačná bezpečnosť** je zachovanie **dôvernosti, integrity a dostupnosti** informácií [ISO/IEC 27032, čl. 2.33]
- **Kybernetická bezpečnosť** je zachovanie **dôvernosti, integrity a dostupnosti** informácií v kybernetickom priestore [ISO/IEC 27032, čl. 4.20]
- Informačná bezpečnosť (resp. bezpečnosť informácií) sa všeobecne považuje najmä za stav, v ktorom sú informácie považované za odolné voči hrozbám, bez ohľadu na:
 - Fyzikálny stav dát
 - Formát dát
 - Spôsob interpretácie dát
 - Médium, prostredníctvom ktorého sú dáta uchovávané a prenášané





PRÁVNE PREDPISY PODĽA ICH PRÁVNEJ SILY

Právne akty Európskej únie

Primárne právne akty EÚ:

- Záväzné zmluvy medzi členskými štátmi EÚ
- Charta základných práv
- Všeobecné zásady Súdneho dvora Európskej únie

Sekundárne právne akty EÚ:

- Nariadenia
- Smernice
- Rozhodnutia
- Odporúčania

Národná legislatíva SR

- Ústava SR a ústavné zákony
- Medzinárodné zmluvy a referendá so silou zákona
- Medzinárodné zmluvy a referendá so silou ústavného zákona

- Zákony NRSR

- Vykonávacie právne predpisy (Vyhlášky)
 - Nariadenia vlády



PLATNÁ EURÓPSKA PRÁVNA ÚPRAVA KB

Smernica (EÚ) 2016/1148
o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti
sietí a informačných systémov v Únii

NIS

Nariadenie (EÚ) 2019/881
o agentúre ENISA (Agentúra Európskej únie pre kybernetickú
bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a
komunikačných technológií

Cyber Act

Nariadenie (EÚ) 2019/887
ktorým sa zriaďuje Európske centrum odvetvových, technologických a
výskumných kompetencií a sieť národných koordinačných centier

ECCC

Nariadenie (EÚ) 2019/765
ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v
súvislosti s uvádzaním výrobkov na trh

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



PLATNÁ NÁRODNÁ PRÁVNÁ ÚPRAVA KB

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

Vyhláška NBÚ č. 164/2018 Z.z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby)

Vyhláška NBÚ č. 165/2018 Z.z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov

Vyhláška č. 166/2018 o podrobnostiach o technickom, technologickom a personálnom vybavení CSIRT

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

Vyhláška NBÚ č. 436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

Zákon č. 45/2011 Z.z.
o kritickej infraštruktúre

Zákon č. 95/2019 Z.z.
o informačných technológiách vo verejnej správe

Vyhláška ÚPVII č. 179/2020 Z.z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy



OSTATNÉ PRÁVNE AKTY EÚ S DOSAHOM NA IB/KB

Nariadenie (EÚ) 2016/679

o ochrane fyzických osôb pri spracúvaní osobných údajov
a o voľnom pohybe takýchto údajov,
(všeobecné nariadenie o ochrane údajov)

GDPR

Smernica (EÚ) 2015/2366

o platobných službách na vnútornom trhu

PSD2

Nariadenie (EÚ) 910/2014

o elektronickej identifikácii a dôveryhodných službách pre
elektronické transakcie na vnútornom trhu

eIDAS

Smernica (EÚ) 2002/58/ES

týkajúca sa spracovávaní osobných údajov a ochrany súkromia v
sektore elektronických komunikácií

ePD

Smernica (EÚ) 2018/1972

ktorou sa stanovuje európsky kódex elektronických komunikácií

EECC



PRIPRAVOVANÉ PRÁVNE AKTY EÚ S DOSAHOM NA IB/KB

Nariadenie (EÚ)

o rešpektovaní súkromného života a ochrane osobných údajov
v elektronických komunikáciách

ePrivacy

Nariadenie (EÚ)

o digitálnej prevádzkovej odolnosti finančného sektora

DORA

Smernica (EÚ)

o opatreniach na zabezpečenie vysokej spoločnej úrovne
bezpečnosti sietí a informačných systémov v Únii

NIS2

Nariadenie (EÚ)

ktorým sa stanovujú harmonizované pravidlá v oblasti umelej
inteligencie

AI Act

Nariadenie (EÚ)

o jednotnom trhu s digitálnymi službami (akt o digitálnych službách)

DSA

Nariadenie (EÚ)

o konkurencieschopných a spravodlivých trhoch v digitálnom
sektore (akt o digitálnych trhoch)

DMA

Nariadenie (EÚ)

o polovodičových čipoch

Chips Act

Nariadenie (EÚ)

o odolnosti v oblasti kybernetickej bezpečnosti

CRA

Commission work programme 2022: [Making Europe stronger together](#)



TECHNICKÁ NORMALIZÁCIA

Konferencia eFocus: Kybernetická bezpečnosť, hrozby a ohrozenia v digitálnom svete



Význam technickej normalizácie:

- Nie je potrebné definovať, čo už je známe a overené najlepšou praxou
- Prostredníctvom štandardov je možné zaručiť kompatibilitu metód ochrany informačných aktív

Základné delenie ISO noriem, resp. ISO/IEC noriem v oblasti IB/KB:

- Systém manažérstva informačnej bezpečnosti (ISMS)
- Kryptológia
- Posudzovanie a certifikácia bezpečnosti
- Bezpečnostné opatrenia
- Identifikácia a autentizácia

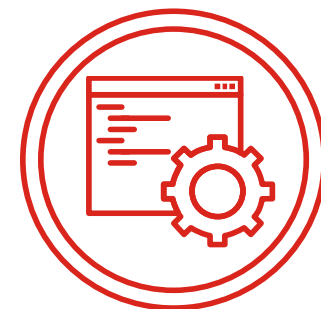
Trieda noriem ISO/IEC 27000 je vyhradená pre riadenie informačnej bezpečnosti

Popis ucelenej triedy noriem 27000 je uvedený napríklad na adrese: www.iso27001security.com



SYSTÉMY MANAŽÉRSTVA RELEVANTNÉ PRE IB/KB

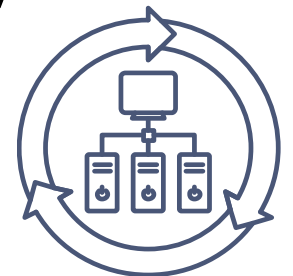
- **Systém manažérstva** je súbor politík, procesov a postupov používaných organizáciou na zabezpečenie zlepšovania výkonnosti, stanovením opakovateľných krokov, ktoré organizácia vedome implementuje na dosiahnutie svojich cieľov a zámerov
- Typické manažérske systémy v oblasti kybernetickej bezpečnosti:
 - **Systém riadenia IT služieb** (ITSM), podľa noriem radu ISO/IEC 20 000
 - **Systém riadenia informačnej bezpečnosti** (ISMS) podľa noriem radu ISO/IEC 27 000
 - **Riadenie kontinuity činností** (BCM) podľa normy ISO/IEC 22 301
 - **Riadenie kvality** (QM) podľa normy ISO 9001





SYSTÉM MANAŽÉRSTVA INFORMAČNEJ BEZPEČNOSTI (ISMS)

- Pre informačnú bezpečnosť existuje rokmi vyskúšaný manažérsky systém, ktorý je známy pod názvom **Systém manažérstva informačnej bezpečnosti (Information Security Management System)**, komplexne opísaný v triede medzinárodných noriem ISO/IEC 27000
- ISMS chráni dôvernosť, integritu a dostupnosť informácií zavedením procesu riadenia rizík a poskytnutím dôvery zainteresovaným stranám, že riziká sú dostatočne riadené
- Pod pojmom **systém zabezpečenia kybernetickej bezpečnosti**, sa v zákone chápe **systém manažérstva informačnej bezpečnosti** so zameraním na bezpečnosť informácií v kybernetickom priestore





AKREDITAČNÉ NORMY RELEVANTNÉ PRE IB/KB

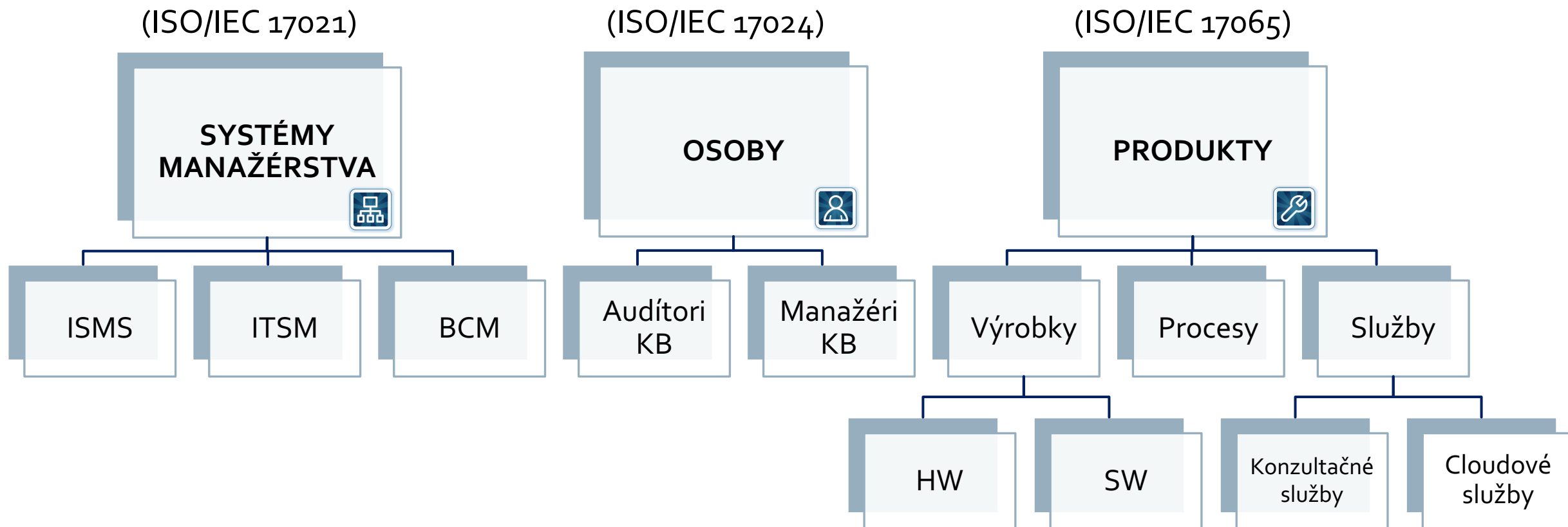


Schéma podľa Nariadenia 2008/765



OBJEKTY POSUDZOVANIA ZHODY (CERTIFIKÁCIA V IB/KB)

OBLASŤ	SYSTÉMY MANAŽÉRSTVA ISO/IEC 17021	OSOBY ISO/IEC 17024	VÝROBKY, PROCESY A SLUŽBY ISO/IEC 17065/ 17025
KB – audítori		✓	
KB – manažéri		✓	
KB - HW			✓
KB - SW			✓
KB – služby v KB			✓
KB – cloudové služby			✓
KB – 5G			✓
OUS - FOB			✓
OUS - TP			✓
OUS - TEMPEST/ NEV			✓
OUS - ŠOI			✓
ISMS (ISO/IEC27001)	✓		
ITSM (ISO/IEC20000)	✓		
BCM (ISO 22301)	✓		
QM (ISO9001)	✓		
eIDAS		✓	✓



NORMY NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

- Národný ústav technickej normalizácie ústav v pôsobnosti Ministerstva obchodu USA
- Vydáva aj niektoré štandardy „Special Publication“ týkajúce sa bezpečnosti informácií:
 - NIST SP 800-30, Risk Management Guide for IT Systems
 - NIST SP 800-39, Managing Risk from Information Systems
 - NIST SP 800-14, Generally Accepted Principles and Practices for Securing IT Systems
 - NIST SP 800-18, Guide For Developing Security Plans for IT Systems
 - NIST SP 800-26, Security Self-Assessment Guide for IT Systems
 - NIST SP 800-64, Security Considerations in the System Development Life Cycle
 - NIST SP 800-27, Engineering Principles for IT Security
 - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
 - NIST SP 800-100 Information Security Handbook: A Guide for Managers



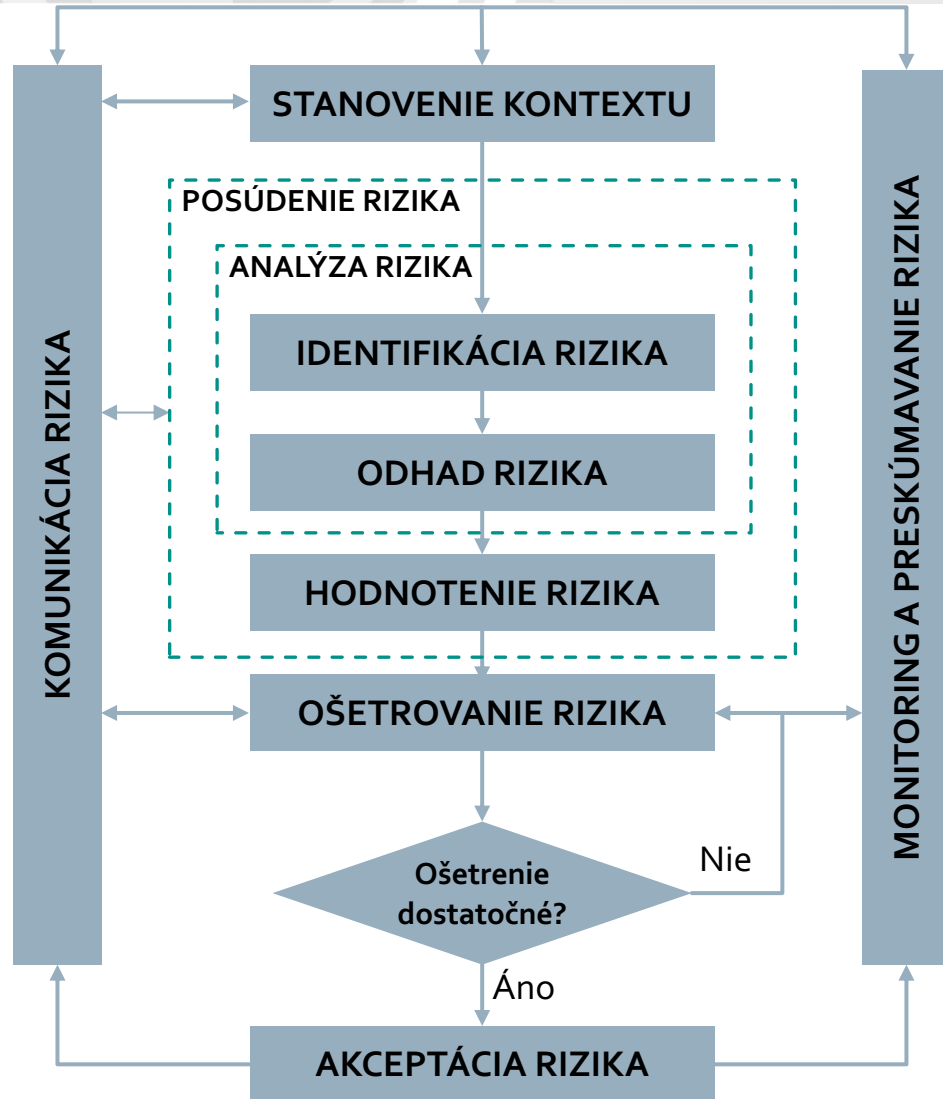


RIADENIE RIZÍK

Konferencia eFocus: Kybernetická bezpečnosť, hrozby a ohrozenia v digitálnom svete



RIADENIE RIZÍK V KONTEXTE REGULÁCIE



- Vo Vyhláške NBÚ č. 362/2018 Z.z. sú obsiahnuté všetky fázy a podprocesy riadenia rizika podľa ISO/IEC 27005
- NBÚ vydal Metodiku analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Väčšina všeobecne záväzných právnych predpisov relevantných z hľadiska IB/KB navrhuje „risk-based“ prístup

ZDROJ: STN ISO/IEC 27 005 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti



ZÁVER (ALEBO SKÔR OTÁZKY NA ZAMYSLENIE)

- Je potreba ochrany informačných aktív relevantným prameňom práva?

- Je požiadavka na zaručenie súladu hlavnou motiváciou pre ochranu informačných aktív?
- Platné a navrhované právne prepisy:
 - stanovujú pravidlá efektívne?
 - dosahujú žiaduce správanie zúčastnených subjektov?

- Je súčasná miera regulácie priklonená:
 - od demokratickej skôr ku princípu laissez-faire?
 - od demokratickej skôr ku autokratickému prístupu?

- Môže bezpečnosť založená na riadení rizika organizáciám napomôcť:
 - priebežne sledovať celkovú rizikovú expozíciu organizácie?
 - stanovovať priority pre ošetrovanie rizík v súlade s rizikovým apetítom organizácie?



Ochrana vlastnických 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 vlastnických 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](https://twitter.com/CybercenterSk)