Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti

Právny rámec, organizácia KB a strategické plánovanie

Kurz: Manažér kybernetickej bezpečnosti

Prof. Ing. Tomáš Loveček, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Tomas.Lovecek@uniza.sk

Blok I.: Právny rámec, organizácia KB a strategické plánovanie

Hod. Obl.	Oblasti	Garant	Vyuč. hod.
2	Organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti	Loveček	1,2
2	Správa aktív, ochrana záznamov, súkromia a označovanie informácií	Loveček	3,4
6	Riadenie kybernetických hrozieb a rizík	Loveček	5,6,7,8,9,10

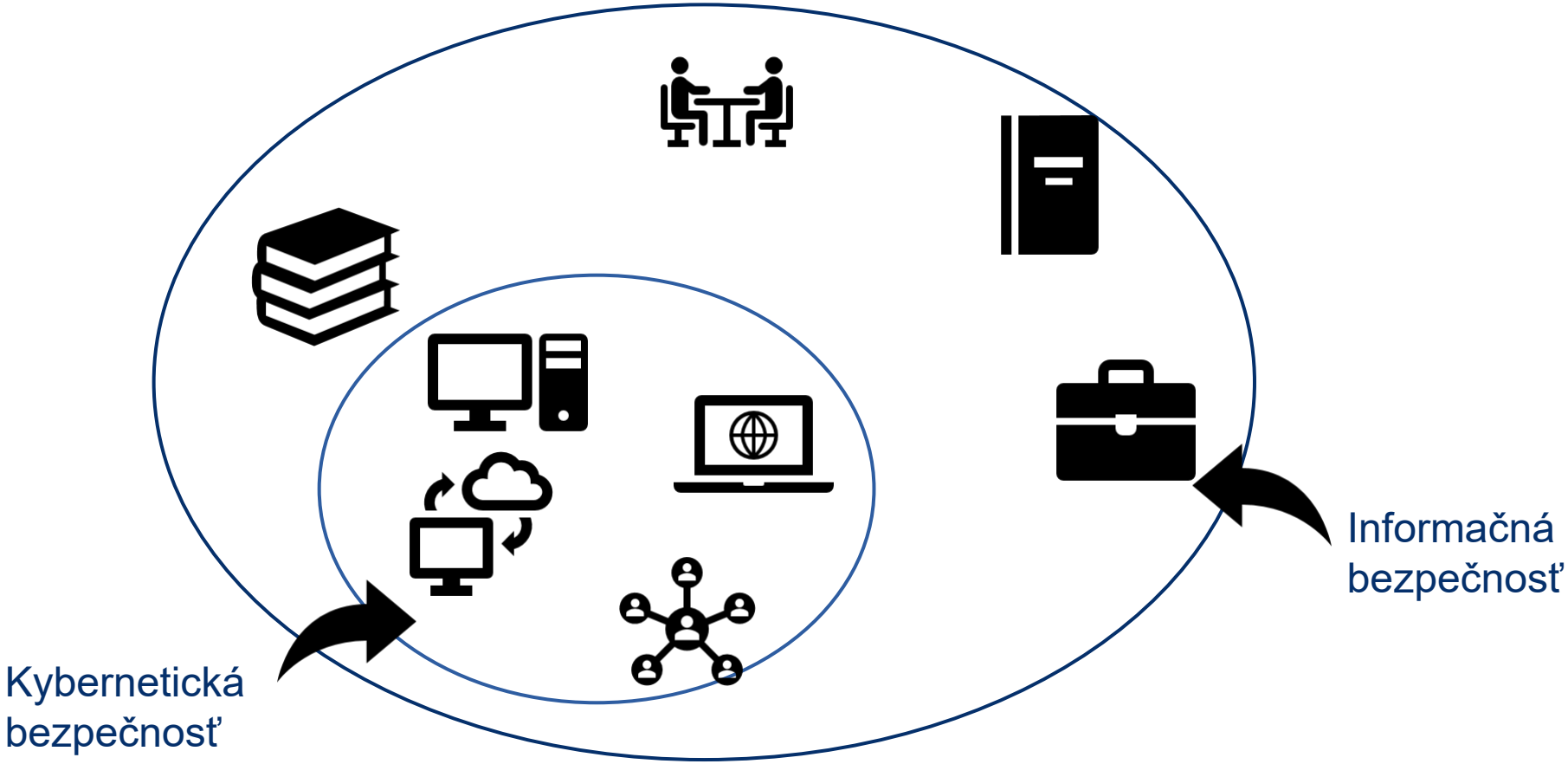
Hodina	Začiatok	Koniec	Rozsah
1	8:00	8:45	0:45
2	8:45	9:30	0:45
3	9:45	10:30	0:45
4	10:30	11:15	0:45
5	11:30	12:15	0:45
6	13:00	13:45	0:45
7	13:45	14:30	0:45
8	14:45	15:30	0:45
9	15:30	16:15	0:45
10	16:30	17:15	0:45

Organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti

- Otvorenie kurzu
- Normatívne rámce informačnej a kybernetickej bezpečnosti vo verejnej správe (NIS2, GDPR, Zákon o KB, Zákon o ITVS, ISO/IEC 27000+)
- Úlohy a zodpovednosti v oblasti informačnej a kybernetickej bezpečnosti
- Systém manažérstva informačnej a kybernetickej bezpečnosti (ISMS)
- Bezpečnostná dokumentácia a jej význam
- Hodnotiace a validačné kritériá v oblasti informačnej a kybernetickej bezpečnosti (KPI, KRI)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Informačná vs kybernetická bezpečnosť



Kybernetická bezpečnosť je podmnožinou množiny informačná bezpečnosť, pretože všetky prvky sú zároveň prvkami množiny informačná bezpečnosť

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Informačná vs kybernetická bezpečnosť

- **Bezpečnosť informácií** (information security) zachovanie dôvernosti, integrity a dostupnosti informácií. Môže tiež zahŕňať ďalšie vlastnosti, napríklad autenticitu, nepopierateľnosť a spoľahlivosť. (ISO/IEC 27000)
- **kybernetická bezpečnosť** (cybersecurity), resp. **bezpečnosť kybernetického priestoru** (cyberspace security) zachovanie dôvernosti, integrity a dostupnosti informácie v kyberpriestore. (ISO/IEC 27032)

- **Kyberpriestor** (the Cyberspace) komplexné prostredie, ktoré je výsledkom interakcie ľudí, softvéru a služieb na internete prostredníctvom technologických zariadení a sietí naň pripojených, ktoré neexistuje v akejkoľvek fyzickej podobe. (ISO/IEC 27032)
- **Kyberzločin** (Cybercrime) trestná činnosť, pri ktorej sa služby alebo aplikácie v kyberpriestore používajú na trestný čin alebo sú jeho cieľom, alebo kde je kyberpriestor zdrojom, nástrojom, cieľom alebo miestom trestného činu. (ISO/IEC 27032)
- **Internetová kriminalita** (Internet crime) trestná činnosť, pri ktorej sa služby alebo aplikácie na internete používajú na trestný čin alebo sú cieľom trestného činu, alebo kde je internet zdrojom, nástrojom, cieľom alebo miestom trestného činu. (ISO/IEC 27032)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Požiadavky na informačnú bezpečnosť

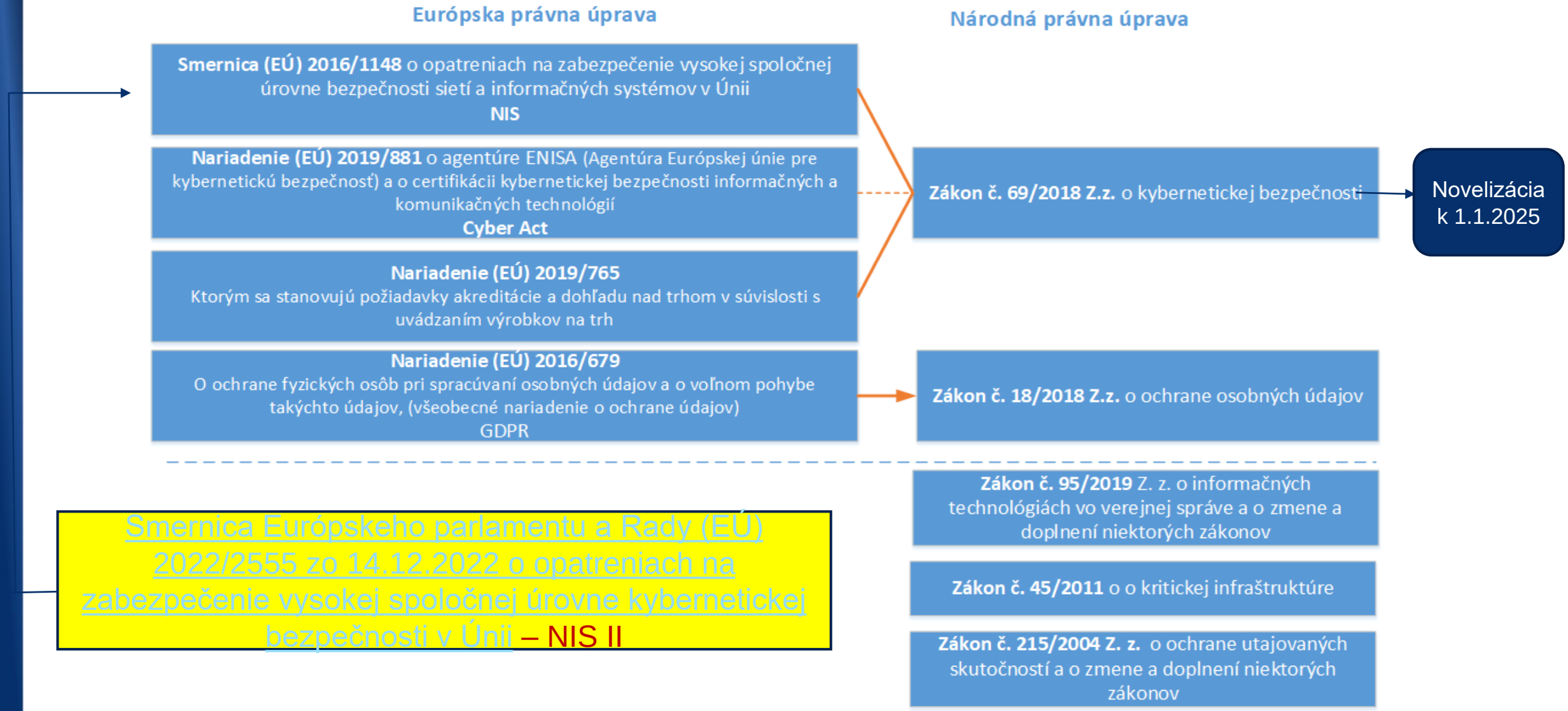
- Je nevyhnutné, aby organizácia určovala svoje požiadavky na informačnú bezpečnosť. Existujú tri hlavné zdroje požiadaviek na informačnú bezpečnosť (ISO/IEC 27002):

a) **posúdenie rizík organizácie**, pričom sa zohľadňuje celková obchodná stratégia a ciele organizácie. To sa dá uľahčiť alebo podporovať prostredníctvom hodnotenia rizík informačnej bezpečnosti. Výsledkom by malo byť určenie opatrení potrebných na zabezpečenie toho, aby zostatkové riziko organizácie spĺňalo jej kritériá pre akceptáciu rizika.

b) **právne, zákonné, regulačné a zmluvné požiadavky**, ktoré organizácia a jej zainteresované strany (obchodní partneri, poskytovatelia služieb atď.) musia dodržiavať a ich sociálno-kultúrne prostredie;

c) **súbor zásad, cieľov a obchodných požiadaviek** pre všetky kroky životného cyklu informácií, ktoré organizácia vyvinula na podporu svojej prevádzky.

Normatívne rámce KIB vo VS



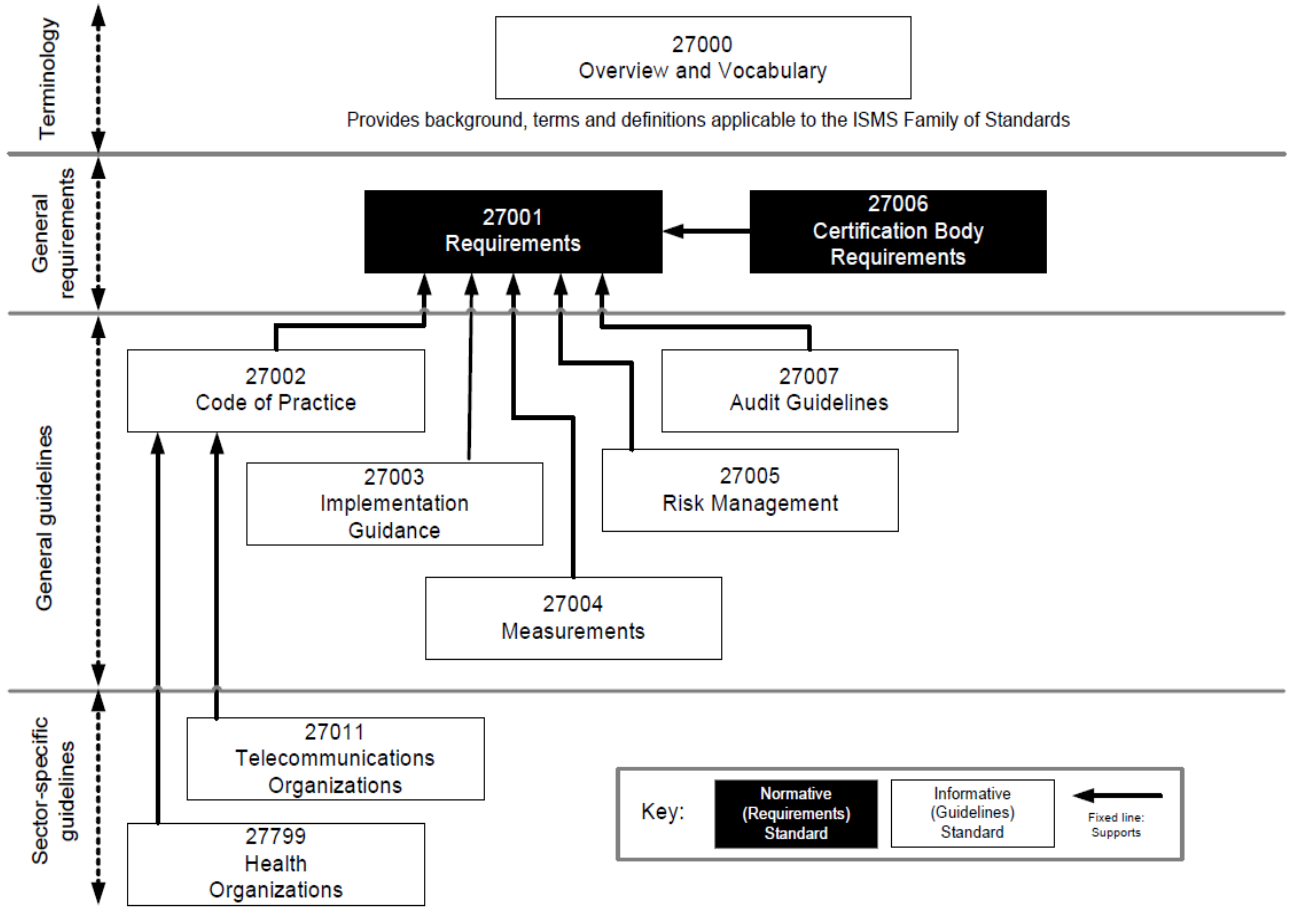
7

Normatívne rámce KIB vo VS

- Rad noriem ISO/IEC 2700 je zložený zo vzájomne súvisiacich noriem, či už zverejnených alebo pripravovaných, a obsahuje celý rad významných štrukturálnych komponentov. Tieto komponenty sú zamerané na:
  a) normy popisujúce požiadavky ISMS (ISO/IEC 27001),
  b) požiadavky certifikačného orgánu na organizácie certifikujúce zhodu s ISO/IEC 27001 a
  c) ďalšie rámcové požiadavky na implementácie ISMS špecifické podľa odborov.
- Ďalšie dokumenty poskytujú návod pre rôzne stránky implementácie ISMS a zaoberajú sa generickým procesom rovnako ako návody špecifickými podľa odborov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Normatívne rámce KIB vo VS

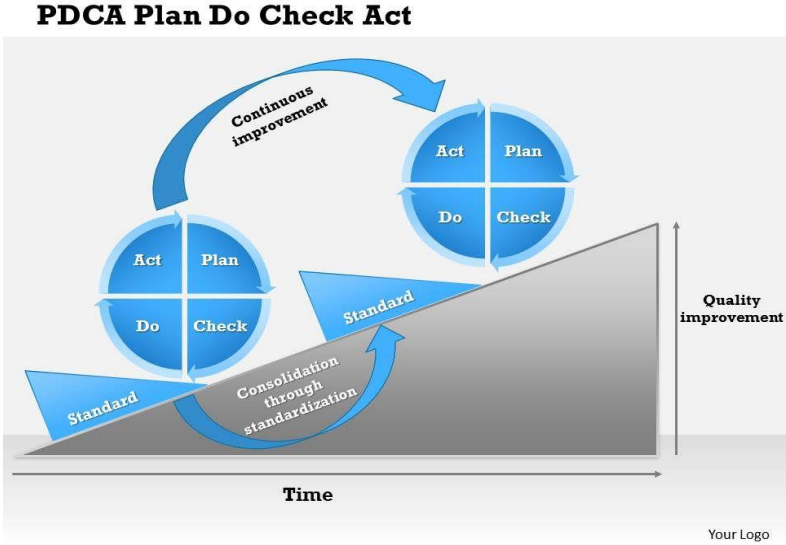


Vzťahy medzi jednotlivými normami rady ISO/IEC 27000 (ISO/IEC 27000)

https://www.csirt.gov.sk/prehlad-standardov-iso-iec-27000.html?csrt=9847527579193658880

Systém manažérstva informačnej bezpečnosti

- **Systém Manažérstva Informačnej bezpečnosti** (ISMS: Information Security Management System) pozostáva z politík, postupov, smerníc a príslušných zdrojov a činností, ktoré organizácia riadi, aby zabezpečila ochranu informačných aktív. (ISO/IEC 27000)
- ISMS predstavuje systematický prístup k zriadeniu, implementovaniu, prevádzkovaniu, monitorovaniu, preskúmavaniu, udržiavaniu a zlepšovaniu bezpečnosti informácií organizácie a to tak, aby boli dosiahnuté jej ciele.
- Je založený na posudzovaní rizík a na úrovniach prijatia rizík organizácie, ktoré boli navrhnuté pre efektívne ošetrenie rizík a pre ich riadenie.
- Organizácia musí vybudovať, udržiavať a trvalo zlepšovať systém manažérstva informačnej bezpečnosti vrátane potrebných procesov a ich vzájomných väzieb v súlade s požiadavkami tohto dokumentu.



Bezpečnostná dokumentácia a jej význam

- Bezpečnostné opatrenia sa prijímajú a realizujú na základe **schválenej bezpečnostnej dokumentácie**, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu. §20 ods. 3) Zákona o KB)

- Bezpečnostná dokumentácia obsahuje (Vyhláška NBÚ č. 227/2025 Z.z. o bezpečnostných opatreniach):

a) schválenú stratégiu kybernetickej bezpečnosti určujúcu ciele, ktoré je potrebné v riadení kybernetickej bezpečnosti dosiahnuť, spolu s uvedením základných princípov na ich dosiahnutie a určením právomocí a zodpovedností za systémy manažérstva, riadenie rizík a aktualizáciu bezpečnostnej dokumentácie,

b) schválené bezpečnostné politiky pre jednotlivé oblasti riadenia kybernetickej bezpečnosti vrátane opisu súvisiacej organizačnej štruktúry, procesov a väzieb, pracovných rolí, zodpovednosti a delenia právomocí a opisu rámca riadenia bezpečnostných rizík,

c) vykonanú klasifikáciu informácií,

d) určenie sietí a informačných systémov a operačných technológií do príslušnej kategórie informačných a komunikačných technológií alebo operačných technológií,

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostná dokumentácia a jej význam

a) vykonanú analýzu rizík a určenie úrovne identifikovaných rizík, akceptovaných rizík a zvyškových rizík pre aktíva spolu so zoznamom aktív,

e) zadokumentované určenie rozsahu a spôsobu prijatia, dodržiavania a vykonávania bezpečnostných opatrení vrátane odôvodnenia neprijatia bezpečnostného opatrenia,

f) poslednú záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti,

g) iné dokumenty, ak to ustanovuje osobitný predpis (napr. Posúdenie vplyvu na ochranu osobných údajov - GDPR).

Bezpečnostná dokumentácia a jej význam

- **Koncepcia rozvoja** je **dokument** vypracovaný orgánom riadenia pre informačné technológie verejnej správy, ktorých je správcom, definujúci ciele, organizačné, technické a technologické nástroje, architektúru informačných technológií verejnej správy a plánovanie jednotlivých aktivít, najmä s cieľom riadneho a včasného naplnenia požiadaviek národnej koncepcie a strategických priorít informatizácie verejnej správy. (§13 Zákona o ITVS)
- Správca pri vytváraní alebo nadobúdaní informačného systému verejnej správy zabezpečí pre tento systém vypracovanie bezpečnostnej dokumentácie vrátane bezpečnostného projektu. (§20 Zákona o ITVS)
- **Bezpečnostný projekt informačného systému verejnej správy** sa vypracúva v súlade so všeobecne záväzným právnym predpisom vydaným ministerstvom investícií a tvorí súčasť bezpečnostnej dokumentácie. Vypracovanie bezpečnostného projektu informačného systému verejnej správy zabezpečí správca, vychádzajúc:

a) z bezpečnostnej stratégie kybernetickej bezpečnosti a bezpečnostných politík,

b) zo všeobecne akceptovaných štandardov riadenia informačných technológií, ktoré vychádzajú z uznaných technických noriem,

c) z metodických usmernení orgánu vedenia.

Bezpečnostná dokumentácia a jej význam

- **Zdokumentované informácie** sú informácie, ktoré musí organizácia kontrolovať a uchovávať, a médium, na ktorom sú uložené. (ISO/IEC 27000)

- Poznámka 1 k termínu: Zdokumentované informácie môžu byť v akomkoľvek formáte a na akomkoľvek médiu a z akéhokoľvek zdroja.
- Poznámka 2 k termínu: Zdokumentované informácie môžu odkazovať na:

a) systém riadenia vrátane súvisiacich procesov;

b) informácie vytvorené na účely fungovania organizácie (dokumentácia);

c) dôkazy o dosiahnutých výsledkoch (záznamy).

Úlohy a zodpovednosti v oblasti KIB podľa Zákona o KB

- Bezpečnostné opatrenia musia zahŕňať najmenej (§20 ods. 4)):

a) **určenie manažéra kybernetickej bezpečnosti**, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa **znalostné štandardy** pre výkon roly manažéra kybernetickej bezpečnosti. určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,

b) určenie kontaktnej **osoby pre prijímanie a evidenciu hlásení**,

c) určenie a pridelenie úloh, **rolí** a zodpovednosti podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené roly,

d) určenie konkrétnej osoby alebo konkrétnych **osôb zodpovedných za schvaľovanie bezpečnostných opatrení, dohľad, kontrolu a audit, zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie**.

- Personálna bezpečnosť pozostáva najmenej z postupov pri zaradení osoby do niektorých z **bezpečnostných rolí**, presunu práv, povinností a zodpovedností vo vzťahu ku kybernetickej bezpečnosti na inú osobu. (Vyhláška NBÚ č. 362/2018 Z.z.).

Znalostné štandardy v oblasti KB

- Znalostné štandardy sú určené na preukazovanie minimálnych požiadaviek na výkon konkrétnej roly (Vyhláška NBÚ č.492/2022 Z.z.):

a) odborný zamestnanec,
b) špecialista kybernetickej bezpečnosti,
c) manažér kybernetickej bezpečnosti,
d) audítor kybernetickej bezpečnosti,
e) tester kybernetickej bezpečnosti,
f) architekt kybernetickej bezpečnosti,
g) špecialista riadenia rizík,
h) špecialista pre analýzu digitálnych stôp,
i) špecialista pre riadenie súladu,
j) špecialista pre riešenie kybernetických incidentov,
k) analytik kybernetickej bezpečnosti,
l) lektor kybernetickej bezpečnosti.

Znalostné štandardy v oblasti KB

Manažér kybernetickej bezpečnosti

Rola:	**Manažér kybernetickej bezpečnosti**	
Vedomosti:	**Riadenie bezpečnosti**	
	1) procesy, systémy a zásady riadenia kybernetickej bezpečnosti vrátane zásad riadenia fyzickej a objektovej bezpečnosti	BL5
	2) organizácia kybernetickej bezpečnosti	BL6
	3) terminológia a skratky v oblasti kybernetickej bezpečnosti	BL6
	4) princípy riadenia IT služieb, správy systémov a správy počítačových sietí	BL5
	5) hodnotiace a validačné kritériá v oblasti kybernetickej bezpečnosti (KPI, KRI atď.)	BL5
	6) zdroje, charakteristiky a použitie informačných aktív organizácie	BL6
	7) organizačné politiky, organizačné štruktúry a koncepty plánovania vzťahov s internými a/alebo externými organizáciami	BL6
	8) koncepcie zlepšovania organizačných procesov a modely hodnotenia vyspelosti procesov (napr. CMMI)	BL6
	9) zásady a techniky plánovania kapacity a plánovania zdrojov	BL5
	10) princípy riadenia ľudských zdrojov	BL6
	11) rozpočtové pravidlá, zásady plánovania a riadenia nákladov a plánovania a riadenia investícií	BL5
	12) základy compliance v oblasti kybernetickej bezpečnosti (právny rámec aspoň na úrovni zákona o ITVS, GDPR, ePrivacy, ISO 20000)	BL3

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
	5) návrh požiadaviek na rozpočet a na iné zdroje súvisiace s bezpečnostnými opatreniami a procesmi relevantnými z hľadiska kybernetickej bezpečnosti vrátane riadenia nákladov a riadenia investícií
	6) metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie
	7) poskytovanie informácií bezpečnostnému výboru alebo štatutárnemu orgánu o stave kybernetickej bezpečnosti v organizácii, o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach
	8) riadenie kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri obstarávaní a vývoji softvéru a systémov

Úlohy a zodpovednosti v oblasti KIB podľa Zákona o ITVS

- V rámci zabezpečenia riadenia bezpečnosti je správca povinný vo svojej organizácii zaviesť a udržiavať systém riadenia informačnej bezpečnosti, ktorý zriadi **riadiacu**, **výkonnú** a **kontrolnú zložku systému riadenia bezpečnosti**, ktoré sú navzájom **personálne a kompetenčne oddelené**. (§18 ods. 1))
- Vytvorenie bezpečnostného výboru s rozsahom povinností a právomocí určených štatútom, ktorý sa skladá najmenej z (Vyhláška Úradu podpredsedu vlády SR pre investície a informatizáciu č. 179/2020 Z.z.):

a) štatutára správcu, jeho zástupcu alebo ním poverenej osoby,

b) manažéra kybernetickej bezpečnosti a informačnej bezpečnosti,

c) vedúceho zamestnanca organizačného útvaru zodpovedného za správu informačno-komunikačnej infraštruktúry,

d) vedúceho zamestnanca organizačného útvaru zodpovedného za právne a legislatívne služby,

- Vytvorenie **pozície manažéra kybernetickej bezpečnosti a informačnej bezpečnosti** v organizácii správcu mimo organizačného útvaru zodpovedného za správu a prevádzku informačných technológií verejnej správy (Vyhláška č. 179/2020 Z.z.).

Znalostné štandardy v oblasti KB

Špecialista kybernetickej bezpečnosti

KARTA ZAMESTNANIA | OBLASŤ PRE CŽV | O SEKTORE | PRIPOMIENKY A OTÁZKY | GARANCIA

Špecialista kybernetickej bezpečnosti vykonáva odborné činnosti v oblasti bezpečnosti služieb IKT. Navrhuje, implementuje, udržiava a prevádzkuje bezpečnostné mechanizmy a riešenia. Navrhuje a prezentuje bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru. Posudzuje právne a etické požiadavky na zaručenie bezpečnosti informačných aktív, navrhuje a vykonáva procesy riadenia rizík v informačnej a kybernetickej bezpečnosti. Vykonáva a podporuje kontroly a posudzovanie bezpečnostných procesov, systémov a mechanizmov a ošetruje odchýlky od požadovaného stavu. Spolupracuje na projektoch, na rozvoji nástrojov a postupov k optimalizácii bezpečnostných systémov, mechanizmov a opatrení. Stanovuje požiadavky, podmienky a štandardy pre oblasť bezpečnosti programov, databáz, systémov a sietí. Vyhodnocuje efektívnosť bezpečnostných mechanizmov a riešení a uplatňuje ich v procesoch organizácie. Spracováva príslušné interné predpisy a dohliada nad ich plnením. Posudzuje zranit...
viac...

Sektorová rada	Sektorová rada pre informačné technológie a telekomunikácie
Kód/revízia	17928/2
Garant	Republiková únia zamestnávateľov
Alternatívne názvy	EN Cyber security specialist EN Security analyst EN Security engineer

https://www.sustavapovolani.sk/register-zamestnani/pracovna-oblast/karta-zamestnania/17928-specialista-kybernetickej-bezpecnosti/

Znalostné štandardy v oblasti KB

https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F276ba420-ef09-4a0e-b215-2c2e2f80ad28

Znalostné štandardy v oblasti KB

chief ICT security officer

Download

Professionals > Information and communications technology professionals > Database and network professionals > Database and network professionals not elsewhere classified > chief ICT security officer

Concept overview

Code

2529.1

Description

Chief ICT security officers protect company and employee information against unauthorized access. They also define the Information System security policy, manage security deployment across all Information Systems and ensure the provision of information availability.

Scope note

Includes people performing corporate security functions.

Alternative Labels

chief ICT security officer | chief ICT security officers | chief information security officer | CISO | cybersecurity programme director | head IT security officer | head of information security | head of IT security | ICT security officer | information security administrator | information security manager | information security officer | ISO | IT security officer

Regulatory Aspect

To see if and how this occupation is regulated in EU Member States, EEA countries or Switzerland please consult the Regulated Professions Database of the Commission. Regulated Professions Database:
http://ec.europa.eu/growth/single-market/services/free-movement-professionals/qualifications-recognition_en

chief ICT security officer

Skills & Competences

Essential Skills and Competences

advice on security risk management | communicate with stakeholders | comply with legal regulations | develop information security strategy | educate on data confidentiality | engage with stakeholders | ensure adherence to organisational ICT standards | ensure compliance with legal requirements | ensure cross-department cooperation | ensure information privacy | establish an ICT security prevention plan | establish an Information Security Management System | forecast organisational risks | identify ICT security risks | implement ICT risk management | implement ICT security policies | implement corporate governance | lead disaster recovery exercises | maintain plan for continuity of operations | manage IT security compliances | manage disaster recovery plans | manage system security | monitor developments in field of expertise | monitor technology trends | utilise decision support system

Essential Knowledge

ICT network security risks | ICT process quality models | ICT project management | ICT project management methodologies | ICT safety | ICT security legislation | ICT security standards | assessment of risks and threats | attack vectors | audit techniques | cyber attack counter-measures | cyber security | data protection | decision support systems | ethical hacking principles | ethics | information confidentiality | information security strategy | internal risk management policy

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hodnotiace a validačné kritériá v oblasti KIB

- **Stratégia kybernetickej bezpečnosti** obsahuje najmenej (Príloha č. 1 k vyhláške č. 362/2018 Z. z.:

a) určenie bezpečnostných cieľov z hľadiska kybernetickej bezpečnosti,

b) určenie **spôsobu vyhodnocovania bezpečnostných cieľov**, **kritérií vyhodnocovania dosahovania bezpečnostných cieľov**, spôsobov priebežného hodnotenia ich primeranosti a spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov.

c) Kľúčové ukazovatele výkonnosti (Key Performance Indicators), merateľné ukazovatele sú spojené s určitým procesom, službou, jednotlivcom alebo tímom ľudí. Cez tieto ukazovatele vieme efektívne zmerať výkonnosť rôznych procesov v čase vo vzťahu k stanoveným cieľom.

Hodnotiace a validačné kritériá podľa ISO/IEC 27004

- Meracia entita - objekt, ktorý sledujeme. Je to vec, oblasť alebo aktivita, ku ktorej sa metrika vzťahuje.
- Metriky sú ukazovatele vlastností tejto entity, merateľná veličina.
- ISO/IEC 27004 podporuje organizácie pri nastavení ukazovateľov výkonnosti a efektívnosti informačnej bezpečnosti.

Prvok/Cieľ	Popis
Meracia entita	Oblasť, ktorú sledujeme (napr. autentifikácia používateľov)
Metrika (KPI)	Čo meriame (napr. % používateľov s MFA)
Vzorec	Ako to vypočítame
Frekvencia merania	Ako často meriame (napr. mesačne, štvrťročne)
Zodpovednosť	Kto zodpovedá za zber a vyhodnotenie
Cieľová/prahová hodnota	Kedy považujeme výsledok za úspešný
Zdroje dát	Odkiaľ berieme údaje (napr. logy, záznamy z nástroja SIEM, reporty)
Formát výstupu	Ako budeme výsledok prezentovať (graf, tabuľka, správa)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Preskúmanie politík – príklad definovania postupu

Popis informácie	Význam alebo účel
ID miery	Definuje organizácia
Informačná potreba	Vyhodnotiť, či politiky pre bezpečnosť informácií sú preskúmavané v plánovaných intervaloch alebo keď sa vyskytli významné zmeny.
Metrika	Percento preskúmaných politík
Vzorec/bodovanie	Počet politík bezpečnosti informácii, ktoré boli preskúmané v predošlom roku / Počet politík bezpečnosti informácií zavedených do praxe * 100
Cieľová/prahová hodnota	Zelený: > 80%, Oranžový>=40%, Červený < 40%
Dôkaz implementácie	História dokumentov zmieňujúcich preskúmanie dokumentov alebo zoznamu dokumentov uvádzajúcich dátum posledného preskúmania
Početnosť	Zhromažďovanie: po plánovanom intervale definovanom pre preskúmanie (napríklad ročne alebo po významnej zmene). Podávanie správ: pre každú kolekciu.
Zodpovedné strany	▪ Vlastník aktíva: Vlastník politiky, ktorý schválil zodpovednosť vedenia za vývoj, preskúmanie a hodnotenie politiky. ▪ Osoba zhromažďujúca informácie: Interný audítor ▪ Zákazník merania: Vedúci pracovník bezpečnosti informácií / MKB
Zdroj dát	Plán preskúmania politík, časť história politík bezpečnosti, zoznam dokumentov
Formát podávania správ	Kruhový graf pre bežnú situáciu a čiarový graf pre znázornenie vývoja zhody.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hodnotiace a validačné kritériá v oblasti KIB

- **KPI (Key Performance Indicator)** a **KRI (Key Risk Indicator)** sú dôležité ukazovatele používané pri riadení výkonnosti a rizík v oblasti informačnej bezpečnosti.

- **KPI (Kľúčový ukazovateľ výkonnosti):**

a) KPI merajú efektivitu bezpečnostných opatrení a procesov,

b) pomáhajú organizáciám hodnotiť, či dosahujú svoje bezpečnostné ciele,

c) sú spätne orientované – ukazujú úspešnosť implementovaných bezpečnostných kontrol.

- Príklady KPI v informačnej bezpečnosti:

a) počet úspešne vykonaných bezpečnostných školení zamestnancov,

b) miera splnenia požiadaviek bezpečnostných auditov,

c) počet aplikácií alebo systémov, ktoré prešli penetračným testovaním.

Hodnotiace a validačné kritériá v oblasti KIB

KRI (Kľúčový ukazovateľ rizík)

a) KRI identifikujú potenciálne bezpečnostné riziká.
b) slúžia ako varovné signály pred možnými bezpečnostnými incidentmi.
c) sú dopredu orientované – pomáhajú predchádzať kybernetickým útokom a narušeniam.

- Príklady KRI v informačnej bezpečnosti:

a) počet zistených kritických zraniteľností v systémoch,
b) počet phishingových útokov zachytených bezpečnostnými riešeniami,
c) počet neúspešných pokusov o prihlásenie do citlivých systémov,
d) miera neaktualizovaných softvérových riešení v organizácii.

- Hlavný rozdiel:

a) KPI hodnotia výkonnosť bezpečnostných procesov a opatrení.
b) KRI monitorujú potenciálne bezpečnostné riziká a slúžia ako varovanie pred incidentmi.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti

Právny rámec, organizácia KB a strategické plánovanie (Blok I)

Kurz: Manažér kybernetickej bezpečnosti

prof. Ing. Tomáš Loveček, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Tomas.Lovecek@uniza.sk