Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Správa aktíva a riadenie kybernetických rizík

Riadenie bezpečnosti (Blok I.)
Kurz: Špecialista kybernetickej bezpečnosti

prof. Ing. Tomáš Loveček, PhD.

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

Tomas.Lovecek@uniza.sk

Normatívne požiadavky Vyhlášky NBÚ č.227/2025 Z.z.

- Aktívum sa identifikuje a vedie v evidencii aktív. Evidencia aktív sa skladá z identifikovateľných primárnych aktív a podporných aktív.
- Aktíva sa identifikujú tak, že sú jednoznačne určené hranice jednotlivých sietí a informačných systémov a rozhrania medzi určenými hranicami.
- Evidencia aktív je centralizovane riadená a zodpovedá aktuálnemu stavu.
- Evidencia aktív sa môže skladať z textovej časti, tabuľkovej časti alebo grafickej časti a jej súčasťou je aj označenie bezpečnostných funkcií podporných aktív alebo odkazy na príslušnú časť bezpečnostnej dokumentácie týchto funkcií.
- Evidencia aktív obsahuje najmä identifikáciu a evidenciu
  a) primárnych aktív,
  b) podporných aktív,
  c) vlastníkov aktív,
  d) zodpovedných osôb za identifikáciu a evidenciu aktív.

- Podporné aktívum, ktoré súvisí s viacerými primárnymi aktívami, preberá najvyššiu hodnotu zo súvisiacich aktív.

Normatívne požiadavky zákona o ITVS

- Správca – orgán riadenia (napr. UNIZA) je na úseku obstarávania a implementácie informačných technológií verejnej správy povinný **zabezpečiť riadenie aktív**. *(§15 ods. 1), písm. u))*
- V rámci zabezpečenia riadenia aktív v informačných technológiách verejnej správy správca *(§15 ods. 8))*:

  a) identifikuje a udržiava zoznam svojich aktív,

  b) vyhodnocuje možnosti využitia existujúcich informačných technológií alebo informačných technológií určených na spoločné využitie viacerými orgánmi riadenia a možnosti zdieľania svojich aktív s iným orgánom riadenia (napr. ministerstvo, obec, vyšší územný celok, právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti, atď.),

  c) identifikuje časti aktív, ktorých nedostupnosť alebo znížená kvalita má zásadný vplyv na poskytovanie služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb,

  d) plánuje životný cyklus aktív v súlade so strategickými plánmi rozvoja informačných technológií verejnej správy a s aktuálnymi potrebami ich prevádzky.

Normatívne požiadavky zákona o ITVS

- V rámci zabezpečenia riadenia konfigurácií je správca povinný udržiavať zoznam konfigurácií svojich aktív. *(§15 ods. 9), písm. b))*
- V rámci nastavenia riadenia prevádzky informačných technológií verejnej správy **je správca povinný klasifikovať aktíva** (podľa nedostupnosti alebo zníženej kvality majúc zásadný vplyv na poskytovanie služieb), a to najmä s použitím kritérií potrieb konkrétnych služieb verejnej správy a dodržania povinností (dodržiavať princíp transparentnosti, princíp proporcionality a princíp hospodárnosti a efektívnosti). *(§16 ods. 2), písm. b))*

Normatívne požiadavky zákona o ITVS

- **Kategória II**
- **Identifikácia všetkých významných informačných aktív** v organizácii správcu a **určenie ich vlastníka**, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu.
- **Zaradenie informačných aktív** podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu **do určených klasifikačných stupňov**, pre ktoré sú určené bezpečnostné opatrenia najmenej na ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu.
- Klasifikačné stupne pre informačné aktíva ustanovuje osobitný predpis (Vyhláška NBÚ, ktorou sa ustanovuje obsah bezpečnostných opatrení).

- **Kategória III**
- **Vytvorenie a udržiavanie zoznamu informačných aktív každého organizačného útvaru** organizácie správcu, ktorý je zároveň ich vlastníkom a ktorý určí požiadavky na dôvernosť, dostupnosť a integritu každého informačného aktíva v jeho vlastníctve.

Normatívne požiadavky STN ISO/IEC 27001:2023 (Príloha A.1)

- Musí sa vypracovať a udržiavať inventárny zoznam informácií. (5.9)
- Informácie sa musia klasifikovať podľa potrieb organizácie v oblasti informačnej bezpečnosti na základe požiadaviek na dôvernosť, integritu, dostupnosť a príslušných zainteresovaných strán. (5.12)
- Musí sa vypracovať a implementovať vhodný súbor postupov na označovanie informácií v súlade s klasifikačnou schémou prijatou organizáciou. (5.13)

Inventárny zoznam podľa STN ISO/IEC 27002:2023 (5.9)

- Organizácia by mala **identifikovať** svoje **informácie a iné súvisiace aktíva** a **určiť ich dôležitosť** z hľadiska informačnej bezpečnosti.
- Inventárny zoznam informácií a iných súvisiacich aktív by mal byť presný, aktuálny, konzistentný a zosúladený s ostatnými zoznamami.
- Možnosti zabezpečenia presnosti inventárneho zoznamu informácií a iných súvisiacich aktív zahŕňajú automatické vynútenie aktualizácie inventárneho zoznamu v procese inštalácie, zmeny alebo odstránenia aktíva.
- V prípade potreby by sa do inventárneho zoznamu malo zahrnúť aj umiestnenie aktíva.
- Inventárny zoznam nemusí byť len jeden zoznam informácií a iných súvisiacich aktív.
- Vzhľadom na to, že inventárny zoznam by mali udržiavať príslušné funkcie, možno ho chápať ako súbor dynamických inventárov, ako sú inventáre **informačných aktív, hardvéru, softvéru, virtuálnych strojov (VM), zariadení, personálu, kompetencií, schopností a záznamov.**
- **Každé aktívum by malo byť klasifikované v súlade s klasifikáciou informácií**, ktoré sú s týmto aktívom spojené.

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

Inventárny zoznam podľa STN ISO/IEC 27002:2023 (5.9)

- **Granularita inventárneho zoznamu** informácií a iných súvisiacich aktív **by mala byť na úrovni zodpovedajúcej potrebám organizácie**.
- Niekedy nie je možné zdokumentovať konkrétne prípady aktív v životnom cykle informácií vzhľadom na povahu aktíva. Príkladom krátkodobého aktíva je inštancia virtuálneho stoja, ktorého životný cyklus môže mať krátke trvanie.
- V prípade identifikovaných informácií a iných súvisiacich aktív by sa malo priradiť vlastníctvo aktív jednotlivcovi alebo skupine a mala by sa určiť klasifikácia.
- **Inventárne zoznamy** informácií a iných súvisiacich aktív **podporujú aj riadenie rizík**, audítorské činnosti, riadenie zraniteľností, reakciu na incidenty a riadenie obnovy.
- Ďalšie informácie o správe aktív informačných technológií (IT) nájdete v norme **ISO/IEC 19770-1 Specifies requirements for an IT asset management**. Ďalšie informácie o správe aktív nájdete v norme ISO 55001.

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

Aktívum vs informačné aktívum

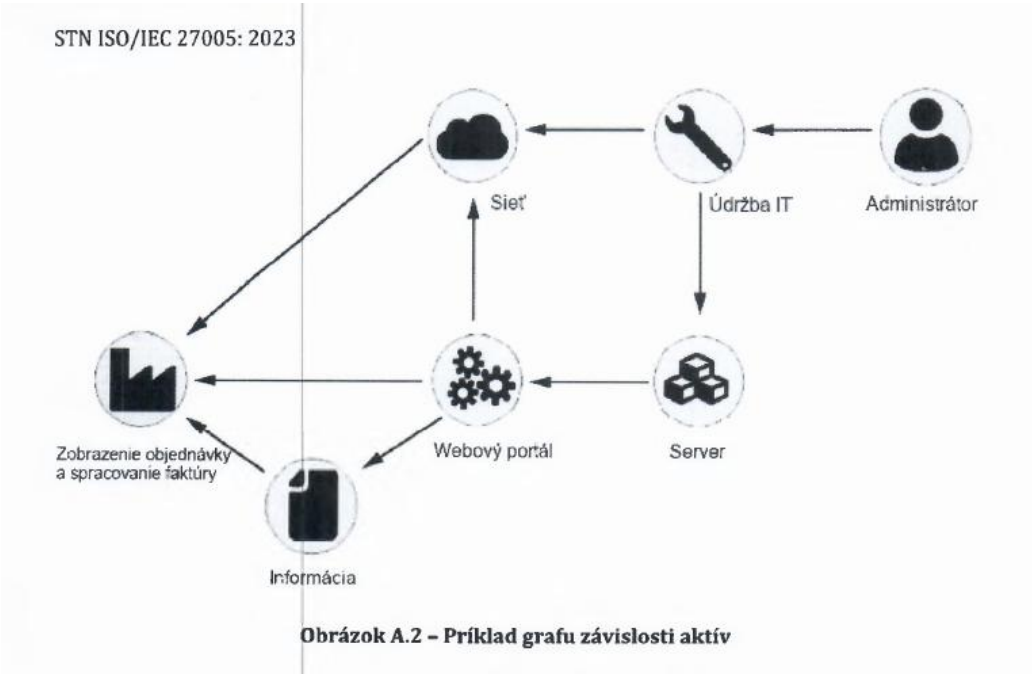
- **Aktívum** - programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaná osoba, dobré meno orgánu riadenia a informácia, dokumentácia, zmluva a iná skutočnosť, ktorú považuje orgán riadenia za citlivú. *(Zákon o ITVS §3 písm. u))*
- Klasifikačné stupne opisujú citlivosť **informácií**, **údajov** alebo ďalších s nimi spojených informačných aktív (ďalej len „**informačné aktíva**“). *(Vyhláška NBÚ č.227/2025 Z.z., Príloha č.2)*

Aktíva podľa Vyhlášky č. 179/2020 Z.z.

- Zoznam aktív obsahuje označenie operačného systému alebo firemného softvéru a jeho aktuálne používanej verzie všetkých týchto komponentov informačných technológií verejnej správy (Príloha 1):
  a) pracovná stanica – stolová,
  b) pracovná stanica – prenosná,
  c) aplikačný softvér,
  d) kancelársky softvér,
  e) internetový prehliadač,
  f) antivírusový softvér,
  g) komunikačný softvér,
  h) ďalší využívaný komerčný softvér,
  i) všetky druhy serverov,
  j) virtualizačné prostredie,
  k) databázové prostredie,
  l) komerčný podnikový softvér,
  m) sieťový firewall,
  n) sieťový router,
  o) sieťový prepínač,
  p) komunikačné prostredie,
  q) zálohovacie prostredie,
  r) mobilné zariadenia,
  s) dátové úložiská,
  t) ostatné zariadenia alebo sieťové prvky schopné komunikovať so zvyškom ekosystému informačných technológií verejnej správy,
  u) prenosné zariadenia.

Aktívum vs informačné aktívum

- Aktíva možno rozdeliť do divoch kategórií (STN ISO/IEC 27005:2023):
  a) **primárne/prevádzkové aktíva** - **informácie** alebo **procesy**, ktoré majú pre organizáciu hodnotu;
  b) **podporné aktíva** - **komponenty informačného systému**, na ktorých je závislé jedno alebo viacero prevádzkových aktív.



Obrázok A.2 – Príklad grafu závislosti aktív

Aktívum vs informačné aktívum

- **Aktívum** (asset) je čokoľvek, čo má pre organizáciu hodnotu. V kontexte informačnej bezpečnosti možno rozlišovať dva druhy aktív (STN ISO/IEC 27002:2023):

  a) **Primárne (prevádzkové) aktíva**:
     i. informácie;
     ii. obchodné procesy a činnosti;

  b) **podporné aktíva** (na ktoré sa primárne aktíva spoliehajú) všetkých typov, napríklad:
     i. hardvér;
     ii. softvér;
     iii. sieť;
     iv. personál (ako riadiaci orgán, vrcholový manažment, zamestnanci, dočasní zamestnanci, dodávatelia a dobrovoľníci);
     v. lokalita;
     vi. štruktúra organizácie.

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

Aktívum vs informačné aktívum

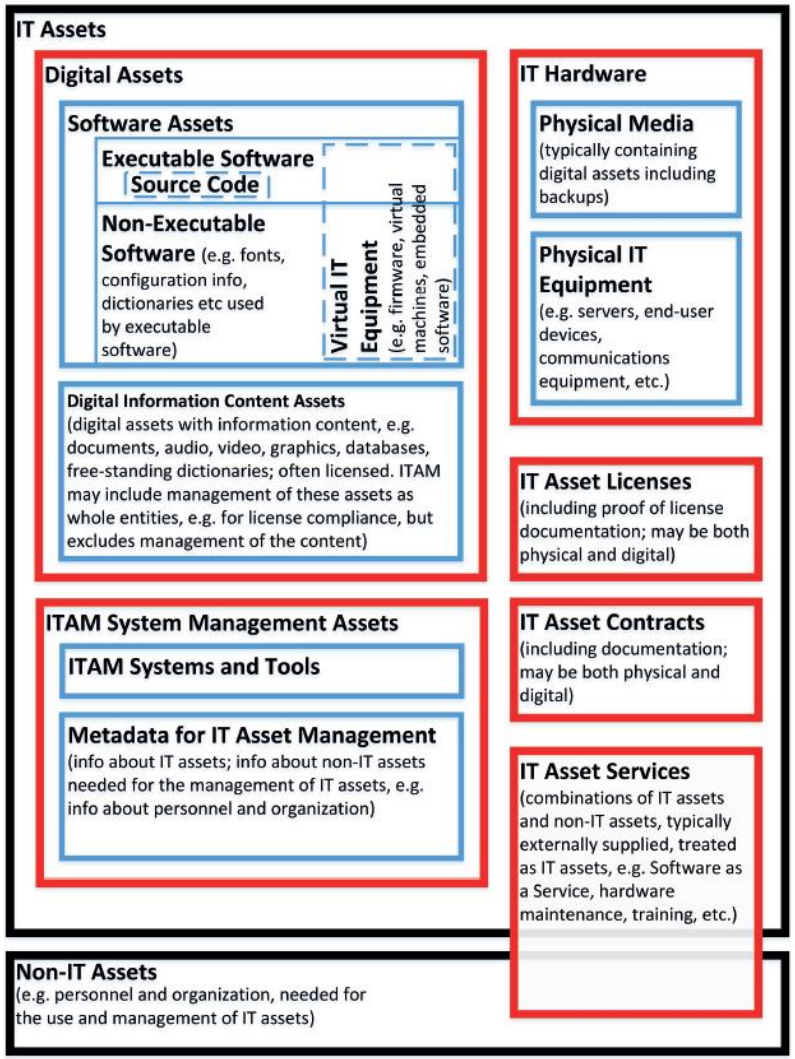
- **Informačné aktívum** (information asset) znalosti alebo údaje, ktoré majú hodnotu pre jednotlivca alebo organizáciu. (ISO/IEC 27032)
- **Fyzické aktívum** (physical asset) sú aktíva, ktoré majú hmotnú alebo materiálnu existenciu. (ISO/IEC 27032)
- **Virtuálne aktívum** (virtual asset) reprezentácia aktíva v kyberpriestore. (ISO/IEC 27032) (napr. online identita)

- **Proces** (process) je súbor aktivít majúcich vzájomný vzťah alebo vzájomne na seba pôsobiacich a premieňajúcich vstupy na výstupy. (STN ISO/IEC 27000:2023)

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

Aktívum vs informačné aktívum

ISO/IEC 19770-1:2017
Správa aktív IT – Systémy správy aktív IT - Požiadavky



Informačný systém vs sieť

- **Informačný systém** (information system) súbor aplikácií, služieb, aktív informačných technológií alebo iných komponentov na spracovanie informácií. (STN ISO/IEC 27000)
- **Informačný systémom** je funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov. (Zákon o KB).
- **Informačný systém** je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov. (Zákon o ITVS)
- **Informačným systémom verejnej správy** je informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby. (Zákon o ITVS)
- **Informačný systém** je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. (GDPR).

Normatívne požiadavky Zákona o KB

- Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby v závislosti od vykonanej **analýzy rizík** prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20. *(§19 ods.1))*

- Prevádzkovateľ základnej služby je povinný pri výkone činnosti, ... prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností ...; pri uzatvorení zmluvy sa vykonáva **analýza rizík**. *(§19 ods.2)*).

- Bezpečnostné opatrenia sú realizované na základe vykonanej **analýzy rizík** a s prihliadnutím na bezpečnostné metodiky a politiky úradu... *(§20 ods.1)*).

- Bezpečnostné opatrenia sa prijímajú aspoň pre:
  c) správu aktív a **riadenie kybernetických hrozieb a rizík**,... *(§20 ods.2)*).
- Súčasťou analýzy rizík je aj **analýza politického rizika** tretej strany... *(§20 ods.5)*).

Normatívne požiadavky Zákona o KB

- Prevádzkovateľ základnej služby je ďalej povinný **analyzovať závislosti svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb** s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu. *(§19 ods.6), písm. f)*

- Bezpečnostné opatrenia sa prijímajú aspoň pre **správu aktív** a riadenie kybernetických hrozieb a rizík. *(§20 ods.2), písm. c)*

Normatívne požiadavky zákona o ITVS

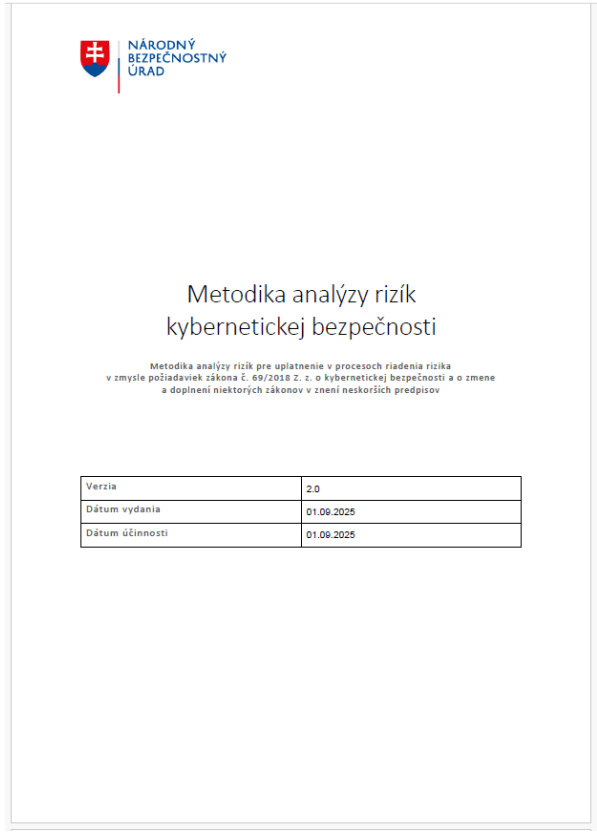
- Plánovanie a organizácia informačných technológií verejnej správy
  h) zabezpečiť **riadenie rizík**, (§14 ods. 1))

- Procesnými podmienkami sa rozumie najmä určenie postupov riadenia informačných technológií verejnej správy a kontrola dodržiavania všeobecne záväzných právnych predpisov v tejto oblasti, ako aj **riadenie kvality, rizík a bezpečnosti** ITVS. .... (§14 ods. 5))

- V rámci zabezpečenia riadenia rizík je správca povinný vydať **vnútorný predpis pre riadenie rizík**. (§14 ods. 8))

- zabezpečí a zdokumentuje identifikovanie aktív v informačných technológiách verejnej správy a **riadenie rizík**, najmä vo forme bezpečnostnej dokumentácie vrátane bezpečnostného projektu ... (§19 ods. 1), písm. c))

Štandardy



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Metodika analýzy rizík kybernetickej bezpečnosti

Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Verzia	2.0
Dátum vydania	01.09.2025
Dátum účinnosti	01.09.2025

Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.1 | kyberbezpecnost@mirri.gov.sk | december 2022

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Metodika analýzy rizík a analýzy dopadov

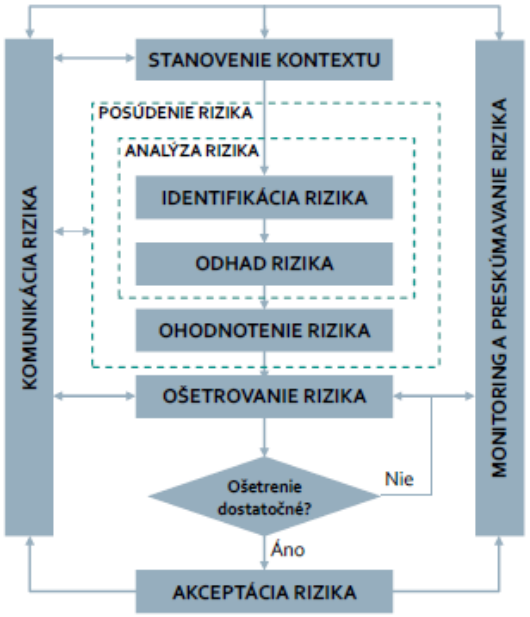
1

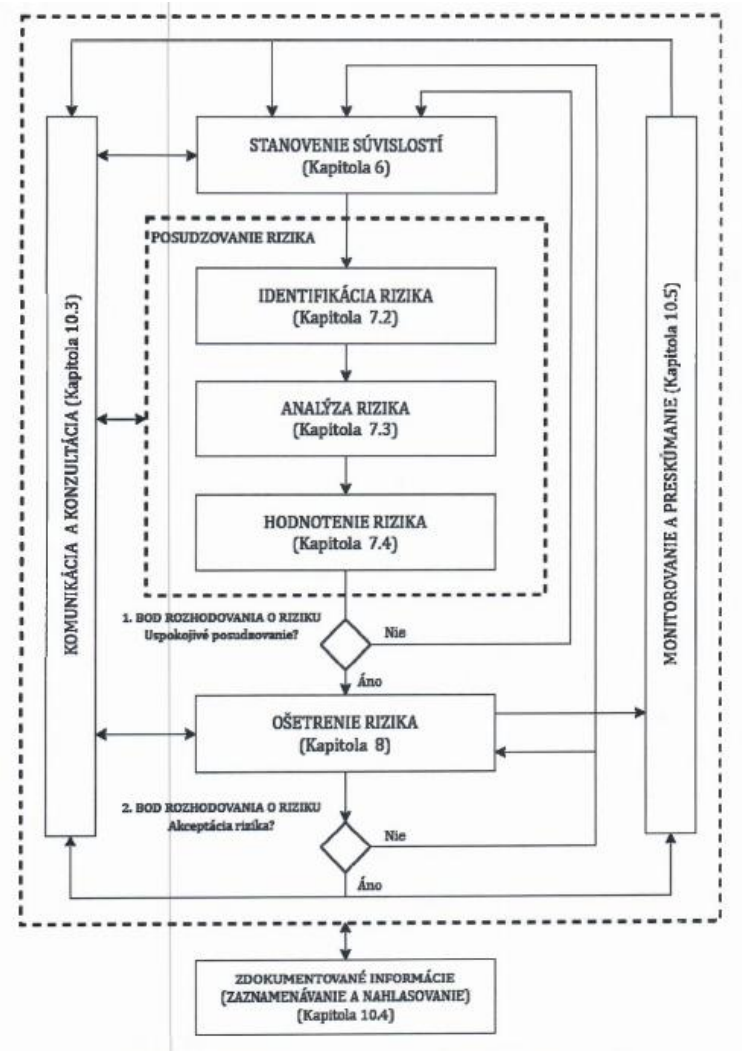
Štandardy

- Metodika sa opiera najmä o nasledovné právne predpisy a technické normy:
  a) **Zákon č. 69/2018 Z.z.** o kybernetickej bezpečnosti
  b) **Vyhláška NBÚ č. 227/2018 Z.z.** o bezpečnostných opatreniach
  c) **ISO/IEC 27001:2022** Information security, cybersecurity and privacy protection — Information security management systems — Requirements
  d) **ISO/IEC 27002:2022** Information security, cybersecurity and privacy protection — Information security controls
  e) **ISO/IEC 27005:2022** Information security, cybersecurity and privacy protection — Guidance on managing information security risks
  f) **ISO 31000:2018** - Risk management — Guidelines
  g) **NIST Special Publication 800-39** Managing Information Security Risk
  h) **NIST Special Publication 800-30** Rev. 1 Guide for Conducting Risk Assessments

Štandardy

Všeobecná schéma procesu riadenia rizík informačnej bezpečnosti podľa ISO/IEC 27005:



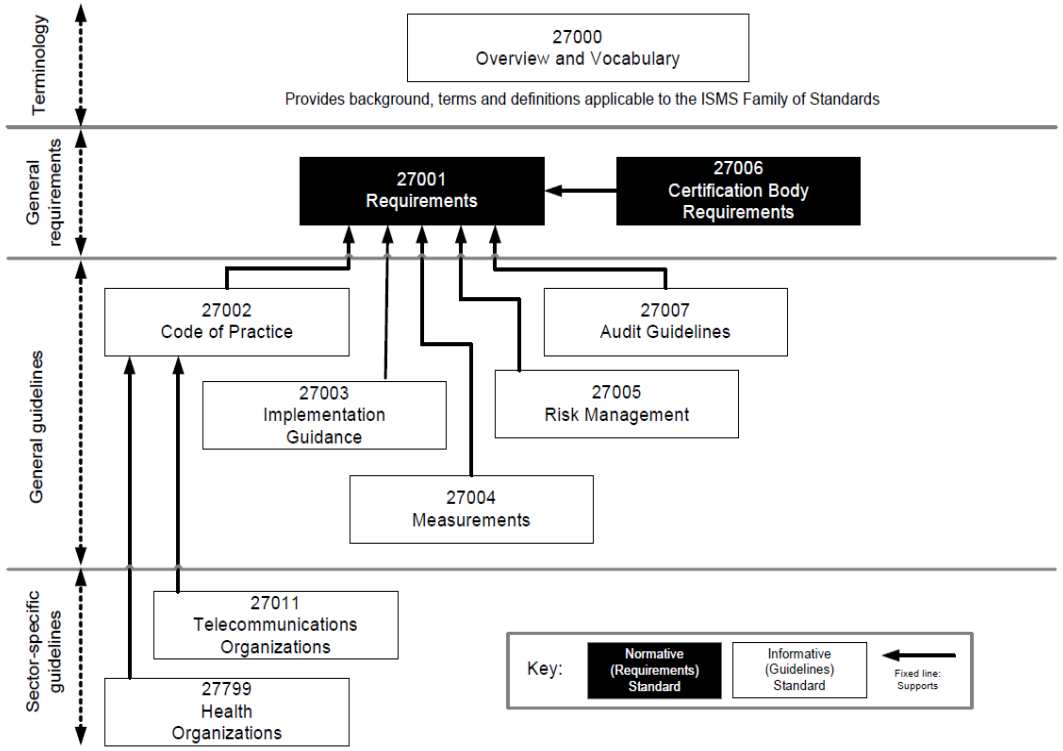


Systém manažérstva informačnej bezpečnosti (ISO/IEC 27001)

- SMIB (**ISMS: Information Security Management System**) pozostáva z politík, postupov, smerníc a príslušných zdrojov a činností, ktoré organizácia riadi, aby zabezpečila ochranu informačných aktív.

- Je založený na **posudzovaní rizík** a na úrovniach prijatia rizík organizácie, ktoré boli navrhnuté pre efektívne **ošetrenie rizík** a pre ich riadenie.

Rad technických noriem ISMS



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

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

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Systémy manažérstva informačnej bezpečnosti – požiadavky (ISO/IEC 27001)

- 6 Plánovanie
  - 6.1 Opatrenia na zvládnutie rizík a príležitostí
    - 6.1.1 Všeobecne
    - **6.1.2 Posúdenie rizík informačnej bezpečnosti**
    - **6.1.3 Ošetrenie rizík informačnej bezpečnosti**
  - 6.2 Ciele informačnej, bezpečnosti a plánovanie ich splnenia
  - 6.3 Plánovanie zmien
- 7 Podpora
  - 7.1 Zdroje
  - 7.2 Kompetentnosť
  - 7.3 Povedomie
  - 7.4 Komunikácia
  - 7.5 Zdokumentované informácie

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

- Štvrté vydanie ruší a nahrádza tretie vydanie (ISO/IEC 27005: 2018), ktoré bolo technicky revidované.
- Hlavné zmeny sú tieto:
  a) celý text usmernenia bol zosúladený s normami ISO/IEC 27001: 2022 a ISO 31000: 2018;
  b) terminológia bola zosúladená s terminológiou v norme ISO 31000: 2018;
  c) štruktúra kapitol bola prispôsobená štruktúre normy ISO/IEC 27001: 2022;
  d) boli zavedené koncepty rizikových scenárov;
  e) prístup založený na udalostiach je v kontraste s prístupom k identifikácii rizík založeným na aktívach;
  f) obsah príloh bol revidovaný a reštrukturalizovaný do jednej prílohy.

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

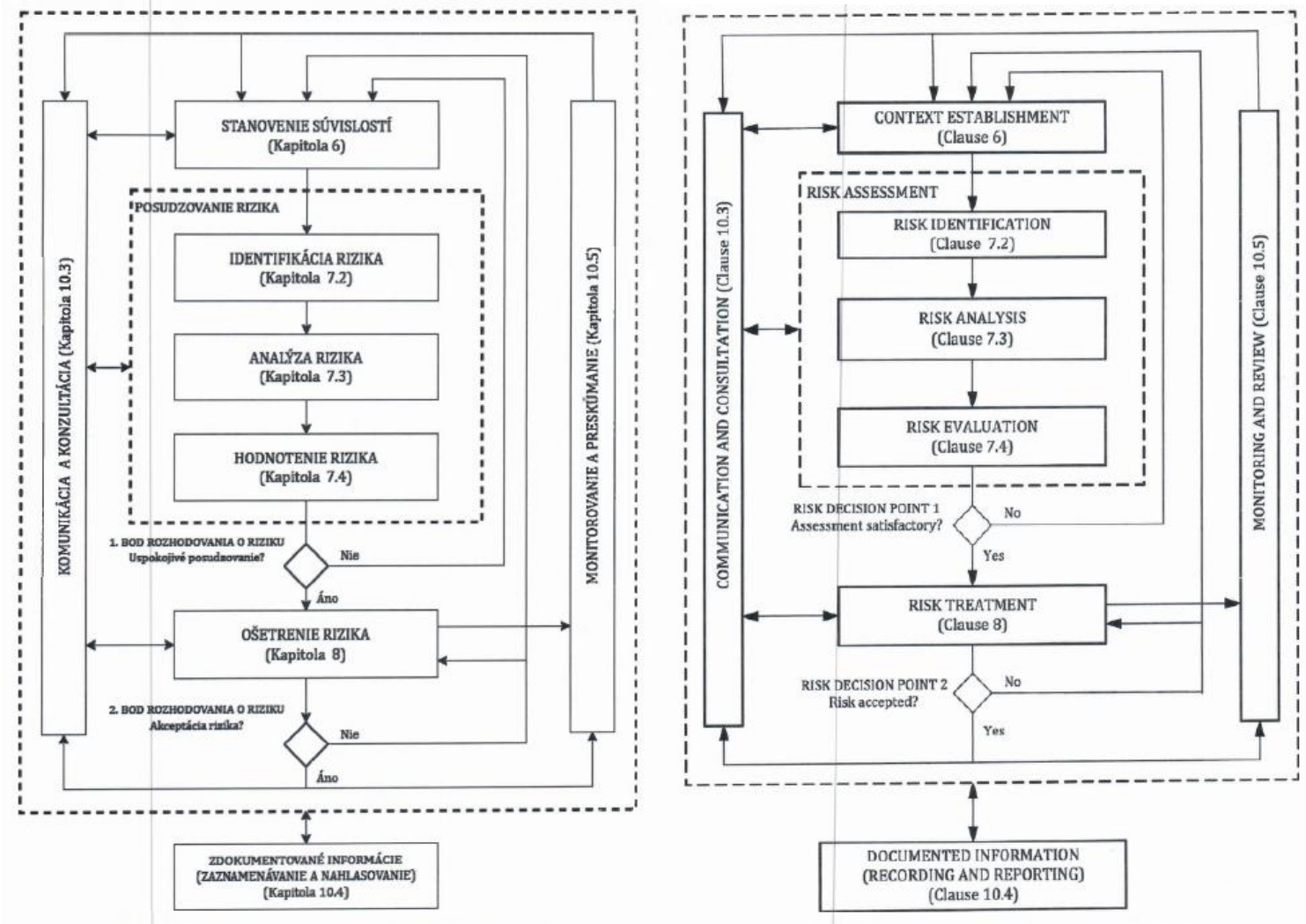
Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

- Norma je štruktúrovaná nasledovne:
  a) Kapitola 5: Riadenie rizík informačnej bezpečnosti;
  b) Kapitola 6: Stanovenie súvislostí;
  c) Kapitola 7: Proces posúdenia rizík informačnej bezpečnosti;
  d) Kapitola 8: Proces ošetrenia rizík informačnej bezpečnosti;
  e) Kapitola 9: Prevádzka;
  f) Kapitola 10: Využívanie súvisiacich procesov ISMS.

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

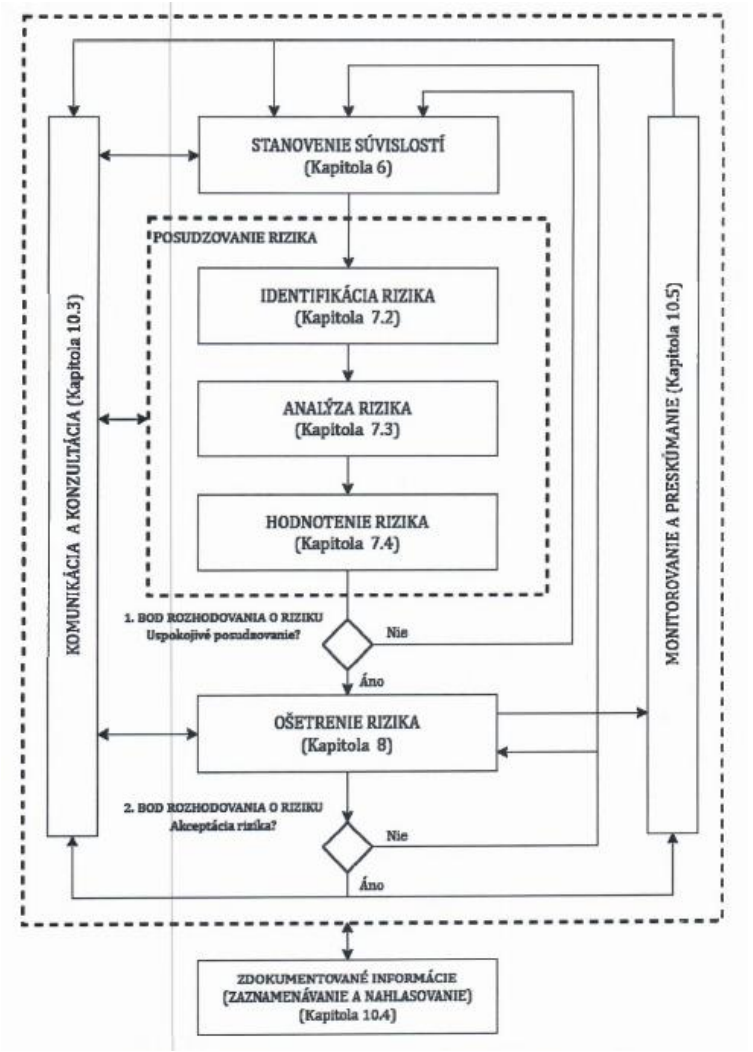
5 Riadenie rizík informačnej bezpečnosti

5.1 Proces riadenia rizík informačnej bezpečnosti



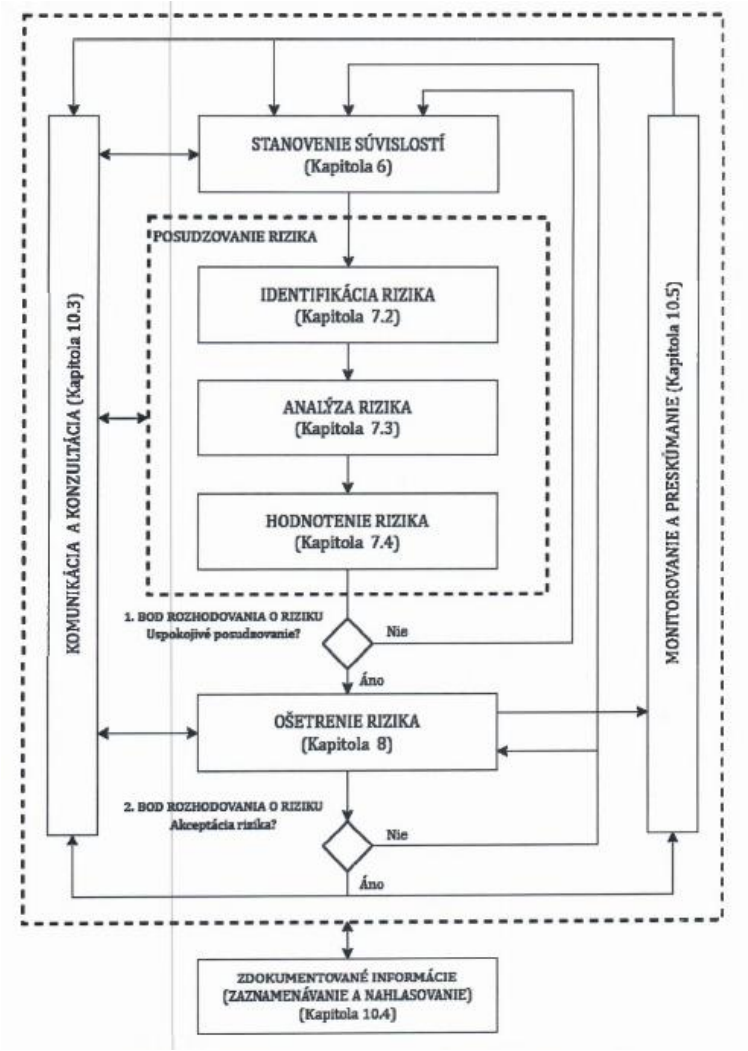
Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

- **Riziko** potenciál straty alebo narušenia v dôsledku kybernetického bezpečnostného incidentu vyjadrený ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu kybernetického bezpečnostného incidentu. (Zákon o KB)
- Riziká informačnej bezpečnosti môžu byť spojené s možnosťou, že hrozby zneužijú zraniteľnosti informačného aktíva alebo skupiny informačných aktív a spôsobia tak organizácii škodu. (ISO/IEC 27005).



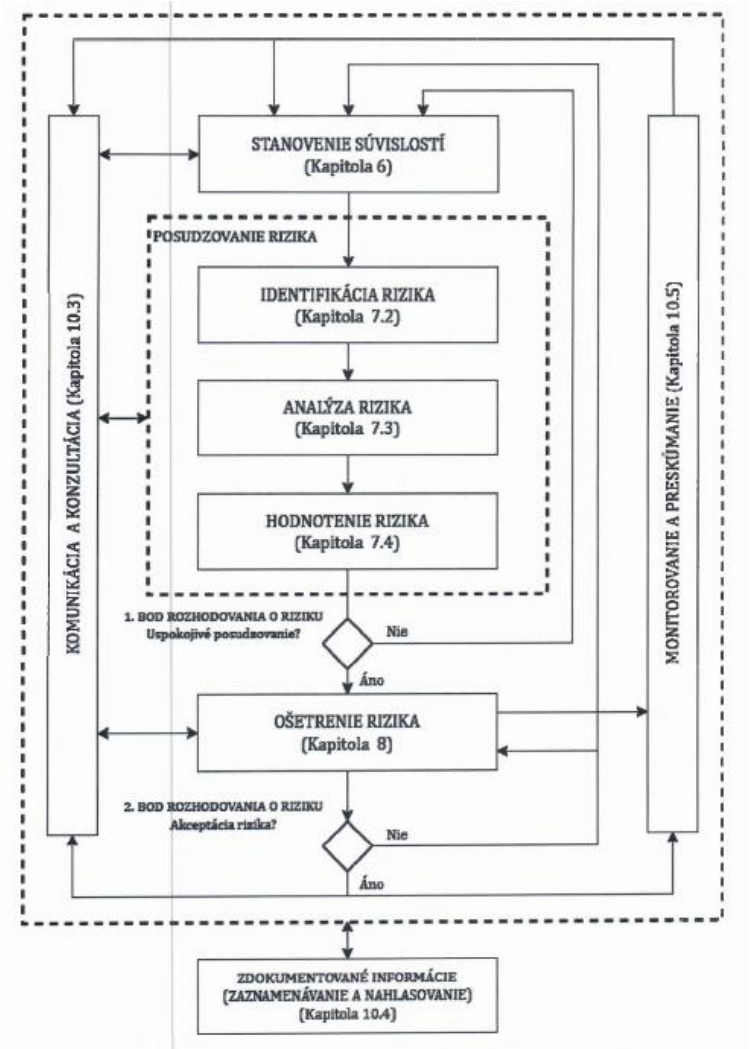
Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

- **Úroveň/stupeň rizika** (level of risk) je vyjadrená ako kombinácia následkov a ich pravdepodobnosti. (ISO 31073)
- **Scenár rizika** (risk scenario) postupnosť alebo kombinácia udalostí vedúca od počiatočnej príčiny k nežiaducemu následku. (ISO/IEC 27005)



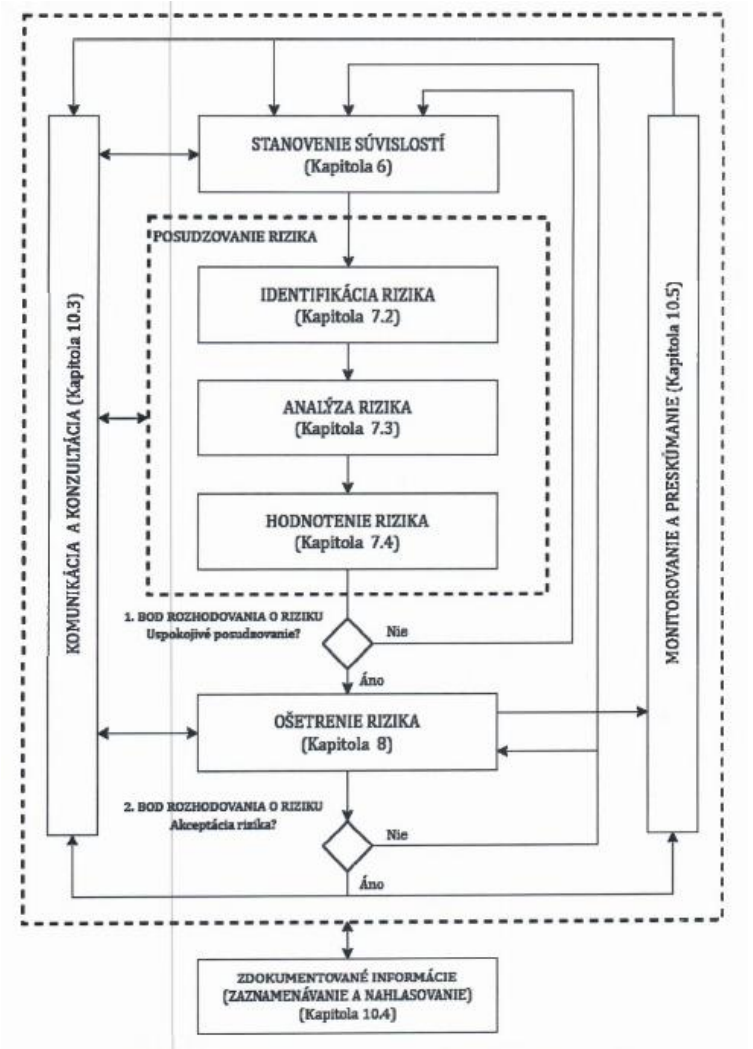
Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

- **Posúdenie rizika** (risk assessment) celkový proces identifikácie rizika, analýzy rizika a hodnotenia rizika. (ISO 31073)
- **Identifikácia rizika** (risk identification) proces vyhľadávania, rozpoznávania a opisu rizík. Identifikácia rizík zahŕňa identifikáciu zdrojov rizík, udalostí, ich príčin a potenciálnych následkov. (ISO 31073)
- **Analýza rizík** (risk analysis) proces na pochopenie povahy rizika a určenie úrovne rizika. Analýza rizika poskytuje základ pre hodnotenie rizík a rozhodnutia o ošetrení rizík .Analýza rizika zahŕňa odhad rizika. (ISO 31073)
- **Hodnotenie rizík** (risk evaluation) proces porovnávania výsledkov analýzy rizík s kritériami rizika s cieľom určiť, či je riziko a/alebo jeho významnosť. Hodnotenie rizika pomáha pri rozhodovaní o ošetrení rizík. (ISO 31073)
- **Ošetrenie rizík** (risk treatment) proces na úpravu rizika. (ISO 31073)



Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Usmernenie k riadeniu rizík informačnej bezpečnosti. (ISO/IEC 27005)

- **Akceptovanie rizika** (risk aceptance) informované rozhodnutie podstúpiť určité riziko. K akceptácii rizika môže dôjsť bez ošetrenia rizika alebo počas procesu ošetrenia rizika. Prijaté riziká podliehajú monitorovaniu a preskúmaniu. (ISO 31073)
- **Zvyškové riziko** (residual risk) je riziko zostávajúce po ošetrení rizika. Zvyškové riziko môže obsahovať neidentifikované riziko. Zvyškové riziká môžu obsahovať aj ponechané riziko. (ISO 31073)
- **Vlastník rizika** (risk owner) osoba alebo subjekt so zodpovednosťou a právomocou riadiť riziko. (ISO/IEC 27000)
- **Ochota podstupovať riziko** (risk appetite) množstvo a typ rizika, ktoré je organizácia ochotná podstúpiť alebo si ponechať. (ISO/IEC 27005)



5 Riadenie rizík informačnej bezpečnosti
5.1 Proces riadenia rizík informačnej bezpečnosti

- Proces riadenia rizík informačnej bezpečnosti môže byť iteratívny pre činnosti posúdenia rizík a/alebo ošetrenia rizík.
- Iteratívny prístup poskytuje dobrú rovnováhu medzi minimalizáciou času a úsilia vynaloženého na identifikáciu opatrení a zároveň zabezpečuje, aby boli riziká primerane posúdené.
- Ak sú informácie nedostatočné, mala by sa vykonať ďalšia iterácia posúdenia rizík. To môže zahŕňať zmenu súvislostí posúdenia rizík (napr. revidovaný rozsah), zapojenie odborníkov z príslušnej oblasti alebo iné spôsoby zhromažďovania informácií potrebných na umožnenie úpravy rizík na prijateľnú úroveň („bod rozhodovania o riziku 1" na obrázku).
- Je možné, že ošetrenie rizík nevedie okamžite k prijateľnej úrovni zvyškových rizík. V tejto situácii sa môže vykonať ďalší pokus o nájdenie ďalšieho ošetrenia rizík alebo môže dôjsť k ďalšej iterácii posúdenia rizík, a to buď ako celku, alebo po častiach. („bod rozhodovania o riziku 2" na obrázku).

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

6 Stanovenie súvislostí
6.1 Organizačné aspekty (ISO/IEC 27001: 2022, 4.1.)

- Organizácia nemusí byť nevyhnutne spoločnosť, iný orgán spoločnosti alebo právnická osoba, môže to byť aj podmnožina právnickej osoby (napr. oddelenie IT spoločnosti a v súvislostiach ISMS sa môže považovať za „organizáciu".
- Je dôležité pochopiť, že ochota podstupovať riziko, definovaná ako miera rizika, ktorú je organizácia ochotná podstúpiť alebo akceptovať, sa môže v jednotlivých organizáciách značne líšiť.

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

6 Stanovenie súvislostí
6.2 Identifikácia základných požiadaviek zainteresovaných strán (ISO/IEC 27001: 2022, 4.2.)

- Mali by sa identifikovať **základné požiadavky** príslušných zainteresovaných strán, ako aj stav plnenia týchto požiadaviek. To zahŕňa identifikáciu všetkých referenčných dokumentov, ktoré definujú bezpečnostné pravidlá a opatrenia, a ktoré sa uplatňujú v rámci rozsahu posúdenia rizík informačnej bezpečnosti.
- Tieto referenčné dokumenty môžu okrem iného zahŕňať:
  a) ISO/IEC 27001: 2022;
  b) ďalšie normy, ktoré sa vzťahujú na ISMS;
  c) ďalšie normy, ktoré sa vzťahujú na konkrétne odvetvie (napr. finančné, zdravotnícke);
  d) špecifické medzinárodné a/alebo vnútroštátne predpisy;
  e) vnútorné bezpečnostné predpisy organizácie;
  f) bezpečnostné pravidlá a opatrenia zo zmlúv alebo dohôd;
  g) bezpečnostné opatrenia zavedené na základe predchádzajúcich činností súvisiacich s ošetrením rizík.

6 Stanovenie súvislostí
6.3 Uplatňovanie posúdenia rizík (ISO/IEC 27001: 2022, 4.2.)

- Organizácie môžu vykonávať posúdenia rizík v rámci mnohých rôznych procesov, ako je projektové riadenie, riadenie zraniteľností, riadenie incidentov, riadenie problémov alebo dokonca na improvizovanom základe pre danú identifikovanú špecifickú tému.
- Bez ohľadu na to, ako sa posúdenia rizík vykonávajú, mali by spoločne pokrývať všetky otázky relevantné pre organizáciu v rámci rozsahu ISMS.

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.1 Všeobecne

- Norma ISO/IEC 27001:2022,6, špecifikuje požiadavky na organizácie aby definovali svoje kritériá rizík, (t. j. referenčné podmienky, podľa ktorých hodnotia významnosť rizík, ktoré identifikujú, a prijímajú rozhodnutia týkajúce sa rizík):

  a) kritériá akceptácie rizík;

  b) kritériá na vykonanie posúdenia rizík informačnej bezpečnosti.

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.2 Kritériá akceptácie rizík (ISO/IEC 27001: 2022, 6.1.2 a) 1).

- Pri hodnotení rizík by sa na určenie toho, či je riziko akceptovateľné alebo nie, mali použiť kritériá akceptácie rizík.
- Pri ošetrení rizík sa kritériá akceptovateľnosti rizík môžu použiť na určenie, či je navrhované ošetrenie rizík dostatočné na dosiahnutie prijateľnej úrovne rizík, alebo či je potrebné ďalšie ošetrenie rizík.
- Počas vývoja by sa mali zvážiť nasledujúce skutočnosti:

  a) súlad medzi kritériami akceptovateľnosti rizík informačnej bezpečnosti a všeobecnými kritériami akceptovateľnosti rizík organizácie;

  b) určenie úrovne riadenia s delegovanou právomocou prijímať rozhodnutia o akceptácii rizík;

  c) kritériá akceptácie rizík môžu obsahovať viacero prahových hodnôt a právomoc na akceptáciu môže byť pridelená rôznym úrovniam riadenia;

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.2 Kritériá akceptácie rizík (ISO/IEC 27001: 2022, 6.1.2 a) 1).

d) jednoduché kritérium akceptácie (áno/nie) v praxi nie vždy postačuje;

e) kritériá akceptácie rizík môžu byť založené len na pravdepodobnosti a následkoch alebo môžu byť rozšírené tak, aby zohľadňovali aj pomer nákladov a výnosov medzi potenciálnymi stratami a nákladmi na opatrenia;

f) na rôzne triedy rizík sa môžu vzťahovať rôzne kritériá akceptácie rizík (napr. riziká, ktoré môžu viesť k nesúladu s predpismi alebo zákonmi, sa nie vždy ponechávajú, zatiaľ čo akceptácia rizík môže byť povolená, ak je akceptácia výsledkom zmluvnej požiadavky);

g) kritériá akceptovateľnosti rizík by mali byť definované na základe ochoty podstupovať riziko, ktorá udáva výšku a typ rizika, ktoré je organizácia ochotná podstúpiť alebo si ponechať;

h) kritériá akceptácie rizík sa môžu líšiť v závislosti od toho, ako dlho sa očakáva, že budú riziká existovať (napr. riziká môžu byť spojené s dočasnou alebo krátkodobou činnosťou).

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.2 Kritériá akceptácie rizík (ISO/IEC 27001: 2022, 6.1.2 a) 1).

Úroveň rizika	Hodnotenie rizika	Popis
Nízka (zelená)	Akceptovateľné tak, ako je	Riziko možno akceptovať bez ďalších opatrení.
Stredná (oranžová)	Znesiteľné pod kontrolou	Mali by sa vykonať následné opatrenia z hľadiska riadenia rizík a mali by sa stanoviť opatrenia v rámci trvalého zlepšovania v strednodobom a dlhodobom horizonte.
Vysoká (červená)	Neakceptovateľné	Opatrenia na zníženie rizika by sa mali bezpodmienečne prijať v krátkodobom horizonte. V opačnom prípade by sa mala celá činnosť alebo jej časť zamietnuť.

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.1 Všeobecne (ISO/IEC 27001: 2022, 6.1.2 a) 2).

- Kritériá hodnotenia rizík špecifikujú, ako sa určuje významnosť rizika z hľadiska jeho následkov, pravdepodobnosti a úrovne rizika.
- Kritériá posúdenia rizík alebo formálny základ na ich definovanie by mali byť štandardizované v rámci organizácie pre všetky typy posúdenia rizík, pretože to môže uľahčiť komunikáciu, porovnávanie a agregáciu rizík spojených s viacerými oblasťami podnikania.

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.2 Kritéria následkov

- Kritériá následkov by mali byť vypracované a špecifikované z hľadiska rozsahu škody alebo straty, alebo poškodenia organizácie alebo jednotlivca v následku straty dôvernosti, integrity a dostupnosti informácií.
- Pri definovaní kritérií následkov by sa mali zohľadniť najmä tieto skutočnosti:

a) straty na životoch alebo poškodenie jednotlivcov alebo skupín;

b) strata slobody, dôstojnosti alebo práva na súkromie;

c) strata personálu a intelektuálneho kapitálu (zručností a odborných znalostí);

d) narušenie vnútorných operácií alebo operácií tretích strán (napr. poškodenie prevádzkovej funkcie alebo procesu);

e) účinky na plány a termíny;

f) strata prevádzkovej a finančnej hodnoty;

g) strata prevádzkových výhod alebo podielu na trhu;

h) poškodenie dôvery verejnosti alebo poškodenie dobrého mena;

i) porušenie právnych, regulačných alebo zákonných požiadaviek;

j) porušenie zmlúv alebo úrovne služieb;

k) nepriaznivý vplyv na zainteresované strany...

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.2 Kritéria následkov

Následky	Popis
5 – Katastrofické	**Odvetvové alebo regulačné následky mimo organizácie** Podstatne ovplyvnený sektorový ekosystém (ekosystémy) s následkami, ktoré môžu byť dlhodobé. A/alebo: ťažkosti pre štát, či dokonca neschopnosť zabezpečiť regulačnú funkciu alebo jednu z jeho misií zásadného významu. A/alebo: kritické následky na bezpečnosť osôb a majetku (zdravotná kríza, veľké znečistenie životného prostredia, zničenie základných infraštruktúr atď.)
4 – Kritické	**Havarijné následky pre organizáciu** Neschopnosť organizácie zabezpečiť celú svoju činnosť alebo jej časť s možnými vážnymi následkami na bezpečnosť osôb a majetku. Organizácia s najväčšou pravdepodobnosťou situáciu neprekoná (je ohrozené jej prežitie), odvetvia činnosti alebo štátne odvetvia, v ktorých pôsobí, budú pravdepodobne ovplyvnené mierne, bez dlhodobých následkov.
3 – Vážne	**Podstatné následky pre organizáciu** Vysoké zhoršenie výkonu činnosti s možnými závažnými následkami na bezpečnosť osôb a majetku. Organizácia prekoná situáciu s vážnymi ťažkosťami (prevádzka vo vysoko degradovanom režime), bez dopadu na sektor alebo štát.
2 – Významné	**Významné, ale obmedzené následky pre organizáciu** Zhoršenie výkonu činnosti bez následkov na bezpečnosť osôb a majetku. Organizácia situáciu prekoná napriek niekoľkým ťažkostiam (prevádzka v zhoršenom režime).
1 – Drobné	**Zanedbateľné následky pre organizáciu** Žiadne následky na prevádzku alebo výkon činnosti alebo na bezpečnosť osôb a majetku. Organizácia situáciu prekoná bez väčších ťažkostí (budú využité rezervy).

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.2 Kritéria následkov

Následok (strata)	Logaritmické vyjadrenie	Hodnota stupnice
1 000 000 £	(10^6)	6
100 000 £	(10^5)	5
10 000 £	(10^4)	4
1 000 £	(10^3)	3
100 £	(10^2)	2
Menej ako 100 £	(10^1)	1

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.3 Kritéria pravdepodobnosti

- Určenie kritérií pravdepodobnosti závisí od aspektov, ako sú/je:
  a) náhodné alebo prírodné udalosti;
  b) stupeň vystavenia príslušných informácií alebo aktív súvisiacich s informáciami o hrozbe;
  c) stupeň, v akom je zraniteľnosť organizácie zneužitá;
  d) zlyhanie technológie;
  e) ľudské činy alebo opomenutia.
- Pravdepodobnosť sa dá vyjadriť pravdepodobnostne (šanca, že sa udalosť vyskytne v danom časovom rámci) alebo frekvenčné (pomyselný priemerný počet výskytov v danom časovom rámci).

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.3 Kritéria pravdepodobnosti

Pravdepodobnosť	Popis
5 – Takmer isté	Zdroj rizika s najväčšou pravdepodobnosťou dosiahne svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť rizikového scenára je veľmi vysoká.
4 – Veľmi pravdepodobné	Zdroj rizika pravdepodobne dosiahne svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť rizikového scenára je vysoká.
3 – Pravdepodobné	Zdroj rizika je schopný dosiahnuť svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť rizikového scenára je značná.
2 – Skôr nepravdepodobné	Zdroj rizika má relatívne malú šancu dosiahnuť svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť rizikového scenára je nízka.
1 – Nepravdepodobné	Zdroj rizika má veľmi malú šancu dosiahnuť svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť výskytu rizikového scenára je veľmi nízka.

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.3 Kritéria pravdepodobnosti

Približná priemerná frekvencia	Logaritmické vyjadrenie	Hodnota stupnice
Každú hodinu	(cca 10^5)	5
Každých 8 hodín	(cca 10^4)	4
Dvakrát týždenne	(cca 10^3)	3
Raz mesačne	(cca 10^3)	2
Raz ročne	(10^1)	1
Raz za desaťročie	(10^0)	0

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.4 Kritériá na určenie úrovne rizika

- Účelom stupníc pre úroveň rizika je pomôcť vlastníkom rizík pri rozhodovaní o zachovaní alebo inom ošetrení rizík a určiť ich prioritu pre ošetrenie rizík.
- Posúdená úroveň konkrétneho rizika by mala organizácii pomôcť určiť naliehavosť riešenia tohto rizika.
- V závislosti od situácie sa odporúča zvážiť **inherentnú úroveň rizika** (bez zohľadnenia akýchkoľvek opatrení) alebo **súčasnú úroveň rizika** (s prihliadnutím na účinnosť všetkých, už zavedených, opatrení).

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.4 Kritériá na určenie úrovne rizika

- Kritériá úrovne rizika môžu byť kvalitatívne (napr. veľmi vysoké, vysoké, stredné, nízke) alebo kvantitatívne (napr. vyjadrené očakávanou hodnotou peňažnej straty, straty na životoch alebo trhového podielu za určité obdobie).
- Ak sa používa kvalitatívny prístup, úrovne akejkoľvek kvalitatívnej stupnice by mali byť jednoznačné, jej prírastky by mali byť jasne definované, kvalitatívne opisy pre každú úroveň by mali byť vyjadrené objektívnym jazykom a úrovne by sa nemali prekrývať.
- Ak sa používajú rôzne stupnice (napr. na riešenie rizík v rôznych oblastiach podnikania), mala by existovať ekvivalencia, ktorá umožní porovnateľné výsledky.

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.4 Kritériá na určenie úrovne rizika

Pravdepodobnosť	Následok				
	Katastrofické	Kritické	Vážne	Významné	Drobné
Takmer isté	Veľmi vysoké	Veľmi vysoké	Vysoké	Vysoké	Stredné
Veľmi pravdepodobné	Veľmi vysoké	Vysoké	Vysoké	Stredné	Nízke
Pravdepodobné	Vysoké	Vysoké	Stredné	Nízke	Nízke
Skôr nepravdepodobné	Stredné	Stredné	Nízke	Nízke	Veľmi nízke
Nepravdepodobné	Nízke	Nízke	Nízke	Veľmi nízke	Veľmi nízke

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.4 Kritériá na určenie úrovne rizika

Tabulka E.1

	Pravděpodobnost výskytu – Hrozba	Nízká			Střední			Vysoká		
	Snadnost zneužití	L	M	H	L	M	H	L	M	H
Hodnota aktiva	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tabulka E.2

	Pravděpodobnost scénáře incidentu	Velmi nízká (Velmi nepravdě-podobná)	Nízká (Nepravdě-podobná)	Střední (Možná)	Vysoká (Pravděpodobná)	Velmi vysoká (Častá)
Dopad na podnikání	Velmi nízká	0	1	2	3	4
	Nízká	1	2	3	4	5
	Střední	2	3	4	5	6
	Vysoká	3	4	5	6	7
	Velmi vysoká	4	5	6	7	8

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

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.4 Kritériá na určenie úrovne rizika

Tabulka E.4

Pravděpodobnost hrozby	Nízká			Střední			Vysoká		
Úrovně zranitelnosti	L	M	H	L	M	H	1	M	H
Pravděpodobnostní hodnota scénáře incidentu	0	1	2	1	2	3	2	3	4

Tabulka E.5

Hodnota aktiv	0	1	2	3	4
Hodnota pravděpodobnosti					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

6 Stanovenie súvislostí
6.4 Stanovenie a udržiavanie kritérií rizík informačnej bezpečnosti
6.4.3 Kritériá na vykonávanie posúdenia rizík informačnej bezpečnosti
6.4.3.4 Kritériá na určenie úrovne rizika

Tabulka E.3

Popisovač hrozby (a)	Hodnota následků (aktivum) (b)	Pravděpodobnost výskytu hrozby (c)	Míra rizika (d)	Klasifikace hrozby (e)
Hrozba A	5	2	10	2
Hrozba B	2	4	8	3
Hrozba C	3	5	15	1
Hrozba D	1	3	3	5
Hrozba E	4	1	4	4
Hrozba F	2	4	8	3

7 Proces posúdenia rizík informačnej bezpečnosti
7.1 Všeobecne

- Posúdenie rizík pozostáva z nasledujúcich činností:
  - a) **identifikácia rizík**, čo je proces vyhľadávania, rozpoznávania a opisu rizík;
  - b) **analýza rizík**, čo je proces na pochopenie druhov rizík a určenie úrovne rizika. Analýza rizík zahŕňa zváženie príčin a zdrojov rizík, pravdepodobnosti výskytu konkrétnej udalosti, pravdepodobnosti, že táto udalosť bude mať následky, a závažnosti týchto následkov;
  - c) **hodnotenie rizík**, čo je proces porovnávania výsledkov analýzy rizík s kritériami rizík s cieľom určiť, či je riziko a/alebo jeho významnosť prijateľná, a stanoviť priority analyzovaných rizík pre ošetrenie rizík. Na základe tohto porovnania možno zvážiť potrebu ošetrenia.

7 Proces posúdenia rizík informačnej bezpečnosti
7.1 Všeobecne

- Norma ISO/IEC 27001 nepredpisuje konkrétny prístup, ktorý sa má použiť na splnenie požiadaviek.

- Napriek tomu existujú dva hlavné prístupy k posudzovaniu:
  a) **prístup založený na udalostiach,**
  b) **prístup založený na aktívach.**

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- **Vstup:** Udalosti, ktoré môžu negatívne ovplyvniť dosiahnutie cieľov informačnej bezpečnosti v organizácii alebo v iných organizáciách.
- **Činnosť:** Mali by sa identifikovať riziká spojené so stratou dôvernosti, integrity a dostupnosti informácií.
- **Výstup:** Zoznam identifikovaných rizík.

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- Na vykonávanie identifikácie rizík sa bežne používajú dva prístupy.
  a) **Prístup založený na udalostiach**: identifikácia **strategických scenárov** prostredníctvom zváženia zdrojov rizík a spôsobu ich využitia alebo vplyvu na zainteresované strany s cieľom dosiahnuť požadovaný cieľ týchto rizík.
  b) **Prístup založený na aktívach**: identifikácia **prevádzkových scenárov**, ktoré sú podrobne opísané z hľadiska aktív, hrozieb a zraniteľností.

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

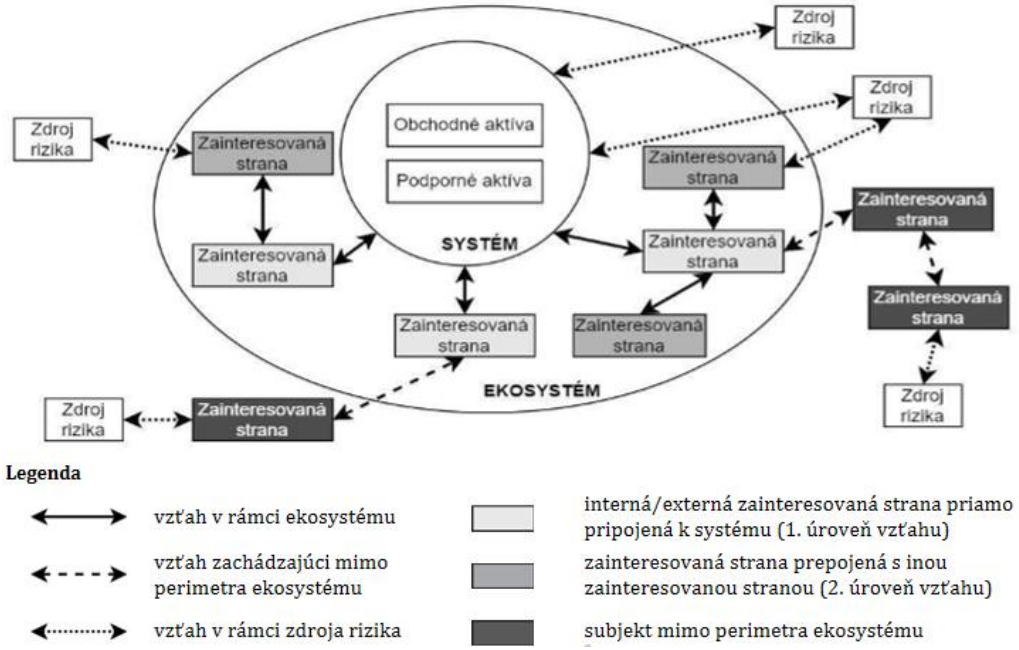
7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- **V prístupe založenom na udalostiach je základnou koncepciou to, že riziká možno identifikovať a posúdiť prostredníctvom hodnotenia zdrojov, udalostí a následkov.**
- Udalosti a následky možno často určiť na základe zistenia záujmov vrcholového manažmentu, vlastníkov rizík a požiadaviek identifikovaných pri určovaní súvislostí organizácie.
- Rozhovory s vrcholovým manažmentom a vlastníkmi procesov, môžu pomôcť pri identifikácii nielen príslušných udalostí a následkov, ale aj vlastníkov rizík.
- Prístup založený na udalostiach môže stanoviť scenáre na všeobecnej úrovni alebo strategické scenáre bez toho, aby sa strávilo značné množstvo času identifikáciou aktív na podrobnej úrovni.
- To umožňuje organizácii zamerať svoje úsilie pri ošetrovaní rizík na kritické riziká.

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- V rámci tohto prístupu by sa rizikové scenáre mali vytvárať analýzou rôznych ciest, ktoré sú relevantné pre interakcie medzi organizáciou a zainteresovanými stranami.



Identifikácia zainteresovaných strán ekosystému (STN ISO/IEC 27005:2023) (pozn. obchodné aktíva sú primárne/prevádzkové aktíva)

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

Zdroj rizika	Príklady a obvyklé metódy útoku
Štátne	Štáty, spravodajské agentúry Metóda: Útoky spravidla vykonávajú profesionáli, ktorí pracujú podľa vopred stanoveného kalendára a spôsobu útoku. Tento profil útočníka sa vyznačuje schopnosťou vykonávať útočnú operáciu počas dlhého časového obdobia (stabilné zdroje, postupy) a prispôsobiť svoje nástroje a metódy topológii cieľa. V nadväznosti na to majú títo aktéri prostriedky na nákup alebo objavenie zraniteľností nultého dňa a niektorí z nich sú schopní infiltrovať izolované siete a vykonávať postupné útoky s cieľom dosiahnuť cieľ alebo ciele (napr. prostredníctvom útoku zameraného na dodávateľský reťazec).
Organizovaný zločin	Kybernetické zločinecké organizácie (mafie, gangy, zločinecké skupiny) Metóda: Podvody online alebo osobne, žiadosť o výkupné alebo útok prostredníctvom ransomvéru, používanie botnetov atď. Najmä v dôsledku šírenia útočných súprav, ktoré sú ľahko dostupné online, kyberzločinci vykonávajú čoraz sofistikovanejšie a organizovanejšie operácie na lukratívne alebo podvodné účely. Niektorí majú prostriedky na nákup alebo objavenie zraniteľností nultého dňa.
Teroristické	Kyberteroristi, kybernetické milície Metóda: Útoky, ktoré zvyčajne nie sú veľmi sofistikované, ale sú vedené s odhodlaním s cieľom destabilizácie a deštrukcie: odmietnutie služby (zamerané napríklad na zneprístupnenie pohotovostných služieb nemocničného centra, predčasné vypnutie priemyselného systému na výrobu energie), zneužitie zraniteľností internetových stránok a znehodnotenie.
Ideologickí aktivisti	Kybernetickí hekeri, záujmové skupiny, sekty Metóda: Metódy útoku a sofistikovanosť útokov sú relatívne podobné metódam kyberteroristov, ale sú motivované menej deštruktívnymi zámermi. Niektorí aktéri vedú tieto útoky s cieľom odovzdať ideológiu, posolstvo (napr. masívne využívanie sociálnych sietí ako hlásnej trúby).
Špecializované organizácie	„Kybernetický žoldnierský" profil s IT kapacitami, ktoré sú z technického hľadiska všeobecne vysoké. Z tohto dôvodu by sa mal odlišovať od nekvalifikovaných jednotlivcov, využívajúcich nástroje (skripty) vyvinuté niekým inými (script-kiddies), s ktorými však zdieľa ducha výzvy a hľadania uznania, ale s lukratívnym cieľom. Takéto skupiny sa môžu organizovať ako špecializované oddiely, ktoré ponúkajú skutočné hekerské služby. Metóda: Tento typ skúsených hekerov často stojí na začiatku navrhovania a vytvárania útočných súprav a nástrojov, ktoré sú dostupné online (prípadne za poplatok) a ktoré potom môžu „na kľúč" používať iné skupiny útočníkov. Neexistuje žiadna osobitná motivácia okrem finančného zisku.

Zdroj rizika	Príklady a obvyklé metódy útoku
Amatérske	Profil script-kiddies heker alebo niekto, kto má dobré znalosti IT; motivovaný snahou o sociálne uznanie, zábavu, výzvu. Metóda: Základné útoky, ale s možnosťou použiť útočné súpravy, ktoré sú dostupné online.
Pomstiteľ	Motivácia tohto profilu útočníka je vedená v duchu akútnej pomsty alebo pocitu nespravodlivosti (napr. zamestnanec prepustený pre závažné pochybenie, nespokojný poskytovateľ služieb po nepredĺžení zmluvy atď.). Metóda: Tento profil útočníka je charakteristický svojou rozhodnosťou a vnútornou znalosťou systémov a organizačných procesov. To ho môže urobiť hrozivým a poskytnúť mu značnú silu na spôsobenie škody.
Patologický útočník	Motivácia tohto profilu útočníka vychádza z patologického alebo oportunistického charakteru a niekedy je vedená motívom zisku (napr. nekalý konkurent, nečestný klient, zlodej a podvodník). Metóda: V tomto prípade útočníci buď disponujú znalostnou bázou v oblasti výpočtovej techniky, ktorá ich vedie k tomu, aby sa pokúsili kompromitovať IS svojho cieľa, alebo využívajú útočné súpravy dostupné online, prípadne sa rozhodnú pre subdodávku IT útoku tým, že si prizvú špecializovanú firmu. V určitých prípadoch môžu útočníci zamerať svoju pozornosť na interný zdroj (nespokojný zamestnanec, bezohľadný poskytovateľ služieb) a pokúsiť sa ho podplatiť.

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- Na základe informácií o zdrojoch rizika a príslušných udalostiach si možno predstaviť realistické scenáre na všeobecnej úrovni (strategické scenáre), ktoré naznačujú, akým spôsobom môže zdroj rizika postupovať, aby dosiahol svoj cieľ.
- Tieto strategické scenáre sa identifikujú dedukciou.Táto dedukcia vychádza z:

a) predpokladaného **zdroja rizí**k a jeho obvyklých **metód útoku**,

b) **motivácie zdroja rizík** (napr. ovládnutie zdrojov alebo trhov, získanie politickej moci alebo vnucovania hodnôt, obmedziť konanie tretej strany, udržanie ideologickej, politickej, hospodárskej alebo sociálnej situácie, zastrašenie protivníka, aby obmedzil svoje aktivity, atď.),

c) **cieľa** (napr. špionáž, strategické predbežné rozmiestnenie, ovplyvňovanie, prekážka fungovania, obohatenie sa, výzva alebo zábava, atď.),

d) **primárnych (prevádzkových) aktív**, ktoré je potrebné na dosiahnutie cieľa,

e) predpokladu **využitia niektorej zainteresovanej strany**, ktorá má prístup k týmto aktíva.

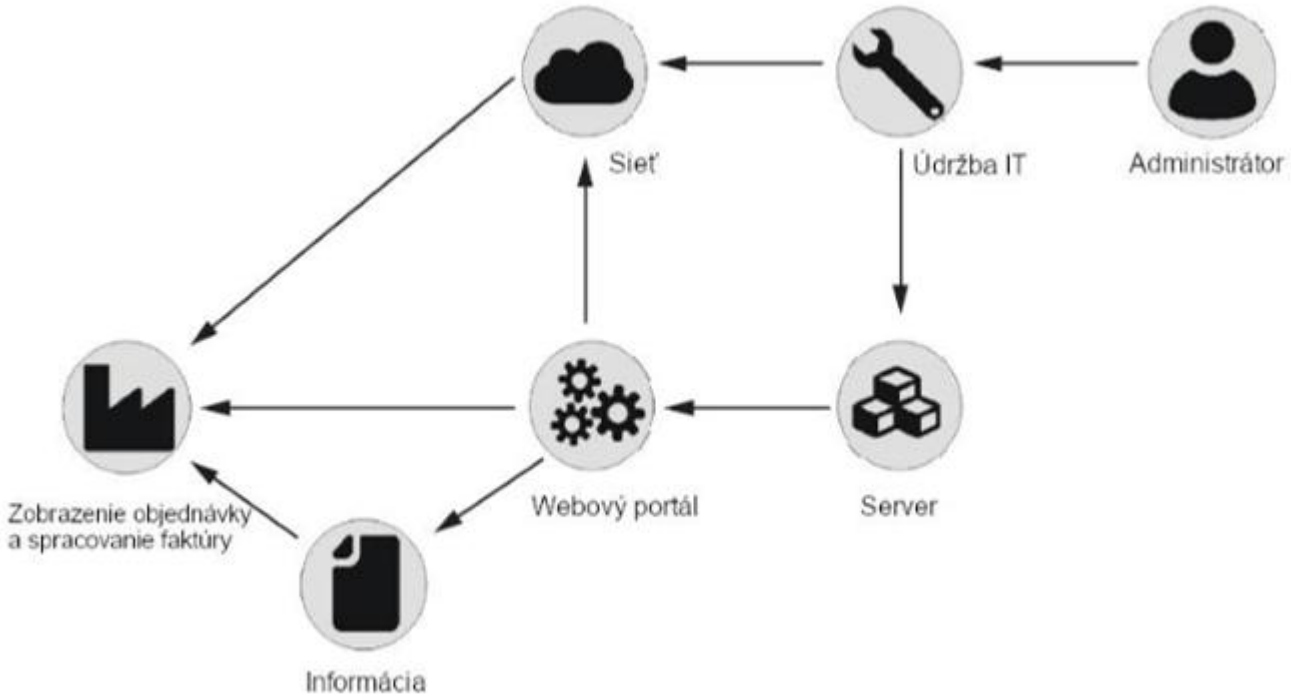
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- **Pri prístupe založenom na aktívach je základnou koncepciou to, že riziká možno identifikovať a posúdiť prostredníctvom kontroly aktív, hrozieb a zraniteľných miest.**
- Aktíva je možné identifikovať ako primárne a podporné aktíva podľa ich typu a priority, pričom sa zdôraznia ich závislosti, ako aj ich interakcie so zdrojmi rizík a zainteresovanými stranami organizácie.
- Hrozba využíva zraniteľnosť aktíva na ohrozenie dôvernosti, integrity a/alebo dostupnosti príslušných informácií.
- Ak je možné vymenovať všetky platné kombinácie aktív, hrozieb a zraniteľností v rámci rozsahu ISMS, potom by teoreticky mali byť identifikované všetky riziká.

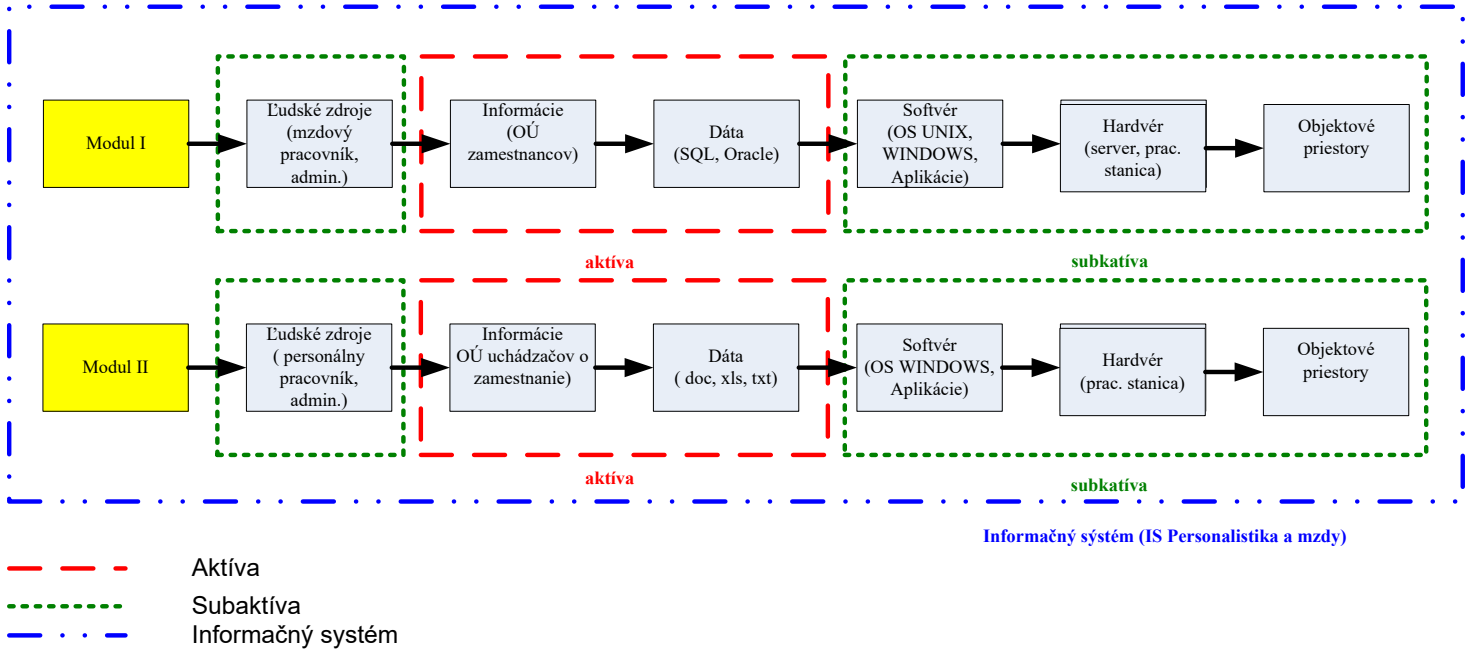
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)



Príklad grafu závislosti aktív

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)



- Príklad vytvárania modulov aktív v informačných systémoch (Loveček, 2008)

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- **Hrozba** (threat) potenciálna príčina nežiaduceho incidentu, ktorý môže mať za následok poškodenie systému, jednotlivca alebo organizácie. (ISO/IEC 27000)
- **Kybernetická hrozba** je každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby. (Zákon o KB)
- **Hrozba** – potencionálny zdroj nebezpečia, ujmy alebo iného nežiadúceho výsledku. (ISO 31073)
- **Zdroj hrozby** (threat agent) je jednotlivec alebo skupina jednotlivcov, ktorí majú akúkoľvek úlohu pri vykonávaní alebo podpore útoku. (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

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- **Útok** (attack) pokus o zničenie, odhalenie, zmenenie, znefunkčnenie, ukradnutie alebo získanie neoprávneného prístupu k aktívam alebo ich neoprávnene používať. (ISO/IEC 27000)
- **Vektor útoku** (attack vector) cesta alebo prostriedok, ktorým útočník môže získať prístup k počítaču alebo sieťovému serveru na vykonanie škodlivej činnosti. (ISO/IEC 27032)
- **Zmiešaný útok** (blended attack) útok, ktorý sa snaží maximalizovať závažnosť škody a rýchlosť šírenia nákazy kombináciou viacerých útočných metód. (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

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

Kategória	Číslo	Popis hrozby	Typ zdroja rizika [a]
Fyzické hrozby	TP01	Požiar	A, D, E
	TP02	Voda	A, D, E
	TP03	Znečistenie, škodlivé žiarenie	A, D, E
	TP04	Vážna nehoda	A, D, E
	TP05	Výbuch	A, D, E
	TP06	Prach, korózia, mráz	A, D, E
Prírodné hrozby	TN01	Klimatický jav	E
	TN02	Seizmický jav	E
	TN03	Vulkanický jav	E
	TN04	Meteorologický jav	E
	TN05	Povodne	E
	TN06	Pandémia/epidémia	E
Zlyhania infraštruktúry	TI01	Porucha zásobovacieho systému	A, D
	TI02	Porucha chladiaceho alebo ventilačného systému	A, D
	TI03	Strata napájania	A, D, E
	TI04	Zlyhanie telekomunikačnej siete	A, D, E
	TI05	Porucha telekomunikačného zariadenia	A, D
	TI06	Elektromagnetické žiarenie	A, D, E
	TI07	Tepelné žiarenie	A, D, E
	TI08	Elektromagnetické impulzy	A, D, E

Kategória	Číslo	Popis hrozby	Typ zdroja rizika [a]
Technické poruchy	TT01	Porucha zariadenia alebo systému	A
	TT02	Nasýtenie informačného systému	A, D
	TT03	Porušenie udržiavateľnosti informačného systému	A, D
Ľudské činy	TH01	Teroristický útok, sabotáž	D
	TH02	Sociálne inžinierstvo	D
	TH03	Zachytenie žiarenia zariadenia	D
	TH04	Špehovanie na diaľku	D
	TH05	Odpočúvanie	D
	TH06	Krádež médií alebo dokumentov	D
	TH07	Krádež zariadenia	D
	TH08	Krádež digitálnej identity alebo poverení	D
	TH09	Získavanie recyklovaných alebo vyradených médií	D
	TH10	Zverejňovanie informácií	A, D
	TH11	Zadávanie údajov z nedôveryhodných zdrojov	A, D
	TH12	Manipulácia s hardvérom	D
	TH13	Manipulácia so softvérom	A, D
	TH14	Zneužitie zraniteľnosti webovou komunikáciou	D
	TH15	Útok opakovaním, útok man-in-the-middle	D
	TH16	Neoprávnené spracúvanie osobných údajov	A, D
	TH17	Neoprávnený vstup do zariadení	D
	TH18	Neoprávnené používanie zariadení	D
	TH19	Nesprávne používanie zariadení	A, D
	TH20	Poškodenie zariadení alebo médií	A, D
	TH21	Podvodné kopírovanie softvéru	D
	TH22	Používanie falšovaného alebo kopírovaného softvéru	A, D
	TH23	Poškodenie údajov	D
	TH24	Nezákonné spracovanie údajov	D
	TH25	Odosielanie alebo distribúcia škodlivého softvéru	A, D, E
	TH26	Zisťovanie polohy	D
Kompromitácia funkcií alebo služieb	TC01	Chyba pri používaní	A
	TC02	Zneužitie práv alebo povolení	A, D
	TC03	Falšovanie práv alebo povolení	D
	TC04	Odmietnutie aktivít	D
Organizačné hrozby	TO01	Nedostatok zamestnancov	A, E
	TO02	Nedostatok zdrojov	A, E
	TO03	Zlyhanie poskytovateľov služieb	A, E
	TO04	Porušenie zákonov alebo predpisov	A, D

[a] D = úmyselná; A = náhodná; E = environmentálna.

Príklad typických hrozieb

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

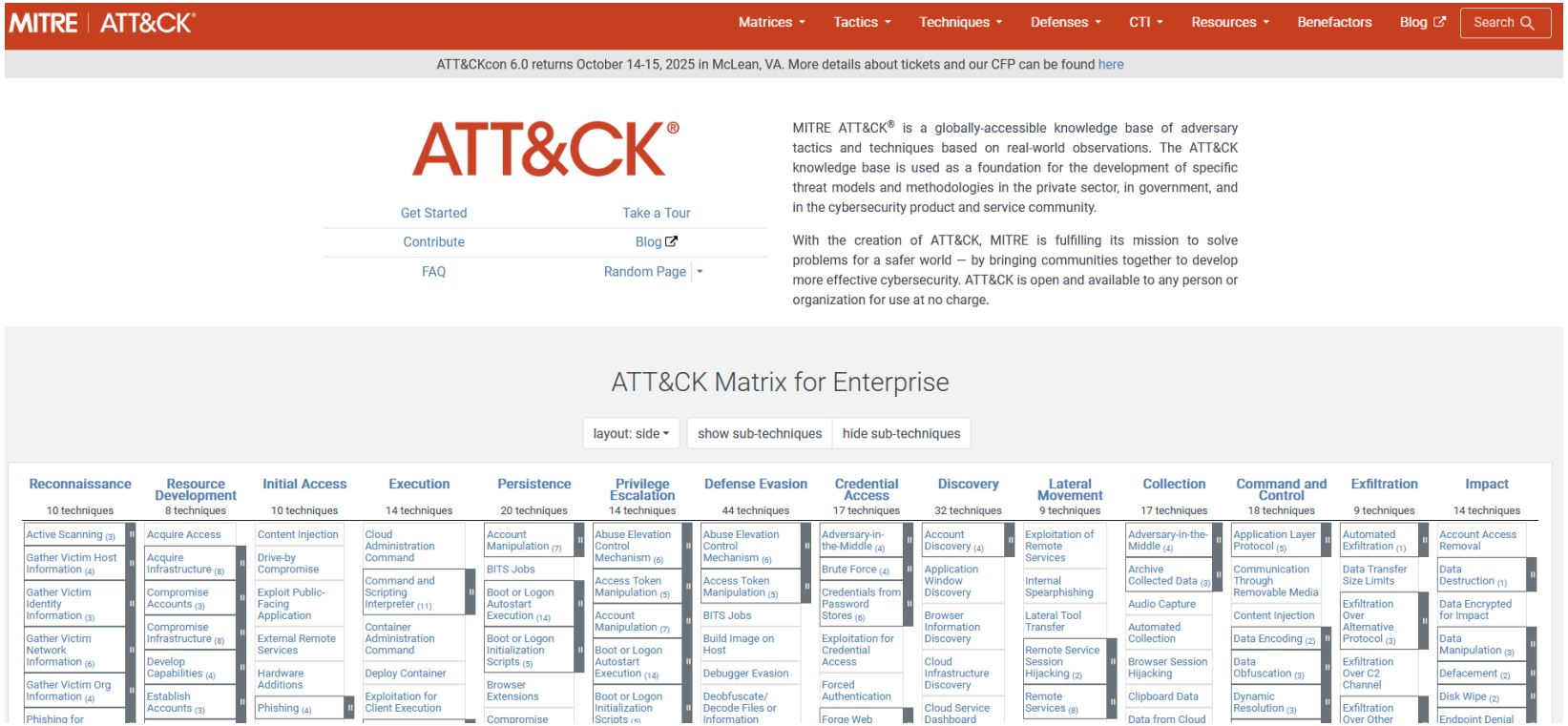
NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verejný katalóg hrozieb

Kategória hrozby	Pôvodný kód hrozby	Kód hrozby	Hrozba	Náhodná hrozba	Úmyselná hrozba	Hrozba prostredia	Popis hrozby (Typický príklad)	Ovplyvnená dôvernosť	Ovplyvnená dostupnosť	Ovplyvnená integrita	Zdrojový katalóg
Fyzické hrozby	TP01	1.1	Oheň	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) požiarom		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP06	1.2	Prach, korózia, mrazy	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) prachom, mrazom, koróziou		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP04	1.3	Veľká nehoda	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) alebo obmedzenie funkcií z dôvodu vplyvu okolitých blízkych udalostí (napríklad únik radiácie, požiar vedľajšej budovy, chemické znečistenie, výbuch v blízkosti, dopravná nehoda, letecká nehoda) vrátane ďalších dôsledkov vyplývajúcich z udalostí - cestné uzávery, zákaz vychádzania a podobne		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP02	1.4	Voda	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) záplavou, vytopením, typicky vodoinštalačnou haváriou.		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP05	1.5	Výbuch	Áno	Áno	Áno	Priemyselná havária, bombový útok, teroristické útoky, vojna, použitie zbraní		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby	TP03	1.6	Znečistenie, škodlivé žiarenie	Áno	Áno	Áno	Poškodenie (typicky nosičov údajov, alebo IT zariadení) znečistením alebo škodlivým elektromagnetickým žiarením		Áno	Áno	ISO/IEC 27005:2022
Fyzické hrozby		1.7	Zničenie zariadenia, alebo médií	Áno	Áno	Áno	Zničenie zariadení, alebo médií napr. vodou, požiarom, vandalizmus, zlyhanie úložného zariadenia, atď.		Áno	Áno	ISO/IEC 27005:2011
Hospodárske a ekonomické hrozby		2.1	Chybný rozpočet	Áno	Áno		Nedostatky finančného rozpočtu			Áno	
Hospodárske a ekonomické hrozby		2.2	Energetická závislosť	Áno		Áno	Nediverzifikovaná závislosť na jednom dodávateľovi energie, resp. zdrojov na jej výrobu		Áno	Áno	
Hospodárske a ekonomické hrozby		2.3	Narušenie hospodárstva štátu		Áno		Narušenie alebo obmedzenie menového, devízového a finančného hospodárstva		Áno	Áno	
Hospodárske a ekonomické hrozby		2.4	Ekonomické ovplyvňovanie tretej strany		Áno		Politické riziko tretej strany vzhľadom na analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany	Áno		Áno	ZoKB 20/5c
Informačné operácie		3.1	Šírenie propagandy		Áno		Úmyselné šírenie propagandy za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Informačné operácie		3.2	Vytvorenie dezinformácií		Áno		Úmyselné vytvorenie a ďalšie šírenie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Informačné operácie		3.3	Zdieľanie dezinformácií		Áno		Zdieľanie účelových dezinformácií za účelom ovplyvňovania mienky v neprospech záujmu organizácie			Áno	
Kompromitácia funkcií alebo služieb	TC01	4.1	Chyba pri používaní	Áno			Nechcená modifikácia údajov v databázach, zmazanie súborov, potrebných pre chod softvéru, chyba operátora, ktorý modifikuje údaje, vysoké pracovné zaťaženie, stres alebo negatívne zmeny pracovných podmienok, zadanie úlohy nad rámec schopností zamestnanca, slabé znalosti a zručnosti, atď.		Áno	Áno	ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb		4.2	Chyby prenosu (vrátane nesprávneho smerovania správ)		Áno		Reorganizácia prenosových kanálov elektronických, alebo materializovaných údajov; zmena pracovného jazyka, zmeny v doručovaní pošty, úprava alebo presmerovanie správ, atď.	Áno	Áno	Áno	ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb	TC03	4.3	Falšovanie práv alebo povolení		Áno		Neoprávnené pozmeňovanie identít a prístupových práv do systémov, a ich zneužitie na podvodné konanie v mene iného používateľa			Áno	ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb	TC04	4.4	Odmietnutie konania		Áno		Odmietnutie vykonania pracovnej aktivity, odopretie pracovnej zodpovednosti v procese, štrajk, atď.		Áno		ISO/IEC 27005:2022
Kompromitácia funkcií alebo služieb		4.5	Odmietnutie služby	Áno	Áno		Narušenie procesov, infraštruktúry alebo iných prvkov za účelom znefunčnenia služby (typicky DoS, DDoS)		Áno		ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb		4.6	Zhoršovanie stavu pamäťových médií	Áno		Áno	Starnutie archivovaných dokumentov, postupné prepisovanie obsahu v čase, dobrovoľné vymazanie časti dokumentu, zničenie médií napr. pri požiari, záplave atď.		Áno	Áno	ISO/IEC 27005:2011
Kompromitácia funkcií alebo služieb	TC02	4.7	Zneužitie práv alebo povolení	Áno	Áno		Neoprávnené získanie identít a prístupových práv do systémov, a ich zneužitie na podvodné konanie v mene iného používateľa	Áno			ISO/IEC 27005:2022
Ľudské konanie		5.1	Popretie	Áno	Áno		Popretie pôvodu informácie (neoprávnené popretie pravdivej informácie). Tiež stav, keď aplikácia alebo systém neprijme informáciu o zaznamenávaní aktivity používateľa, čo umožňuje zlomyselnú manipuláciu alebo sfalšovanie identifikácie aktivít. Hrozba útoku na platnosť a integritu akcií v aplikácii. Manipulácia alebo sfalšovanie identifikácie nepovolených aktivít, vymazanie denníkov alebo zápis nesprávnych údajov do protokolových súborov.			Áno	ISO/IEC 27005:2011
Ľudské konanie	ST26	5.2	Detekcia polohy		Áno		Zistenie údajov o geografickej polohe	Áno			ISO/IEC 27005:2022

Príklad typických hrozieb

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)



Príklad typických taktík a techník

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

- **Zraniteľnosť** (vulnerability) je slabé miesto aktíva alebo opatrenia, ktoré môže byť zneužité jednou alebo viacerými hrozbami. (ISO/IEC 27000)
- **Zraniteľnosť** (vulnerability) chyba, slabina alebo vlastnosť v návrhu alebo implementácii informačného systému (vrátane jeho bezpečnostných opatrení) alebo jeho prostredia, ktoré by mohli byť úmyselne alebo neúmyselne zneužité a ktoré by mohli nepriaznivo ovplyvniť aktíva alebo prevádzku organizácie. (ISO/IEC TR 19791)
- **Zraniteľnosť** akýkoľvek nežiaduci stav alebo chyba technického prostriedku alebo programového prostriedku, alebo nedostatok procesu vrátane nesprávnej bezpečnostnej konfigurácie, ktorá môže byť zneužitá kybernetickou hrozbou. (Zákon o KB)

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

Kategória	Číslo	Príklady zraniteľnosti
Hardvér	VH01	Nedostatočná údržba/chybná inštalácia pamäťových médií
	VH02	Nedostatočné plány pravidelnej výmeny zariadení
	VH03	Náchylnosť na vlhkosť, prach, znečistenie
	VH04	Citlivosť na elektromagnetické žiarenie
	VH05	Nedostatočná kontrola zmien konfigurácie
	VH06	Citlivosť na zmeny napätia
	VH07	Citlivosť na zmeny teploty
	VH08	Nechránené ukladanie
	VH09	Nedostatok starostlivosti pri likvidácii
	VH10	Nekontrolované kopírovanie
Softvér	VS01	Žiadne alebo nedostatočné testovanie softvéru
	VS02	Známe chyby v softvéri
	VS03	Žiadne „odhlásenie" pri opustení pracovnej stanice
	VS04	Likvidácia alebo opätovné použitie pamäťových médií bez riadneho vymazania
	VS05	Nedostatočná konfigurácia logov na účely auditného záznamu
	VS06	Nesprávne pridelenie prístupových práv
	VS07	Široko distribuovaný softvér
	VS08	Použitie aplikačných programov na nesprávne údaje z časového hľadiska
	VS09	Komplikované používateľské rozhranie
	VS10	Nedostatočná alebo chýbajúca dokumentácia
	VS11	Nesprávne nastavenie parametrov
	VS12	Nesprávne dátumy
	VS13	Nedostatočné identifikačné a autentifikačné mechanizmy (napr. na overenie používateľa)
	VS14	Nechránené tabuľky hesiel
	VS15	Slabá správa hesiel
	VS16	Povolené nepotrebné služby
	VS17	Nevyspelý alebo nový softvér
	VS18	Nejasné alebo neúplné špecifikácie pre vývojárov
	VS19	Neúčinná kontrola zmien
	VS20	Nekontrolované sťahovanie a používanie softvéru
	VS21	Nedostatok alebo neúplnosť záložných kópií
	VS22	Nevypracovanie správ o riadení
Sieť	VN01	Nedostatočné mechanizmy na preukázanie odoslania alebo prijatia správy
	VN02	Nechránené komunikačné linky
	VN03	Nechránená citlivá prevádzka
	VN04	Zlá spoločná kabeláž
	VN05	Jediný bod zlyhania

Kategória	Číslo	Príklady zraniteľnosti
Sieť	VN06	Neúčinné alebo chýbajúce mechanizmy na identifikáciu a autentifikáciu odosielateľa a príjemcu
	VN07	Nezabezpečená sieťová architektúra
	VN08	Prenos hesiel v čitateľnej podobe
	VN09	Nedostatočné riadenie siete (odolnosť smerovania)
	VN10	Nechránené verejné sieťové pripojenia
Personál	VP01	Neprítomnosť personálu
	VP02	Nedostatočné postupy pri prijímaní zamestnancov
	VP03	Nedostatočné bezpečnostné školenie
	VP04	Nesprávne používanie softvéru a hardvéru
	VP05	Slabé povedomie o bezpečnosti
	VP06	Nedostatočné alebo chýbajúce mechanizmy monitorovania
	VP07	Práca bez dozoru externých alebo upratovacích pracovníkov
	VP08	Neúčinné alebo chýbajúce zásady správneho používania telekomunikačných médií a zasielania správ
Lokalita	VS01	Nedostatočné alebo nedbalé používanie fyzických opatrení prístupu do budov a miestností
	VS02	Poloha v oblasti náchylnej na záplavy
	VS03	Nestabilná elektrická sieť
	VS04	Nedostatočná fyzická ochrana budovy, dverí a okien
Organizácia	VO01	Formálny postup registrácie a zrušenia registrácie používateľov nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO02	Formálny proces preskúmania prístupových práv (dohľad) nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO03	Nedostatočné ustanovenia (týkajúce sa bezpečnosti) v zmluvách so zákazníkmi a/alebo tretími stranami
	VO04	Postup monitorovania zariadení na spracovanie informácií nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO05	Audity (dohľad) sa nevykonávajú pravidelne
	VO06	Postupy identifikácie a posúdenia rizík nie sú vypracované alebo ich vykonávanie je neúčinné
	VO07	Nedostatočné alebo chýbajúce hlásenia o poruchách zaznamenané v logoch správcu a operátora
	VO08	Neprimeraná reakcia na servisnú údržbu
	VO09	Nedostatočná alebo chýbajúca dohoda o úrovni služieb
	VO10	Postup kontroly zmien nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO11	Formálny postup kontroly dokumentácie ISMS nie je vypracovaný alebo jeho implementácia je neúčinná
	VO12	Formálny postup pre dohľad nad záznamami ISMS nie je vypracovaný alebo jeho vykonávanie je neúčinné
	VO13	Formálny proces autorizácie verejne dostupných informácií nie je vypracovaný alebo jeho vykonávanie je neúčinné

Príklad typických zraniteľností

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

Kategória	Číslo	Príklady zraniteľnosti
Organizácia	V014	Nesprávne rozdelenie zodpovednosti za informačnú bezpečnosť
	V015	Plány kontinuity neexistujú, sú neúplné alebo zastarané
	V016	Politika používania elektronickej pošty nie je vypracovaná alebo jej vykonávanie je neúčinné
	V017	Postupy zavádzania softvéru do prevádzkových systémov nie sú vypracované alebo ich implementácia je neúčinná
	V018	Postupy pre manipuláciu s klasifikovanými informáciami nie sú vypracované alebo ich vykonávanie je neúčinné
	V019	Povinnosti v oblasti informačnej bezpečnosti nie sú uvedené v opisoch pracovných miest
	V020	Nedostatočné alebo chýbajúce ustanovenia (týkajúce sa informačnej bezpečnosti) v zmluvách so zamestnancami
	V021	Disciplinárny postup v prípade incidentu v oblasti informačnej bezpečnosti nie je definovaný alebo nefunguje správne
	V022	Formálna politika používania mobilných počítačov nie je vypracovaná alebo jej uplatňovanie je neúčinné
	V023	Nedostatočná kontrola aktív mimo pracoviska
	V034	Nedostatočná alebo chýbajúca politika „čistého stola a čistej obrazovky"
	V025	Autorizácia zariadení na spracovanie informácií nie je zavedená alebo nefunguje správne
	V026	Mechanizmy monitorovania narušení bezpečnosti nie sú riadne zavedené
	V027	Postupy na nahlasovanie bezpečnostných nedostatkov nie sú vypracované alebo ich vykonávanie je neúčinné
	V028	Postupy dodržiavania ustanovení o duševných právach nie sú vypracované alebo ich uplatňovanie je neúčinné

Príklad typických zraniteľností

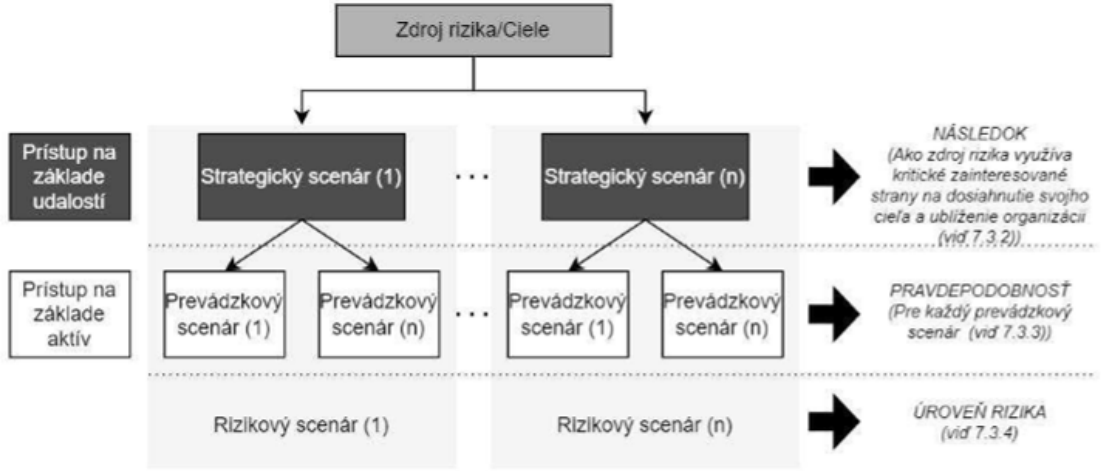
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

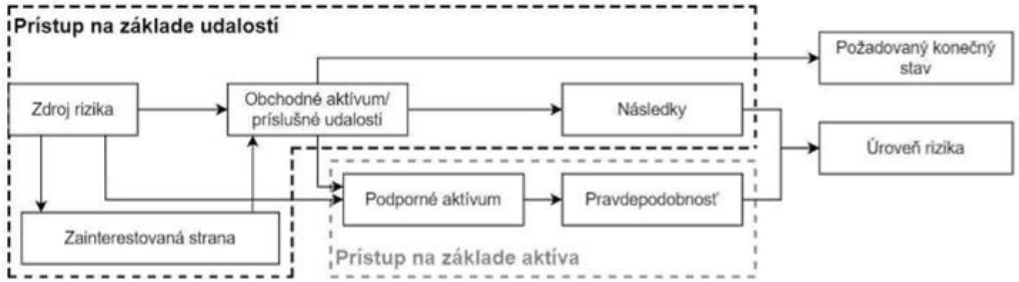
- Identifikácia rizika je rozhodujúca, pretože riziko informačnej bezpečnosti, ktoré nie je identifikované v tejto fáze, nie je zahrnuté do ďalšej analýzy.
- Identifikácia prispievajúcich zdrojov rizík pomocou posúdenia založeného na udalostiach si zvyčajne vyžaduje vŕtanie smerom nadol od všeobecnej úrovne scenára k úrovni detailov, ale posúdenie založené na aktívach zvyčajne hľadá smerom nahor od aktíva k scenáru, aby poskytlo prehľad o tom, ako sa kumulujú následky.
- Rizikové scenáre možno zostaviť buď pomocou prístupu založenom na udalostiach, prístupe založenom na aktívach, alebo pomocou oboch prístupov.
- Na jednej strane z normy vyplýva, že organizácia sa môže rozhodnúť aj iba pre jeden z možných prístupov, pričom však na strane druhej oba prístupy sú nezastupiteľné pri vytváraní rizikových scenárov a následnom stanovení úrovne rizika na základe kritérií akceptácie rizík a kritérií na vykonanie posúdenia rizík informačnej bezpečnosti (kritéria následkov/dôsledkov a kritéria pravdepodobnosti)

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)



Posúdenie rizika na základe rizikových scenárov



Komponenty hodnotenia rizík informačnej bezpečnosti

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.1 Identifikácia a popis rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.2 c) 1).)

Zdroj rizika	Cieľ DES	Scenár strategických rizík (Prístup založený na udalostiach)	Scenár operačného rizika (prístup založený na aktívach)
Autoritársky štát	Získanie strategického vektora útoku	Podvracanie kritickej infraštruktúry	Nasadenie skrytého a perzistentného malvéru v dodávateľskom reťazci
Organizovaný zločin	Rozvoj nezákonných činností	Využívanie prístavnej infraštruktúry	Infiltrácia do odborovej organizácie prístavných robotníkov
			Prevzatie kontroly nad počítačovým systémom riadenia toku
		Karuselový daňový podvod	Vytváranie fiktívnych spoločností na vykonávanie falošných výmen na trhu s uhlíkovou daňou
		Vydieranie	Distribúcia ransomvéru
Agresívne podnikanie	Získanie trhového monopolu	Ovplyvňovanie regulačného orgánu	Korumpovanie osoby s rozhodovacou právomocou
		Odstránenie konkurentov	Kampaň hanobenia na sociálnych sieťach

Rizikové scenáre popísané strategickým a prevádzkového scenára

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.2 Identifikácia vlastníkov rizík (ISO/IEC 27001: 2022, 6.1.2 c) 2).)

- **Vstup:** Zoznam identifikovaných rizík.
- **Činnosť:** Riziká by mali byť priradené k vlastníkom rizík.
- **Výstup:** Zoznam vlastníkov rizík s príslušnými rizikami.

7 Proces posúdenia rizík informačnej bezpečnosti
7.2 Identifikácia rizík informačnej bezpečnosti
7.2.2 Identifikácia vlastníkov rizík (ISO/IEC 27001: 2022, 6.1.2 c) 2).)

- Vlastníkmi rizík môžu byť vrcholový manažment, bezpečnostný výbor, vlastníci procesov, funkční vlastníci, vedúci oddelení a vlastníci aktív.
- Organizácia by mala v súvislosti s identifikáciou by mala definovať kritériá na identifikáciu vlastníkov rizík. Takéto kritériá by mali zohľadňovať, že vlastníci rizík:
  a) sú zodpovední a majú právomoc riadiť riziká, ktoré vlastnia, t. j. mali by mať v organizácii postavenie, ktoré im umožňuje túto právomoc skutočne uplatňovať;
  b) rozumejú daným problémom a sú schopní prijímať informované rozhodnutia (napr. o spôsobe ošetrenia rizík).
- Úroveň rizika a to, na aké aktívum by sa malo riziko vzťahovať, môže slúžiť ako základ pre určenie vlastníkov rizika.

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.1 Všeobecne

- Na normu ISO 31000 sa odkazuje v norme ISO/IEC 27001 ako na všeobecný model. V norme ISO/IEC 27001: 2022, 6.1.2, sa vyžaduje, aby analýza rizík bola pre každé identifikované riziko založená na **posúdení následkov** vyplývajúcich z rizika a **posúdení pravdepodobnosti** rizika s cieľom **určiť úroveň rizika**.

- Techniky analýzy rizík založené na následkoch a pravdepodobnosti môžu byť:
  a) **kvalitatívne** s použitím stupnice kvalifikačných atribútov (napr. vysoká, stredná, nízka); alebo
  b) **kvantitatívne**, s použitím stupnice s číselnými hodnotami (napr. peňažné náklady, frekvencia alebo pravdepodobnosť výskytu); alebo
  c) **semikvantitatívne**, s použitím kvalitatívnej stupnice s pridelenými hodnotami.

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.2 Posúdenie potenciálnych následkov (ISO/IEC 27001: 2022, 6.1.2 d) 1)

- **Vstup:** Zoznam identifikovaných relevantných scenárov rizík.
- **Činnosť:** Mali by sa identifikovať a posúdiť následky vyplývajúce z nedostatočného zachovania dôvernosti, integrity alebo dostupnosti informácií.
- **Výstup:** Zoznam potenciálnych následkov súvisiacich so scenármi rizík s ich následkami týkajúcimi sa aktív alebo udalostí v závislosti od použitého prístupu.

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.2 Posúdenie potenciálnych následkov (ISO/IEC 27001: 2022, 6.1.2 d) 1)

- **Následok/dôsledok** (consequence) výsledok udalosti ovplyvňujúci ciele. (ISO/IEC 27000)

- Poznámka 1 k termínu: Udalosť môže viesť k rôznym dôsledkom.
- Poznámka 2 k termínu: Dôsledok môže byť istý alebo neistý a v súvislostiach informačnej bezpečnosti je zvyčajne negatívny.
- Poznámka 3 k termínu: Dôsledky môžu byť vyjadrené kvalitatívne alebo kvantitatívne.
- Poznámka 4 k termínu: Prvotné dôsledky sa môžu stupňovať prostredníctvom domino efektov. (ISO/IEC 27000)

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.2 Posúdenie potenciálnych následkov (ISO/IEC 27001: 2022, 6.1.2 d) 1)

- Do úvahy by sa mali brať tieto prvky:
  a) odhad (alebo meranie na základe skúseností) strát (času alebo údajov) v následku udalosti ako následku prerušenia alebo narušenia prevádzky;
  b) odhad/vnímanie závažnosti následku (napr. vyjadrený v peniazoch);
  c) náklady na obnovu v závislosti od toho, či je možné obnovu vykonať interne (tímom vlastníka rizika), alebo je potrebné zavolať externý subjekt.

Následky	Popis
5 – Katastrofické	**Odvetvové alebo regulačné následky mimo organizácie** Podstatne ovplyvnený sektorový ekosystém (ekosystémy) s následkami, ktoré môžu byť dlhodobé. A/alebo: ťažkosti pre štát, či dokonca neschopnosť zabezpečiť regulačnú funkciu alebo jednu z jeho misií zásadného významu. A/alebo: kritické následky na bezpečnosť osôb a majetku (zdravotná kríza, veľké znečistenie životného prostredia, zničenie základných infraštruktúr atď.)

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.3 Posúdenie pravdepodobnosti (ISO/IEC 27001: 2022, 6.1.2 d) 2)

- **Vstup:** Zoznam identifikovaných relevantných scenárov rizík.
- **Činnosť:** Pravdepodobnosť výskytu možných alebo skutočných scenárov by sa mala posúdiť a vyjadriť pomocou stanovených kritérií pravdepodobnosti.
- **Výstup:** Zoznam udalostí alebo rizikových scenárov doplnený o pravdepodobnosť, že sa vyskytnú.

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.3 Posúdenie pravdepodobnosti (ISO/IEC 27001: 2022, 6.1.2 d) 2)

- Malo by sa pri ňom zohľadniť, **ako často sa zdroje rizika vyskytujú alebo ako ľahko sa niektoré z nich** (napr. zraniteľnosti) **dajú zneužiť**, pričom sa berú do úvahy:
  a) skúsenosti a použiteľné štatistiky pre pravdepodobnosť zdrojov rizika;
  b) **pre úmyselné zdroje rizika**: stupeň motivácie (napr. životaschopnosť (náklady/výnosy) útoku) a schopnosti (napr. úroveň zručností možných útočníkov), ktoré sa v priebehu času meniía, zdroje, ktoré majú možní útočníci k dispozícii, a vplyvy na možných útočníkov, ako je závažná trestná činnosť, teroristické organizácie alebo zahraničné spravodajské služby, ako aj vnímanie atraktívnosti a zraniteľnosti informácií pre možného útočníka;
  c) **pre náhodné zdroje rizík**: geografické faktory (napr. blízkosť nebezpečných zariadení alebo činností), možnosť prírodných katastrof (sopečná činnosť, zemetrasenia, záplavy, cunami) a faktory, ktoré môžu ovplyvniť ľudské chyby a poruchy zariadení.
- Na zvýšenie spoľahlivosti odhadu pravdepodob-nosti by organizácie mali zvážiť používanie:
  a) tímových posúdení namiesto individuálnych;
  b) jednoznačných kategórií, ako napríklad „raz ročne" namiesto „zriedkavo".

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.3 Posúdenie pravdepodobnosti (ISO/IEC 27001: 2022, 6.1.2 d) 2)

- **Pravdepodobnosť** (likelihood) šanca, že sa niečo stane.
- V terminológii riadenia rizík sa slovo „pravdepodobnosť" používa na označenie šance, že sa niečo stane, bez ohľadu na to, či je definovaná, meraná alebo určená objektívne alebo subjektívne, kvalitatívne alebo kvantitatívne, a opísaná pomocou všeobecných pojmov alebo matematicky (napríklad, pravdepodobnosť alebo frekvencia za dané časové obdobie).

- V niektorých jazykoch nemá anglický termín „likelihood" priamy ekvivalent; namiesto toho sa často používa ekvivalent termínu „probability". V angličtine sa však „probability" často interpretuje úzko ako matematický termín. Preto sa v terminológii riadenia rizík pojem „likelihood" používa so zámerom, aby mal rovnako široký výklad, aký má pojem „probability" v mnohých iných jazykoch ako v angličtine. (ISO 31000: 2018)

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.3 Posúdenie pravdepodobnosti (ISO/IEC 27001: 2022, 6.1.2 d) 2)

Pravdepodobnosť	Popis
5 – Takmer isté	Zdroj rizika s najväčšou pravdepodobnosťou dosiahne svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť rizikového scenára je veľmi vysoká.
4 – Veľmi pravdepodobné	Zdroj rizika pravdepodobne dosiahne svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť rizikového scenára je vysoká.
3 – Pravdepodobné	Zdroj rizika je schopný dosiahnuť svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť rizikového scenára je značná.
2 – Skôr nepravdepodobné	Zdroj rizika má relatívne malú šancu dosiahnuť svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť rizikového scenára je nízka.
1 – Nepravdepodobné	Zdroj rizika má veľmi malú šancu dosiahnuť svoj cieľ použitím jednej z uvažovaných metód útoku. Pravdepodobnosť výskytu rizikového scenára je veľmi nízka.

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.4 Určenie úrovne rizík (ISO/IEC 27001: 2022, 6.1.2 d) 3)

- **Vstup:** Zoznam rizikových scenárov s ich následkami týkajúcimi sa aktív alebo udalostí a ich pravdepodobnosťou (kvantitatívnou alebo kvalitatívnou).
- **Činnosť:** Úroveň rizika by sa mala určiť ako kombinácia posúdenej pravdepodobnosti a posúdených následkov pre všetky relevantné rizikové scenáre.
- **Výstup:** Zoznam rizík s pridelenými hodnotami úrovní.

7 Proces posúdenia rizík informačnej bezpečnosti
7.3 Analýza rizík informačnej bezpečnosti
7.3.4 Určenie úrovne rizík (ISO/IEC 27001: 2022, 6.1.2 d) 3)

- Úroveň rizika sa dá určiť mnohými možnými spôsobmi. Bežne sa určuje ako kombinácia posúdenej pravdepodobnosti a posúdených následkov pre všetky relevantné rizikové scenáre.
- Alternatívne výpočty môžu okrem pravdepodobnosti a následkov zahŕňať aj hodnotu aktíva.
- Okrem toho výpočet nemusí byť nevyhnutne lineárny, napr. môže to byť pravdepodobnosť na druhú v kombinácii s následkami.

Pravdepodobnosť	Následok				
	Katastrofické	Kritické	Vážne	Významné	Drobné
Takmer isté	Veľmi vysoké	Veľmi vysoké	Vysoké	Vysoké	Stredné
Veľmi pravdepodobné	Veľmi vysoké	Vysoké	Vysoké	Stredné	Nízke
Pravdepodobné	Vysoké	Vysoké	Stredné	Nízke	Nízke
Skôr nepravdepodobné	Stredné	Stredné	Nízke	Nízke	Veľmi nízke
Nepravdepodobné	Nízke	Nízke	Nízke	Veľmi nízke	Veľmi nízke

7 Proces posúdenia rizík informačnej bezpečnosti
7.4 Hodnotenie rizík informačnej bezpečnosti
7.4.1 Porovnanie výsledkov analýzy rizík s kritériami rizík (ISO/IEC 27001: 2022, 6.1.2 e) 1)

- **Vstup:** Zoznam kritérií rizík a rizík s priradenými hodnotami úrovní.
- **Činnosť:** Úroveň rizík by sa mala porovnať s kritériami hodnotenia rizík, najmä s kritériami akceptácie rizík.
- **Výstup:** Zoznam návrhov na rozhodnutia o ďalších opatreniach týkajúcich sa riadenia rizík.

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.4 Hodnotenie rizík informačnej bezpečnosti
7.4.1 Porovnanie výsledkov analýzy rizík s kritériami rizík (ISO/IEC 27001: 2022, 6.1.2 e) 1)

Úroveň rizika	Hodnotenie rizika	Popis
Nízka (zelená)	Akceptovateľné tak, ako je	Riziko možno akceptovať bez ďalších opatrení.
Stredná (oranžová)	Znesiteľné pod kontrolou	Mali by sa vykonať následné opatrenia z hľadiska riadenia rizík a mali by sa stanoviť opatrenia v rámci trvalého zlepšovania v strednodobom a dlhodobom horizonte.
Vysoká (červená)	Neakceptovateľné	Opatrenia na zníženie rizika by sa mali bezpodmienečne prijať v krátkodobom horizonte. V opačnom prípade by sa mala celá činnosť alebo jej časť zamietnuť.

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

7 Proces posúdenia rizík informačnej bezpečnosti
7.4 Hodnotenie rizík informačnej bezpečnosti
7.4.2 Stanovenie priorít analyzovaných rizík pre ošetrenie rizík (ISO/IEC 27001: 2022, 6.1.2 e) 2)

- **Vstup:** Zoznam výsledkov rizík porovnaných s kritériami rizík.
- **Činnosť:** Riziká uvedené v zozname by mali byť prioritne určené na ošetrenie rizík s ohľadom na posúdené úrovne rizík.
- **Výstup:** Zoznam prioritizovaných rizík s rizikovými scenármi, ktoré k týmto rizikám vedú.

7 Proces posúdenia rizík informačnej bezpečnosti
7.4 Hodnotenie rizík informačnej bezpečnosti
7.4.2 Stanovenie priorít analyzovaných rizík pre ošetrenie rizík (ISO/IEC 27001: 2022, 6.1.2 e) 2)

- Kritériá rizík použité na stanovenie priorít by mali zohľadňovať ciele organizácie, zmluvné, právne a regulačné požiadavky a názory príslušných zainteresovaných strán.
- Prioritizácia prijatá v rámci činnosti hodnotenia rizík je založená najmä na kritériách akceptovateľnosti.

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.1 Všeobecne

- Vstup pre ošetrenie rizík informačnej bezpečnosti je založený na výsledkoch procesu posúdenia rizík vo forme prioritizovaného súboru rizík, ktoré sa majú ošetriť, na základe kritérií rizík.
- Výstupom tohto procesu je súbor potrebných opatrení informačnej bezpečnosti, ktoré sa majú zaviesť alebo posilniť vo vzájomnej súvislosti v súlade s plánom ošetrenia rizík.
- Takto nasadený plán ošetrenia rizík je účinný, keď upravuje riziko informačnej bezpečnosti, ktorému čelí organizácia, tak, aby splnilo kritériá organizácie na akceptáciu.

8 Proces ošetrenia rizík informačnej bezpečnosti
8.2 Výber vhodných možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 a)

- **Vstup:** Zoznam prioritných rizík s udalosťami alebo scenármi rizík, ktoré vedú k týmto rizikám.
- **Činnosť:** Mali by sa vybrať možnosti ošetrenia rizík.
- **Výstup:** Zoznam prioritizovaných rizík s vybranými možnosťami ošetrenia rizík.

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.2 Výber vhodných možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 a)

- Medzi niekoľko možností ošetrenia rizík patrí:
  a) vyhnutie sa riziku, a to rozhodnutím nezačať alebo nepokračovať v činnosti, ktorá spôsobuje riziko;
  b) úprava rizika zmenou pravdepodobnosti výskytu udalosti alebo následku alebo zmenou závažnosti následku;
  c) zachovanie rizika prostredníctvom informovaného rozhodnutia;
  d) zdieľanie rizika rozdelením zodpovednosti s inými stranami, buď interne, alebo externe (napr. rozdelenie následkov prostredníctvom poistenia).

8 Proces ošetrenia rizík informačnej bezpečnosti
8.3 Určenie všetkých opatrení, ktoré sú potrebné na implementáciu možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 b)

- **Vstup:** Zoznam prioritných rizík s vybranými možnosťami ošetrenia rizík.
- **Spúšťač:** Súlad so systémom ISMS; riadenie rizík informačnej bezpečnosti.
- **Výstup:** Všetky potrebné opatrenia.

8 Proces ošetrenia rizík informačnej bezpečnosti
8.3 Určenie všetkých opatrení, ktoré sú potrebné na implementáciu možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 b)

- Osobitná pozornosť by sa mala venovať určeniu potrebných opatrení.
- Každé opatrenie by sa malo skontrolovať, aby sa určilo, či je potrebné, položením otázky:
  a) aký vplyv má toto opatrenie na pravdepodobnosť alebo následok tohto rizika;
  b) akým spôsobom opatrenie udržiava úroveň rizika.
- Ako „nevyhnutné" by sa mali označiť len opatrenia, ktoré majú na riziko väčší ako zanedbateľný vplyv. Na každé riziko vyhodnotené ako riziko vyžadujúce ošetrenie by sa malo uplatniť jedno alebo viac opatrení.
- Existuje mnoho zdrojov súborov opatrení. Možno ich nájsť v norme ISO/IEC 27001: 2022, v prílohe A, v kódexoch postupov špecifických pre odvetvia a v iných národných, regionálnych a priemyselných súboroch opatrení.

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.3 Určenie všetkých opatrení, ktoré sú potrebné na implementáciu možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 b)

- Opatrenia možno klasifikovať ako preventívne, detekčné a nápravné:
  - a) **preventívne opatrenie**: opatrenie, ktorého cieľom je zabrániť výskytu udalosti v oblasti informačnej bezpečnosti, ktorá môže viesť k výskytu jedného alebo viacerých následkov;
  - b) **detekčné opatrenie**: opatrenie, ktoré je určené na zistenie výskytu udalosti informačnej bezpečnosti;
  - c) **nápravné opatrenie**: opatrenie, ktorého cieľom je obmedziť následky udalosti informačnej bezpečnosti.

8 Proces ošetrenia rizík informačnej bezpečnosti
8.3 Určenie všetkých opatrení, ktoré sú potrebné na implementáciu možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 b)

- Za predpokladu, že existuje vhodná kombinácia preventívnych, detekčných a nápravných opatrení:
  a) detekčné opatrenia by mali zmierniť riziko v prípade zlyhania preventívnych opatrení;
  b) nápravné opatrenia by mali zmierniť riziko v prípade zlyhania detekčných opatrení;
  c) preventívne opatrenia by mali znížiť pravdepodobnosť, že sa niekedy budú musieť použiť nápravné opatrenia.

8 Proces ošetrenia rizík informačnej bezpečnosti
8.3 Určenie všetkých opatrení, ktoré sú potrebné na implementáciu možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 b)

- Medzinárodná norma ISO/IEC 27002 je určená pre organizácie všetkých typov a veľkostí. Používa sa ako referencia na určenie a implementáciu opatrení na ošetrenie rizík informačnej bezpečnosti v systéme riadenia informačnej bezpečnosti (ISMS) založenom na ISO/IEC 27001.
- Organizačné alebo prostrediu špecifické opatrenia odlišné od opatrení zahrnutých v norme, je možné určiť prostredníctvom posúdenia rizík podľa potreby.
- Norma poskytuje všeobecnú kombináciu organizačných, ľudských, fyzických a technologických opatrení informačnej bezpečnosti odvodených z medzinárodne uznávaných osvedčených postupov.
- Pri špecifikovaní takýchto opatrení by organizácia mala zvážiť zdroje a investície potrebné na implementáciu a prevádzku opatrení s realizovanou obchodnou hodnotou.

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.3 Určenie všetkých opatrení, ktoré sú potrebné na implementáciu možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 b)

- Existujú normy špecifické pre odvetvie, ktoré obsahujú ďalšie opatrenia, ktorých cieľom je riešiť konkrétne oblasti (napr. ISO/IEC 27017 pre cloudové služby, ISO/IEC 27701 pre ochranu osobných údajov, ISO/IEC 27019 pre energetický priemysel, ISO/IEC 27011 pre telekomunikačné služby a ISO 277999 pre oblasť zdravotníctva).
- Norma je štruktúrovaná do nasledujúcich kapitol/tém:
  a) Organizačné opatrenia (kapitola 5).
  b) Personálne opatrenia (kapitola 6).
  c) Fyzické opatrenia (kapitola 7).
  d) Technické opatrenia (kapitola 8).
- Príloha A - Používanie atribútov

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.3 Určenie všetkých opatrení, ktoré sú potrebné na implementáciu možností ošetrenia rizík informačnej bezpečnosti (ISO/IEC 27001: 2022, 6.1.3 b)

5 Organizačné opatrenia

5.1 Politiky informačnej bezpečnosti

Typ opatrenia	Vlastnosti informačnej bezpečnosti	Koncepty kybernetickej bezpečnosti	Prevádzkové možnosti	Bezpečnostné domény
#Preventívne	#Dôvernosť #Integrita #Dostupnosť	#Identifikovať	#Riadenie	#Riadenie_a_ekosystém #Odolnosť

5 Organizational controls

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.4 Porovnanie určených opatrení s opatreniami uvedenými v norme ISO/IEC 27001: 2022, príloha A (ISO/IEC 27001: 2022, 6.1.3 c)

- **Vstup:** Všetky potrebné opatrenia.
- **Činnosť:** Porovnajte všetky potrebné opatrenia s opatreniami uvedenými v ISO/IEC 27001: 2022, príloha A.
- **Výstup:** Všetky opatrenia, ktoré sa vzťahujú na ošetrenie rizík.
- ISO/IEC 27001 vyžaduje, aby organizácia porovnala opatrenia, ktoré určila ako potrebné na realizáciu vybraných možností ošetrenia rizík, s opatreniami uvedenými v norme ISO/IEC 27001: 2022, príloha A. Cieľom je, aby sa overilo, že pri posudzovaní rizík neboli vynechané žiadne potrebné opatrenia.

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.5 Vypracovanie vyhlásenia o aplikovateľnosti (ISO/IEC 27001: 2022, 6.1.3 d)

- **Vstup:** Všetky opatrenia vzťahujúce sa na ošetrenie rizík.
- **Činnosť:** Vypracujte vyhlásenie o aplikovateľnosti.
- **Výstup:** Vyhlásenie o aplikovateľnosti.

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.5 Vypracovanie vyhlásenia o aplikovateľnosti (ISO/IEC 27001: 2022, 6.1.3 d)

- V súlade s normou ISO/IEC 27001 by vyhlásenie o aplikovateľnosti (SoA - Statement of Applicability) malo obsahovať aspoň:
  a) potrebné opatrenia;
  b) odôvodnenie ich zahrnutia;
  c) či sú alebo nie sú implementované;
  d) odôvodnenie vylúčenia opatrení z normy ISO/IEC 27001: 2022, príloha A.
- Stav implementácie všetkých opatrení obsiahnutých v SoA možno uviesť ako „implementované", „čiastočne implementované" alebo „neimplementované". Môže to byť buď jednotlivo pri každom opatrení, alebo ako celkové vyhlásenie.
- Do SoA možno zahrnúť len opatrenia identifikované v posúdení rizík.
- Opatrenia nie je možné pridať do SoA nezávisle od posúdenia rizík.

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

8 Proces ošetrenia rizík informačnej bezpečnosti
8.6 Plán ošetrenia rizík informačnej bezpečnosti
8.6.1 Formulácia plánu ošetrenia rizík (ISO/IEC 27001: 2022, 6.1.3 e)

- **Vstup:** Výsledky z posúdenia rizík.
- **Činnosť**: Formulovať plán ošetrenia rizík.
- **Výstup:** Plán ošetrenia rizík.
- Cieľom tejto činnosti je vytvoriť plán(y) ošetrenia konkrétnych súborov rizík, ktoré sú na zozname prioritných rizík. Plán ošetrenia rizík je plán na úpravu rizika tak, aby spĺňalo kritériá akceptovateľnosti rizík organizácie.

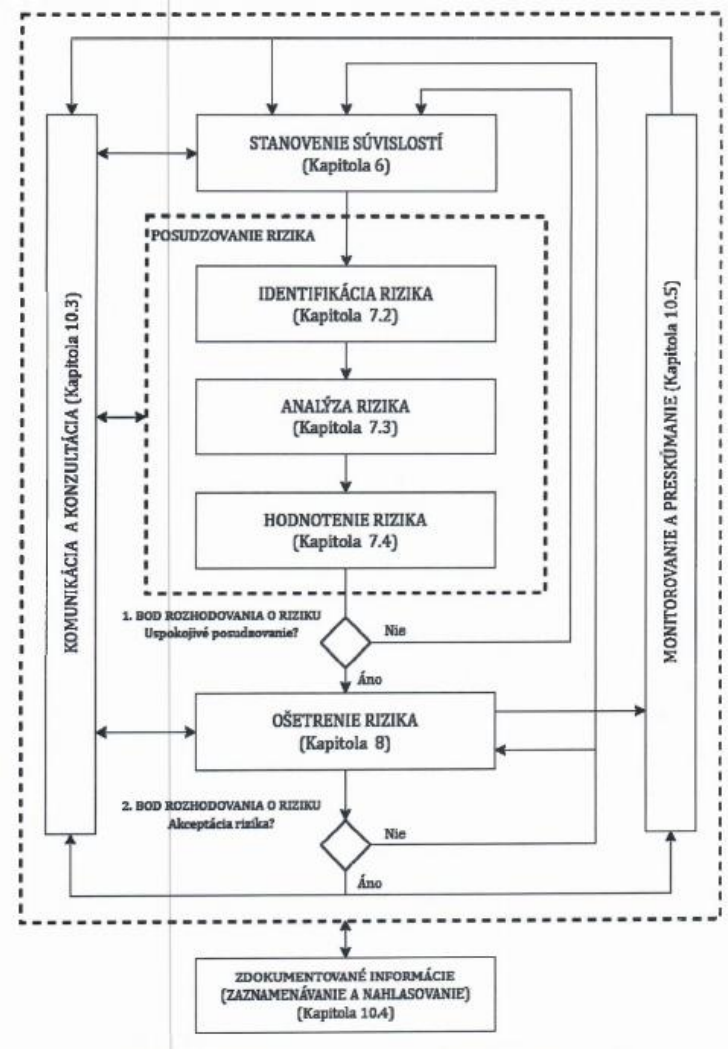
8 Proces ošetrenia rizík informačnej bezpečnosti
8.6 Plán ošetrenia rizík informačnej bezpečnosti
8.6.1 Formulácia plánu ošetrenia rizík (ISO/IEC 27001: 2022, 6.1.3 e)

- Pre každé ošetrované riziko by mal plán ošetrovania obsahovať tieto informácie:
  a) zdôvodnenie výberu možností ošetrenia vrátane očakávaných prínosov, ktoré sa majú dosiahnuť;
  b) osoby zodpovedné a poverené schválením a realizáciou plánu;
  c) navrhované opatrenia;
  d) potrebné zdroje vrátane nepredvídaných udalostí;
  e) ukazovatele výkonnosti;
  f) obmedzenia;
  g) požadované podávanie správ a monitorovanie;
  h) kedy sa očakáva vykonanie a ukončenie opatrení;
  i) stav realizácie.

8 Proces ošetrenia rizík informačnej bezpečnosti
8.6 Plán ošetrenia rizík informačnej bezpečnosti
8.6.2 Schválenie vlastníkmi rizík (ISO/IEC 27001: 2022, 6.1.3 f)

- **Vstup**: Plán(-y) ošetrenia rizík.
- **Činnosť:** Schválenie plánu(-ov) ošetrenia rizík vlastníkmi rizík.
- **Výstup:** Schválený plán (plány) ošetrenia rizík.
- Plán ošetrenia rizík v oblasti informačnej bezpečnosti by mali po jeho sformulovaní schváliť vlastníci rizík. Vlastníci rizík by mali rozhodnúť aj o akceptácii zvyškových rizík informačnej bezpečnosti. Toto rozhodnutie by malo vychádzať z definovaných kritérií akceptácie rizík.

Praktické cvičenie posudzovania a ošetrenia rizík vo verejnom sektore



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

Správa aktíva a riadenie kybernetických rizík

Riadenie bezpečnosti (Blok I.)
Kurz: Špecialista kybernetickej bezpečnosti

prof. Ing. Tomáš Loveček, PhD.

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

Tomas.Lovecek@uniza.sk