Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Riadenie kontinuity činností a krízové riadenie

Tomáš Hettych

17. jún 2025

RIADENIE AKTÍV

ASSET MANAGEMENT

INFORMAČNÉ AKTÍVUM

- **Informačné aktíva** sú všetky objekty a komponenty:
  - podieľajúce sa na dodávke IT produktov, alebo IT služieb,
  - ktoré pre organizáciu priamo, alebo nepriamo predstavujú súčasnú, alebo potenciálnu hodnotu,
  - ktorých narušenie integrity, dôvernosti a dostupnosti môže mať na organizáciu negatívny dopad



Zdroj: NBÚ - Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti

HODNOTA INFORMAČNÝCH AKTÍV

- **Hodnotu informačných aktív** je možné kvantifikovať nasledovne:
  - Informačné aktíva **tvoria hodnotu** pre organizáciu, alebo
  - Hrozby pôsobiace na informačné aktíva **spôsobujú potenciálnu stratu**



- Hodnotu informačných aktív vždy určuje **Vlastník aktíva** (resp. **Vlastník rizika**), odpoveďou na otázku:
  - Akú hodnotu informačné aktívum (napr. dokument, systém) tvorí?
  - O akú hodnotu prídeme, ak aktívum (napr. dokument, systém) nemáme k dispozícii?
  - Aká bude potenciálna strata, ak bude informačné aktívum zneužité?
  - Aká hrozí pokuta, ak informačné aktívum nie je v súlade so zákonnými požiadavkami?

Spolufinancovaný Európskou úniou

TYPY INFORMAČNÝCH AKTÍV PODĽA VÝZNAMNOSTI

PRIMÁRNE AKTÍVA

- PROCESY
- INFORMÁCIE / DÁTA

PODPORNÉ AKTÍVA

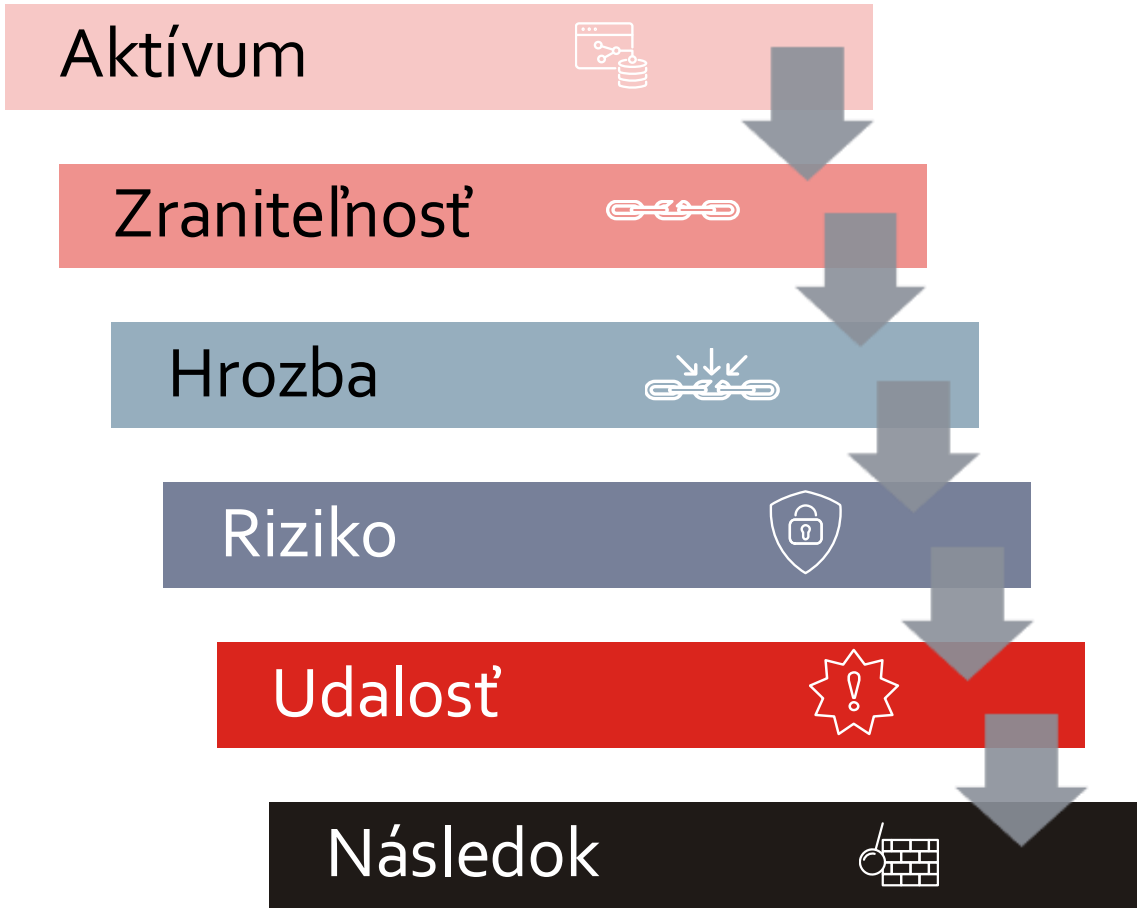
- Technológie (HW, SW, siete)
- Lokality
- Zamestnanci (interní, externí)
- Tretie strany (dodávateľ/odberateľ)

Zdroj: ISO/IEC 27005:2022

Spolufinancovaný Európskou úniou

RIADENIE RIZÍK

RIADENIE RIZÍK – POJMY



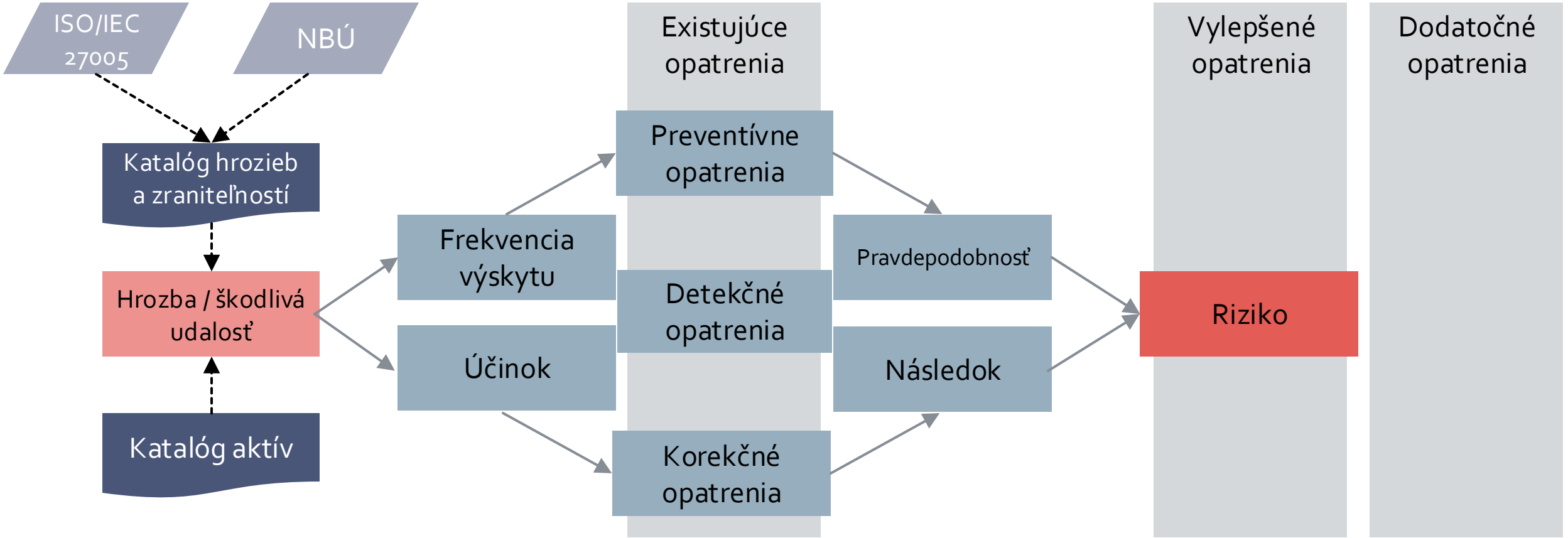
Zraniteľnosť - slabé miesto informačného aktíva, slabina v informačnom systéme, v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať alebo využiť nositeľ hrozieb.

Hrozba - potenciál, že akákoľvek okolnosť či udalosť využije zraniteľnosť informačného aktíva a spôsobí negatívny následok (dopad).

Riziko - funkcia pravdepodobnosti, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu alebo škody.

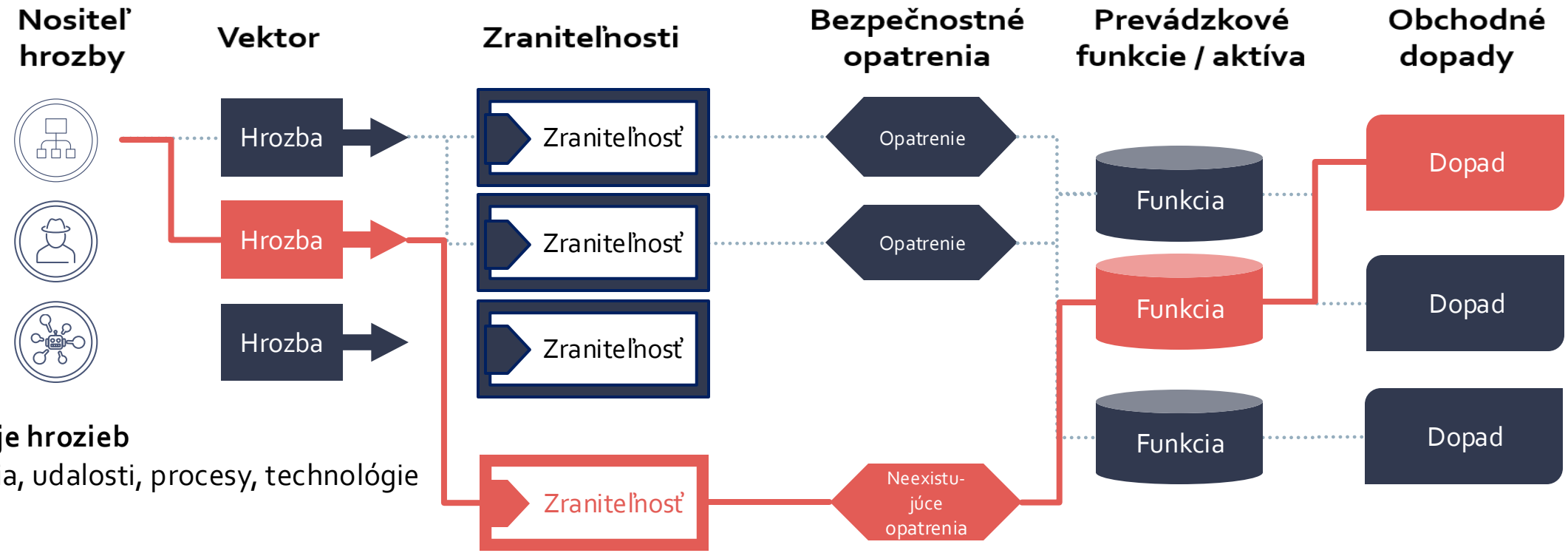
Následok - hodnota závažnosti ujmy, resp. rozsah škody, ktorá môže byť spôsobená zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou.

POSTUP PRI ANALÝZE RIZÍK



SCENÁRE RIZIKA

Scenáre rizika predstavujú špecifické situácie realizácie rizík v kontexte vybraných aktív, pričom môžu byť kombináciou viacerých aktív, kybernetických hrozieb, zraniteľností a ich následkov ako sled alebo kombinácia udalostí vedúcich od počiatočnej príčiny k nežiaducemu následku kybernetického bezpečnostného incidentu.



Zdroje hrozieb
- ľudia, udalosti, procesy, technológie

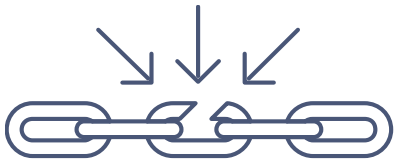
Zdroj: The Open Web Application Security Project (OWASP)

PROCESY RIADENIA KONTINUITY ČINNOSTÍ

BCM – BUSINESS CONTINUITY MANAGEMENT

RIADENIE KONTINUITY ČINNOSTÍ

- **Business continuity** (kontinuita činností organizácie) je schopnosť organizácie pokračovať v dodávke produktov a služieb na prijateľných vopred definovaných úrovniach po závažnom incidente
  [ISO 22301:2019]



- **Business continuity management** (riadenie kontinuity činností) je proces v rámci organizácie, ktorého cieľom je zaistiť kontinuitu činností v prípade závažného incidentu

- Finálnym výstupom BCM sú tzv. plány kontinuity činností (z angl. „**Business Continuity Plan**"- BCP), ktoré vo všeobecnosti obsahujú najmä podrobnosti na zvládnutie okamžitých následkov prerušenia činností

KRÍZOVÉ RIADENIE

Čo je kríza?

- Nepredvídateľná udalosť, alebo kritická situácia s veľkými dôsledkami, ktorá ohrozuje:
  - Funkčnosť časti, alebo celej spoločnosti
  - Bezpečnosť a zdravie zamestnancov, klientov, poistencov a tretích strán
  - Ciele a očakávania zainteresovaných strán
  - Reputáciu a image organizácie
- Niekoľko príkladov krízových situácií:
  - Finančná (značná finančná strata, pokuta)
  - Produktová / Operačná (hromadné stiahnutie produktu, poruchy zariadení)
  - Fyzická bezpečnosť a BOZP (sabotáže, úmrtia, pracovné úrazy)
  - Personálna (násilné činy na pracovisku, štrajk, pandémia)

Spolufinancovaný Európskou úniou

KRÍZOVÉ RIADENIE VS. KONTINUITA ČINNOSTÍ

Krízový manažment

- Reaktívny proces
- Zodpovednosť TOP manažmentu
- Krízový tím:
  - Generálny riaditeľ
  - Právne, Compliance, Risk
  - Komunikácia
  - Bezpečnosť (IT, KB, BOZP)
- Zameranie:
  - Rýchle posúdenie a rozhodnutie
  - Vytvorenie ad-hoc krízového tímu
  - Komunikácia

Kontinuita podnikania

- Preventívny proces
- Podpora TOP manažmentu
- BC tím:
  - BC manažér/koordinátor
  - Vedúci oddelení
  - Vlastníci procesov
  - Kritický personál
- Zameranie:
  - Postupy prevencie a obnovy procesov
  - Plány, zásady, personálne obsadenie, testovanie

Spolufinancovaný Európskou úniou

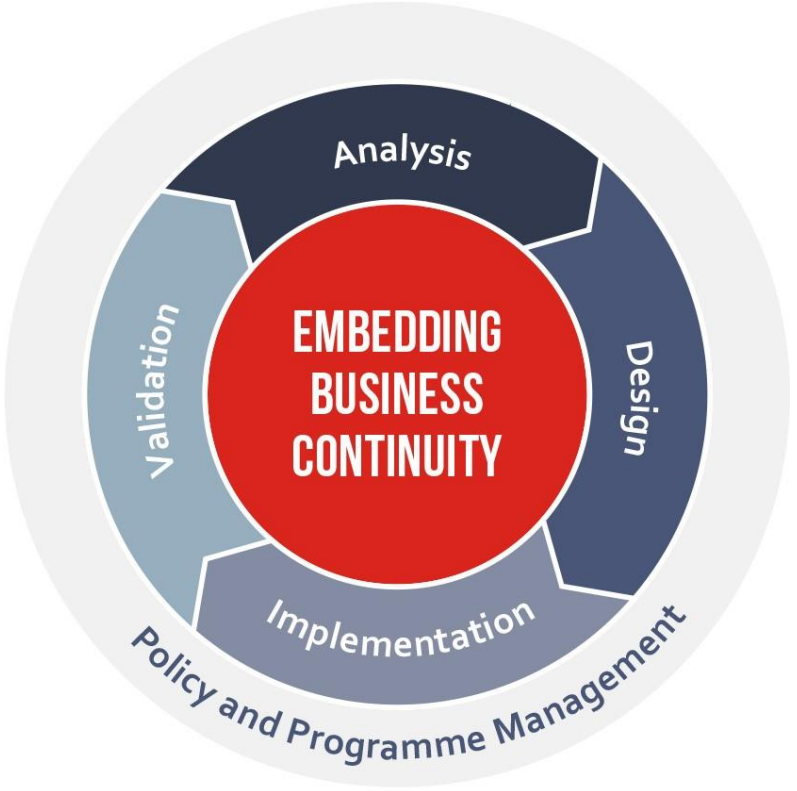
CIELE RIADENIA KONTINUITY ČINNOSTÍ

- Organizácia sama určí, **čo má byť strategickým cieľom procesu BCM**:
  1. Náležitý ohľad na záujem jednotlivca
  2. Predchádzanie ďalším stratám alebo nevykonateľnosti prioritných činností
  3. Vplyv na prostredie a zúčastnené strany
- Organizácia sama určí, **čo má byť hlavným cieľom PLÁNOV kontinuity**:
  a) Ochrana prioritných činností
  b) Stabilizácia a obnova prioritných činností, ich závislostí a podporných zdrojov
  c) Zmiernenie dopadov a reakcia na negatívne vplyvy vyvolané krízovou situ



ŽIVOTNÝ CYKLUS BCM

- **Analýza**
  - BIA – analýza dopadov
  - TRA – analýza hrozieb a rizík
  - Scenáre dopadov
  - Požiadavky na obnovu
- **Návrh riešení**
- **Implementácia procesu a plánov**
- **Validácia (testovanie a schvaľovanie)**
  - Rôzne typy testov (opísané ďalej)
- **Procesy Business Continuity (prevádzka)**
  - Pridaná hodnota
  - Testovanie a neustále zlepšovanie



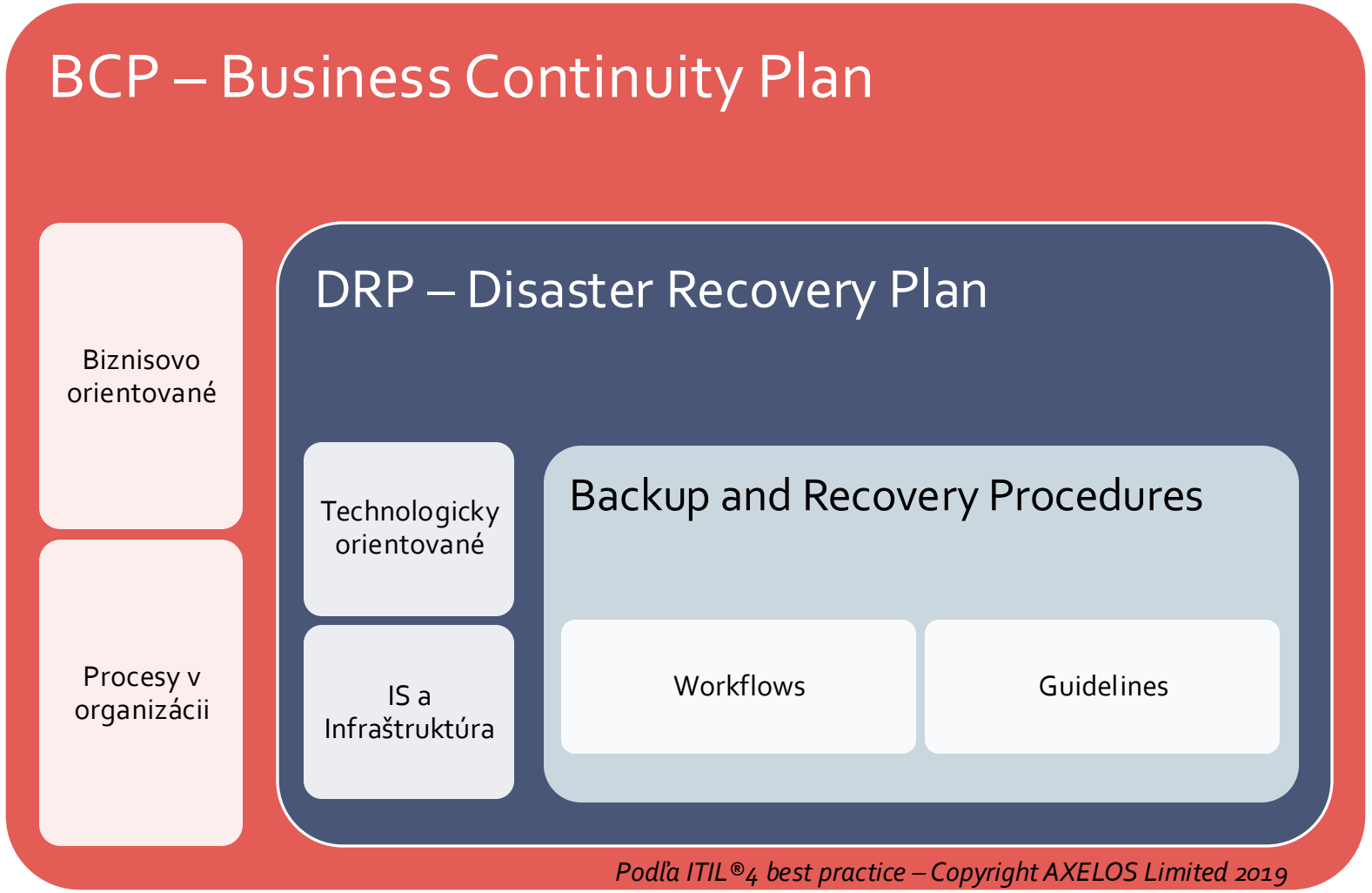
THE BCM LIFECYCLE

improving organizational resilience

Zdroj: BCI Good Practice Guide 2013

BUSINESS CONTINUITY VS. DISASTER RECOVERY

- BCP - Plán kontinuity
  - Napísané biznisom pre biznis
  - Podrobné popisy procesov
- DRP - Plán obnovy
  - Napísané IT pre IT/OT
  - Podrobné plány a postupy obnovy kritických informačných systémov a infraštruktúry
  - Súčasť BCP



Podľa ITIL®4 best practice – Copyright AXELOS Limited 2019

Spolufinancovaný Európskou úniou

STANOVENIE POŽIADAVIEK NA ZDROJE

- V rámci plánovania kontinuity organizácia stanoví požiadavky na zdroje, ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností.
- Medzi **zdroje**, ktoré by mali byť v BCP posúdené a vyčlenené, patria najmä:
  a) Ľudia
  b) Informácie a dáta
  c) Budovy, pracovné prostredie a súvisiace inžinierske siete
  d) Zariadenia, vybavenie a spotrebný materiál
  e) Systémy informačných a komunikačných technológií (IT/OT)
  f) Preprava a logistické činnosti
  g) Financovanie
  h) Partneri a dodávatelia.



ANALÝZA FUNKČNÉHO DOPADU (BIA)

BIA - BUSINESS IMPACT ANALYSIS

ANALÝZA FUNKČNÉHO DOPADU – BIA

- **Analýza funkčných dopadov** (Business Impact Analysis - BIA) identifikuje, kvalifikuje a kvantifikuje potenciálne dopady a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie s cieľom identifikovať tie procesy, ktoré sú pre organizáciu kľúčové / kritické
- Jedná sa o posúdenie ekonomických, reputačných a regulačných vplyvov, hrozieb a nákladov na obnovenie procesu v prípade výpadku v rôznych časových intervaloch od začiatku výpadku



Spolufinancovaný Európskou úniou

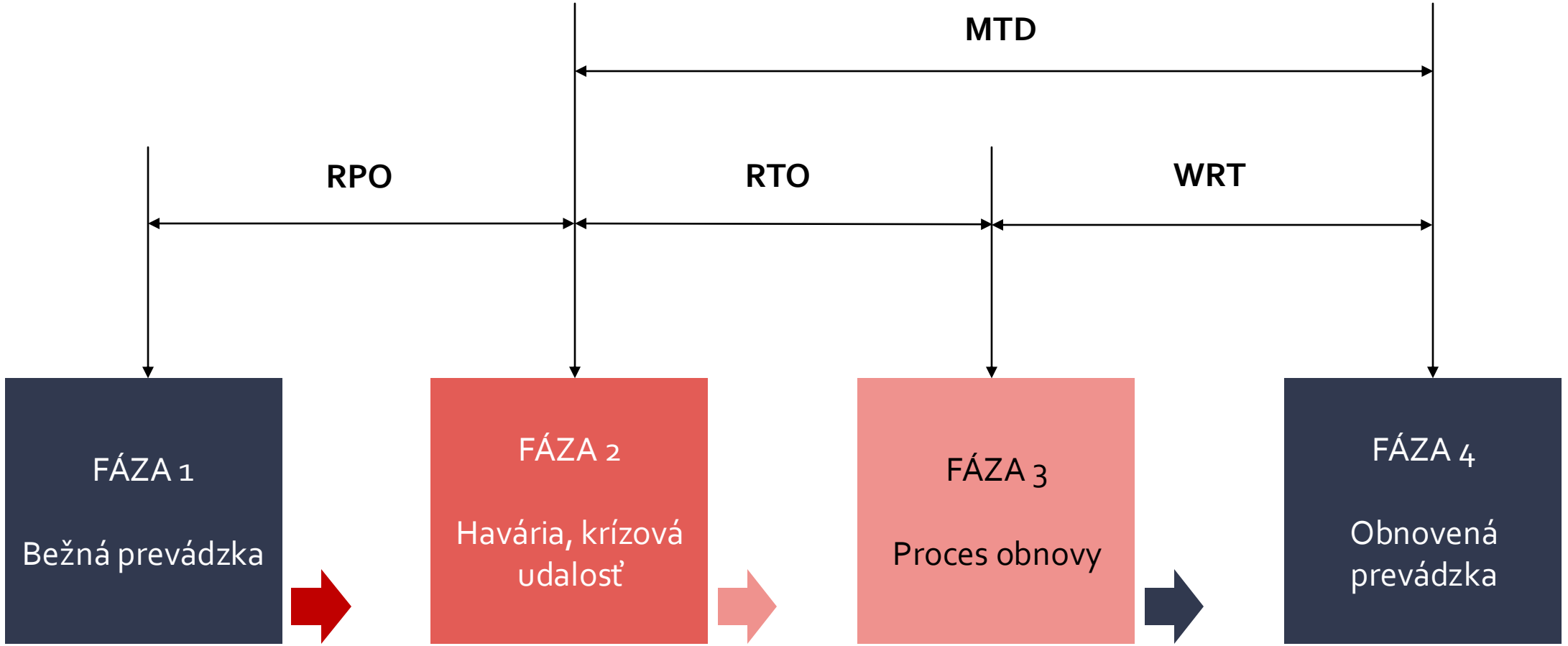
ANALÝZA FUNKČNÉHO DOPADU – BIA

- Neoddeliteľnou súčasťou BIA sú nasledovné metriky:
  - **RTO** (Recovery Time Objective) - identifikácia maximálne tolerovanej doby pre obnovenie činnosti na prijateľnej úrovni
  - **RPO** (Recovery Point Objective) - identifikácia maximálne prijateľného množstva a straty údajov merané v čase - cieľový bod obnovy
  - **WRT** (Work Recovery Time) – celkový čas obnovy
  - **MTD** (Maximum Tolerable Downtime) – maximálna doba výpadku



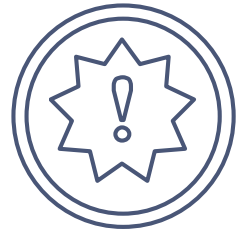
Spolufinancovaný Európskou úniou

CIEĽOVÁ DOBA OBNOVY (RTO) A CIEĽOVÝ BOD OBNOVY (RPO)



PLÁNY KONTINUITY A KRÍZOVÉ SCENÁRE

- Nevyhnutným predpokladom efektívneho plánovania kontinuity je, aby boli vopred definované scenáre rôznych udalostí, ktoré potenciálne môžu mať negatívny vplyv na bežné činnosti organizácie.
- Typickými kategóriami scenárov BCM sú napr.:
    1. **Náhla nedostupnosť personálu**
    2. **Náhla nepoužiteľnosť pracoviska/budovy**
    3. **Náhla nepoužiteľnosť technológií**
    4. **Náhla nedostupnosť médií.**



- Vedenie podniku by malo formálne rozhodnúť, ktoré scenáre majú byť vzhľadom na obmedzené zdroje predmetom BCM.
- Zvyčajne sú riešené len vyššie uvedené kategórie scenárov, pričom nie sú zahrnuté scenáre ako prírodné katastrofy, vojnové konflikty, občianske nepokoje a podobné, ktoré prekračujú rámec plánovacích možností bežnej organizácie.

TESTOVANIE PLÁNOV KONTINUITY A HAVARIJNÝCH PLÁNOV

BCM TESTING

TESTOVANIE BCP/DRP

Kontrola úplnosti plánov (Table-Top)

- Najjednoduchší typ testov.
- Zahŕňa teoretické preskúmanie kompletnosti informácií obsiahnutých v plánoch, overovanie správnosti, úplnosti a aktuálnosti uvedených údajov (kontaktné informácie na členov tímu, záložné lokality, kontakty na servisné spoločnosti, zoznam technických prostriedkov).

Teoretický prechod plánom (Walkthrough)

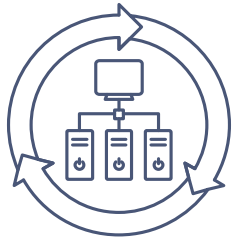
- Kontrola úplnosti plánov rozšírená o teoretické preverenie konkrétnych postupov obnov, overenie znalosti rolí jednotlivých členov tímu a ich vzájomnej komunikácie.
- Cieľom testov je odhaliť nedostatky v navrhnutých postupoch obnovy jednotlivých procesov, prípadne zaškolenie členov tímu.



Spolufinancovaný Európskou úniou

TESTOVANIE BCP/DRP

Test úplného prerušenia (Failover)



- Najťažší test, pri ktorom sa simuluje úplné zničenie lokality s následnou obnovou funkčnosti v záložných priestoroch.

Paralelné testy

- Presunutie jedného alebo viacerých vybraných kritických procesov organizácie do záložnej lokality a ich obnova v požadovanom čase.
- Technicky zamerané testy s cieľom overenia schopnosti organizácie pokračovať v činnosti v prípade vzniku krízovej udalosti.

Simulačné testy

- Praktický nácvik a preverovanie jednotlivých postupov a tímovej interakcie podľa vopred pripravených scenárov.
- Súčasťou testu je overenie funkčnosti komunikačných liniek, otestovanie komunikácie s dodávateľmi, médiami a záchrannými zložkami.
- Príkladom simulačných testov môže byť napr. nácvik evakuácie budovy alebo fiktívny požiar serverovne.

Spolufinancovaný Európskou úniou

PLÁNY TESTOVANIA BCP A DRP

Rok		Simulačný test	Teoretický prechod plánom	Kontrola úplnosti plánu
2023	Počet BCP/Názov			
2023	Počet BCP/Názov			
2024	Počet BCP/Názov			
2024	Počet BCP/Názov			
2025	Počet BCP/Názov			

Rok		Test úplného prerušenia	Paralelný test	Simulačný test	Teoretický prechod plánom	Kontrola úplnosti plánu
2023	Počet DRP/Názov					
2023	Počet DRP/Názov					
2024	Počet DRP/Názov					
2024	Počet DRP/Názov					
2025	Počet DRP/Názov					

#	Názov DRP	Typ testu	Dátum	Zodpovedný	Výsledok	Zistenia
1		Simulačný test				
2		Teoretický prechod plánom				
3		Kontrola úplnosti plánu				
4						
5						
6						
7						
8						
9						
10						

#	Názov DRP	Typ testu	Dátum	Zodpovedný	Výsledok	Zistenia
1		Test úplného prerušenia				
2		Paralelný test				
3		Simulačný test				
4		Teoretický prechod plánom				
5		Kontrola úplnosti plánu				
6						
7						
8						
9						
10						

AKÉ SÚ MOŽNÉ BENEFITY RIADENIA KONTINUITY?

- Identifikuje a spravuje súčasné a budúce hrozby pre vaše podnikanie
- Proaktívny prístup k minimalizácii dopadu incidentov
- Udržuje kritické funkcie v prevádzke v čase krízy
- Minimalizuje prestoje počas incidentov a skracuje čas obnovy
- Preukázateľná odolnosť organizácie pre zákazníkov, dodávateľov a výberové konania
- Znižuje dopad a frekvenciu prerušení podnikania
- Zlepšuje schopnosť reagovať, keď dôjde k narušeniu
- Zlepšuje vzťahy medzi zainteresovanými stranami
- Chráni a zvyšuje reputáciu a dôveryhodnosť
- Úspora nákladov
- Zlepšuje identifikáciu rizík a prináša konzistentný prístup v celej organizácii



Spolufinancovaný Európskou úniou

PÄŤ KROKOV K EFEKTÍVNEMU RIADENIU KONTINUITY ČINNOSTÍ

1) **Znalosť predmetu podnikania, účelu organizácie, resp. misia a vízia**
   - Nástroje pre analýzu dopadov a analýzu rizík sa používajú na identifikáciu kritických výstupov projektov (deliverables) a procesov, vyhodnocovanie priorít pre obnovu a nájdeniu rizík, ktoré môžu viesť ku prerušeniu biznis aktivít.
2) **Príprava rozvojových stratégií**
   - Určenie množiny alternatívnych stratégií pre ošetrenie strát, posúdenie ich relatívnych prínosov v danom prostredí organizácie a ich efektivity z pohľadu udržania kritických biznis funkcií.
3) **Príprava reakcie**
   - Vylepšovanie rizikového profilu pomocou zlepšovania prevádzkových procedúr a praktík, implementácia alternatívnych biznis stratégií s využitím meraní finančných rizík (vrátane poistenia) a budovanie plánov kontinuity.
4) **Údržba a testovanie plánov**
   - Priebežné testovania plánov, auditovanie a riadenie zmien kontinuity plánov a súvisiacich procesov.
5) **Nastavenie kultúry neustáleho zlepšovania**
   - Zavedenie procesu neustáleho zlepšovania pomocou vzdelávacích aktivít a zvyšovania povedomia u všetkých zainteresovaných strán vrátane zamestnancov, zákazníkov, dodávateľov a akcionárov.

Zdroj. BCI Good Practice Guide 2013

ZÁVER

- Ďakujeme za Váš čas
- Nasledujúci webinár na tému „ Bezpečnosť pri prevádzke sietí a informačných systémov.“ 15.7.2025



OTÁZKY?

Limity informácií

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

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

Ochrana vlastníckych práv

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

Vlastnícke práva tretích strán

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

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

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

www.cybercompetence.sk, kyberkomunita.sk

www.linkedin.com/company/cybercompetence

@CybercenterSk