



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



jihomoravský kraj

LEGISLATIVA

Kontinuita činností – vodítka vztažená ke kontinuitě činností (úvod)

Metodický list

Autor: Ing. Jiří Sedláček, Metodik: Mgr. Hana Hrádková

Recenzent: Ing. Lukáš Příbyl

Rok vydání: 2023

Kontinuita činností – vodítka vztažená ke kontinuitě činností (úvod) podléhá licenci CC BY-SA 4.0 International License (Offline use: <http://creativecommons.org/licenses/by-nc-sa/4.0/>).



Obsah

1	Cíle	3
2	Dovednosti	3
3	Pracovní prostředí	4
4	Použitý model.....	4
5	Charakteristika cvičení	4
5.1	Hlavní zásady.....	4
5.2	Výhody.....	5
5.3	Nevýhody.....	5
6	Klíčové charakteristiky	5
7	Zainteresované strany.....	6
7.1	Soutěžící týmy	6
7.1.1	Očekávání od členů týmů.....	6
7.2	Moderátor, hodnotitel, pozorovatel.....	6
7.2.1	Moderátor.....	6
7.2.2	Hodnotitel.....	6
7.2.3	Pozorovatel.....	6
8	Průběh cvičení	7
8.1	Události.....	7
8.2	Odpovědi.....	7
8.3	Diskuze	7
8.4	Závěrečný debrief a vyhodnocení	7
9	Osnova výuky.....	8
A	- Teoretická část	8
A-1	Kontinuita činností organizace – úvod do problematiky.....	10
B	- Praktická část	17
10	Input 1 - Právní normy	17
10.1	Hierarchie právních norem podle právní síly.....	17

10.1.1	Právní normy jsou hierarchicky členěny podle právní síly. Zde uvedené typy právních norem spojte spojnicí od norem s nejvyšší právní silou po nejnižší s níže umístěnou pyramidou:	17
10.2	Zákony ČR a právo EU	18
10.2.1	Proč jsou zákony ČR ovlivněny právními akty EU?.....	18
10.2.2	Jaké typy EU právních aktů ovlivnily ZoKB, VyKB a OOÚ?	18
11	Input 2 – Vybrané pasáže ze ZoKB, VyKB a příslušné normy vzhledem k BCMS	19
11.1	ZoKB.....	19
11.1.1	Definujte pojem „bezpečnostní opatření“ s uvedením čísla paragrafu.	19
11.1.2	Uveďte, jak jsou bezpečnostní opatření rozdělena.....	19
11.1.3	Jaká organizační opatření směřují ke kontinuitě činností?.....	19
11.2	VyKB	19
11.2.1	Jaký paragraf, odstavec a písmeno v rámci řízení aktiv u těchto hodnotí i jejich dostupnost?.....	19
11.2.2	Vyjmenujte cíle řízení kontinuity činností	20
11.2.3	Uveďte hodnoty a označení úrovní u stupnice pro hodnocení dostupnosti.....	20
11.3	ČSN EN ISO 22301	20
11.3.1	Specifikujte význam pojmu BCMS	20
11.3.2	Co musí plány kontinuity podnikání souhrnně obsahovat?	20
11.3.3	Co musí každý plán kontinuity podnikání obsahovat a kdy a kde musí být k dispozici?	21
12	INPUT 3 BCMS	22
12.1	Pojmy z oblasti BCMS.....	22
12.1.1	Popište níže uvedené zkratky – anglický název a český ekvivalent.....	22
12.1.2	Popište význam BIA	22
12.1.3	Na níže uvedené ose doplňte příslušné parametry	23
12.1.4	Uveďte a zdůvodněte vztah parametrů RPO – MTDL, RTO – MTD.....	23
12.1.5	Graficky vyjádřete vztah RPO a nákladů na dostupnost dat, s uvedením rizika ztráty dat a RTO a nákladů na dostupnost systému s uvedením rizik výpadku systému	23
	Shrnutí a závěr	24
	Seznam použitých zdrojů.....	25

1 Cíle

Uvedení všech cílů, kterých bude v rámci této úlohy dosaženo, dle Bloomovy taxonomie výukových cílů (viz. Příloha

1)

- Porozumět smyslu práva v rámci fungování státu.
 - Pochopit hierarchii právních norem podle právní síly a vliv právních předpisů EU na právní předpisy ČR.
 - Pochopit dopady legislativy EU na zákon o kybernetické bezpečnosti (dále jen ZoKB¹) a vyhlášku o kybernetické bezpečnosti (dále jen VyKB²).
 - Pochopit roli NÚKIB coby ústředního správního orgánu v oblasti kybernetické bezpečnosti.
 - Pochopit ZoKB a VyKB ve vztahu ke konkrétní typově popsané organizaci.
 - Aplikovat právo ČR do právních aktů právnické osoby.
-
- Naučit se pracovat se zákonem a vyhláškou o kybernetické bezpečnosti.
 - Naučit se pracovat s webem NÚKIB.
 - Porozumět významu a smyslu kontinuity činností a osvojit si praktickou aplikaci.
 - Prohloubit znalosti účastníků cvičení v oblasti kybernetické bezpečnosti a kontinuity činností.
 - Umožnit účastníkům cvičení sdílení zkušeností a názorů, včetně tréninku týmové práce a spolupráce.
 - Rozvoj analytického myšlení. Uvažování v souvislostech.

2 Dovednosti

- Pracovat se zákonnými předpisy relevantními k cvičenému tématu.
- Aplikovat legislativu ČR dle hierarchie právních hodnot podle právní síly do předpisové základny organizace.
- Identifikovat v legislativě ČR opatření vztažená ke kontinuitě činností a jejich aplikace do hypotetické organizace.
- Pracovat s webem NÚKIB.
- Porozumět kontinuitě činností, analýze dopadů, posouzení rizik, zotavení z havárie, včetně významu, terminologie a vzájemných vztahů.
- Vyjednávat v týmu o řešeních stanovené problematiky.
- Sdílet v týmech názory, znalosti a stanoviska.

¹ ZoKB - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

² VyKB - Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

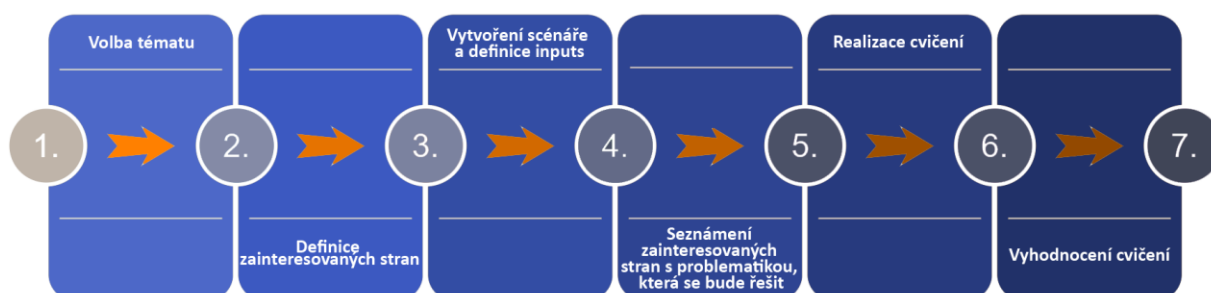
3 Pracovní prostředí

- Úlohu lze realizovat v učebně vybavené výpočetní technikou, tabulí s popisovači, projektorem a místem pro jednotlivé týmy.

Pro práci jsou vhodné následující pomůcky:

- Psací potřeby.
- Poznámkové bloky.
- Dle potřeb popisovací lepíky.
- Projektor s promítacím prostorem (plátno/stěna).
- Počítač s rozhraním pro připojení projektoru.

4 Použitý model



5 Charakteristika cvičení

Tabletop cvičení je druh tréninku, při němž je možné celkem nenákladnou formou procvičit navozená témata, včetně organizačních a technických opatření a znalostí k tomu potřebných. Cvičení je realizováno účastí jednotlivých týmů tzv. „u stolu“.

5.1 Hlavní zásady

- Týmový duch.
- Soutěživost.
- Spolupráce.
- Sdílení znalostí.
- Brainstorming.

- Rovnost názorů.

5.2 Výhody

- Nízko stresové prostředí.
- Nízké náklady.
- Průběžné hodnocení.
- Moderovaná skupinová diskuse o problémových oblastech.

5.3 Nevýhody

- Chybí reálný prožitek.
- Nejedná se o skutečný test provozní schopnosti.
- V rámci simulace je poskytnut pouze povrchní pohled na danou organizaci.

6 Klíčové charakteristiky

- Tento typ cvičení slouží k seznámení zúčastněných osob se související tematikou a k řešení navozené situace či témat. Cílem není hodnotit správnost odpovědí.
- V rámci týmu jsou určeny role a to tak, aby bylo cvičení co nejpřínosnější.
- Navozená situace či řešená témata vyžadují efektivní týmové rozhodování, a to navzdory nedostatku informací a časovému tlaku.
- Přínosnou a žádanou je diskuze, a to jak v týmech, tak i mezi týmy. Vede nejen k učinění relevantního rozhodnutí, ale je i přínosem cvičení.
- Každému rozhodnutí je vhodné předřadit relevantní faktory/roviny (bezpečnostní, věcné, právní, politické, ekonomické, mediální...).
- Navozená situace nemusí být vždy smyšlená. Může být inspirována skutečnou událostí.
- Scénář může popisovat děj podobný ději v reálném světě, v ČR, ve smyšlené organizaci.
- Je žádoucí řešit vždy pouze navozenou situaci či témata.

7 Zainteresoované strany

7.1 Soutěžící týmy

- Cvičení se zúčastní 4 týmy po 5 členech.
- V tomto konkrétním cvičení se nerozlišují role jednotlivých aktérů s výjimkou určení zástupce za každý tým pro komunikaci jménem týmu.
- Týmy mají k dispozici tento manuál a další materiály potřebné k účasti na cvičení – viz níže.

7.1.1 Očekávání od členů týmů

Nezdráhejte se zapojit do konverzace. Buďte aktivní, vyzývejte i ostatní členy týmu k zapojení do diskuze. Je v pořádku nemít odpověď. Přijměte představený scénář a pracujte v rámci uvedených parametrů.

7.2 Moderátor, hodnotitel, pozorovatel

7.2.1 Moderátor

- Zástupce školy, případně externí spolupracovník.
- Moderátor má k dispozici tento manuál a materiály s klíčem k řešení událostí a inputs.

7.2.1.1 Činnosti moderátora

- Seznámí týmy se scénářem/tématy.
- Řídí čas.
- Operativně reaguje v rámci nastalé situace atd.
- Kontrolujte tempo a průběh cvičení.
- Stimulujte a řídí diskusi.
- V případě potřeby dodává vodítka.
- Získává odpovědi a řešení od týmů.

7.2.2 Hodnotitel

- Zástupce školy, případně externí spolupracovník.
- Hodnotitel je seznámen s navozeným tématem či situací v rámci daného cvičení.

7.2.2.1 Činnosti hodnotitele

- U Týmů identifikujte silné stránky a oblasti zlepšení.
- Pomáhá vypracovat zprávu po cvičení.

7.2.3 Pozorovatel

- Zástupce školy, případně externí spolupracovník.
- Pozorovatel je seznámen s navozeným tématem či situací v rámci daného cvičení.

7.2.3.1 Činnosti pozorovatele

- Účastní se diskuze, pokud je požádán.

Pozn.: Pro potřeby cvičení, v prostředí organizace typu střední škola, je možné, s cílem snížení nároků na personální zdroje, role moderátora, hodnotitele a pozorovatele sloučit do jedné role.

8 Průběh cvičení

8.1 Události

- Scénář cvičení je koncipován tak, že dané téma je řešeno v několika oddělených vstupech (inputs – viz materiál pro týmy). Ta budou vždy moderátorem představena ať už ústně či za pomoci prezentace.
- V rámci každého inputu obdrží každý tým otázky, případně formulář pro zaznamenání odpovědí. Otázky mohou být doplněny i grafickými informacemi. Vše je nutné pečlivě přečíst a zanalyzovat.
- Na analýzu každé navozené situace v rámci inputu je určen časový limit, který moderátor hlídá.
- V některých případech, kdy k tomu dá moderátor svolení, bude možné použít internetu jako zdroje informací.

8.2 Odpovědi

- Na každou položenou otázku odpovězte ve stanoveném čase.
- Protože se jedná o týmovou práci, otázky v týmu diskutujte a odpovědi formulujte jako tým společně.
- V případě, že se nemůžete v rámci týmu na výsledné odpovědi shodnout, zaznamenejte to do odpovědního formuláře.

8.3 Diskuze

- Mimo diskuze v týmech je možná taktéž diskuze mezi týmy.
- Tuto diskuzi iniciuje a řídí výhradně pouze moderátor (a to i neplánovaně podle průběhu cvičení).

8.4 Závěrečný debrief a vyhodnocení

- Po uplynutí stanoveného programu a času bude cvičení ukončeno.
- Moderátor ve spolupráci s hodnotitelem cvičení vyhodnotí.

V dohodnutém termínu bude cvičení za přítomnosti všech týmů shrnuto a účastníci budou seznámeni s výsledky.

9 Osnova výuky

Výuka je rozdělena na teoretickou a praktickou část.

A - Teoretická část

Před realizací cvičení je nezbytné ujistit se, že témata řešená v praktické části jsou pro žáky známá, pochopená a srozumitelná. Pokud jsou identifikovány oblasti, které nejsou součástí standardního vzdělávání, je nutné je před realizací cvičení probrat. Jedná se o zákonné normy/oblasti, které jsou uvedeny v Použité literatuře a v kontextu k řešeným úkolům v rámci cvičení.

Cvičení se týká smyšlené organizace, která **není povinnou osobou z pohledu ZoKB**.

Název smyšlené organizace:

Copy&Print s.r.o.



Postavení z pohledu zakotvení právnické osoby, ICT a ochrany informací:

Právní subjektivita, popis společnosti

- Společnost s ručením omezeným.
- Společnost byla založena v roce 2010.
- Předmět podnikání:
 - Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona:
 - Vydavatelské činnosti, polygrafická výroba, knihařské a kopírovací práce.
 - Velkoobchod a maloobchod.
 - Poskytování software, poradenství v oblasti informačních technologií, zpracování dat.
 - Reklamní činnost, marketing, mediální zastoupení.

Vztah společnosti k problematice kybernetické bezpečnosti

- Společnost není povinnou osobou z pohledu ZoKB, nicméně jako rámec pro zajištění KB používá bezpečnostní opatření stanovená ZoKB.
- Společnost používá VyKB jako implementační/prováděcí manuál v rozsahu, který je pro společnost únosným a žádoucím.

ICT společnosti

- Společnost provozuje a je existenčně závislá na těchto informačních systémech:
 - **C&P_Ucto** – ERP IS – jedná se o informační systém poskytující komplexní služby v oblasti řízení společnosti, zejména pak účetnictví, skladové hospodářství, personalistiku, logistiku, atd.
 - **C&P_CRM** – CRM IS – jedná se o obchodní informační systém.
 - **C&P_SP** – jedná se o portál pro sdílení informací a dat.

- **C&P_Exchange** – jedná se o komunikační platformu zajišťující mail komunikaci.
- Serverovna je umístěna v suterénu sídla společnosti.

A-1 Kontinuita činností organizace – úvod do problematiky

Business Continuity

Strategická a taktická způsobilost organizace být připraven a reagovat na incidenty a narušení činností organizace za účelem pokračování na předem stanovené přijatelné úrovni.

Objasnění pojmů

BCP (Business Continuity Plan)

- jedná se o soubor dokumentovaných procedur, které zahrnují všechny činnosti potřebné na zabezpečení nepřetržité dodávky klíčových služeb a produktů na požadované úrovni v případě výskytu incidentu nebo havárie,
- připravuje podmínky na realizaci DRP.

DRP (Disaster Recovery Plan)

- jasně dokumentovaný plán aktivit vedoucích k zajištění obnovy všech procesů a informačních systémů organizace,
- jeho součástí je i seznam zúčastněných osob včetně závislostí mezi nimi, tedy stavu nadřizenosti a podřizenosti.

BIA (Business Impact Analysis)

Analýza dopadu na podnikání (BIA) je proces určování kritičnosti obchodních aktivit a souvisejících požadavků na zdroje, aby byla zajištěna provozní odolnost a kontinuita činností během a po přerušení podnikání.

BIA kvantifikuje dopady přerušení na poskytování služeb, rizika pro poskytování služeb a cíle doby obnovy (RTO) a cíle bodů obnovy (RPO). Tyto požadavky na obnovu se pak používají k vývoji strategií, řešení a plánů.

Jak již název napovídá, BIA odhaduje nejen dopad ztráty kritického obchodního procesu z hlediska finančních nákladů, ale i z pohledu poškození pověsti, z pohledu na dopad dodržování předpisů atd.

RA - Risk Assessment

Posouzení rizik. V organizaci jsou identifikována nejkritičtější aktiva, hrozby a zranitelnosti, následně je stanovena míra rizika. Tak je pak hodnocena z hlediska přijatelnosti a jsou přijímána případná opatření pro snížení míry rizika na přijatelnou mez.

RPO – Recovery Point Objective – Cíl bodu obnovy činností

Na základě tohoto parametru je určen interval zálohování. Platí vztah $RPO < MTDL$

Čas nevědomí, neboli reakční čas je doba, po kterou se incident neřeší ať už z důvodu, že se o něm neví, či z jiného objektivního důvodu.

RTO – Recovery Time Objective – Cíl doby obnovy činností

Jedná se o čas nutný k obnově. Platí vztah $RTO < MTD$.

WRT – Workout Recovery Time

Čas nutný pro provedení kontrolních činností (konzistence dat, atd.) po obnově.

MTO/MTD – Maximum Tolerable Outage/Down Time

Maximální přípustný celkový čas odstávky.

SLA – Service Level Agreement

Úroveň poskytovaných služeb.

MRSL – Minimum Required Service Level – Minimální úroveň poskytovaných služeb

Ukazatel stanovující minimální úroveň poskytovaných služeb, při které je zajištěno dosažení cíle systému.

MTDL – Maximum Tolerable Data Loss
 Maximální přípustná ztráta dat.

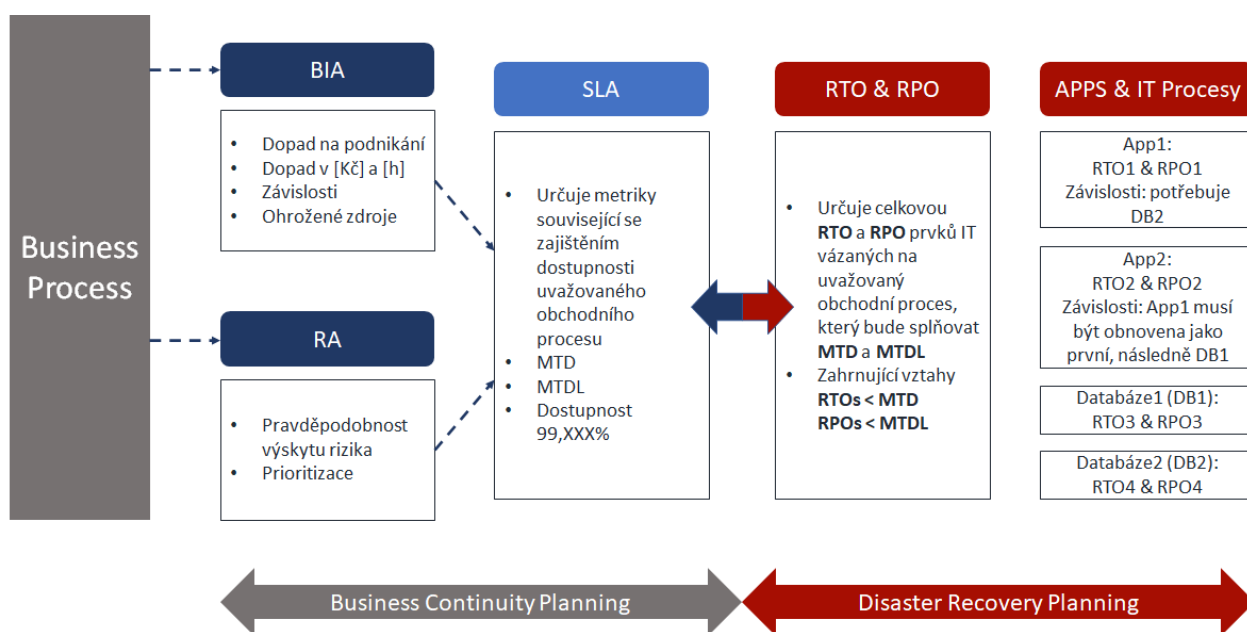
Kategorie kritičnosti

Kategorie kritičnosti se používají k určení kritických funkcí nebo procesů, které se s největší pravděpodobností stanou středem zájmu z hlediska kontinuity podnikání. Kritičnost daného procesu se může v průběhu času měnit, protože dopad tohoto procesu se zhoršuje, čím déle zůstává nedostupný.

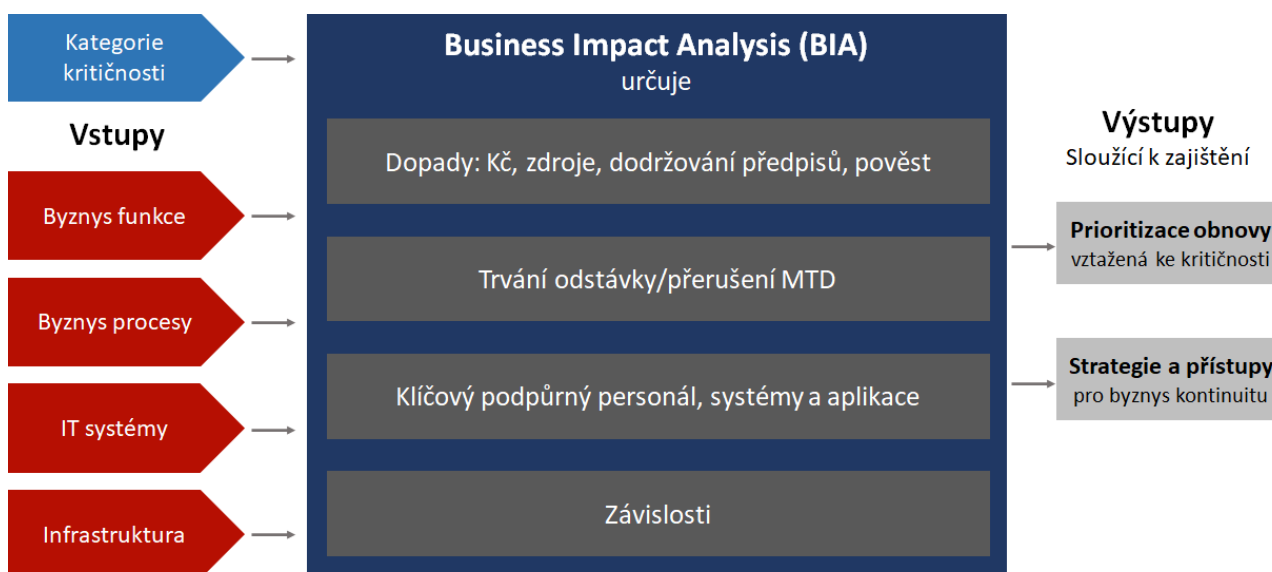
Proces

Soubor vzájemně souvisejících nebo vzájemně působících činností, které přeměňují vstupy na výstupy

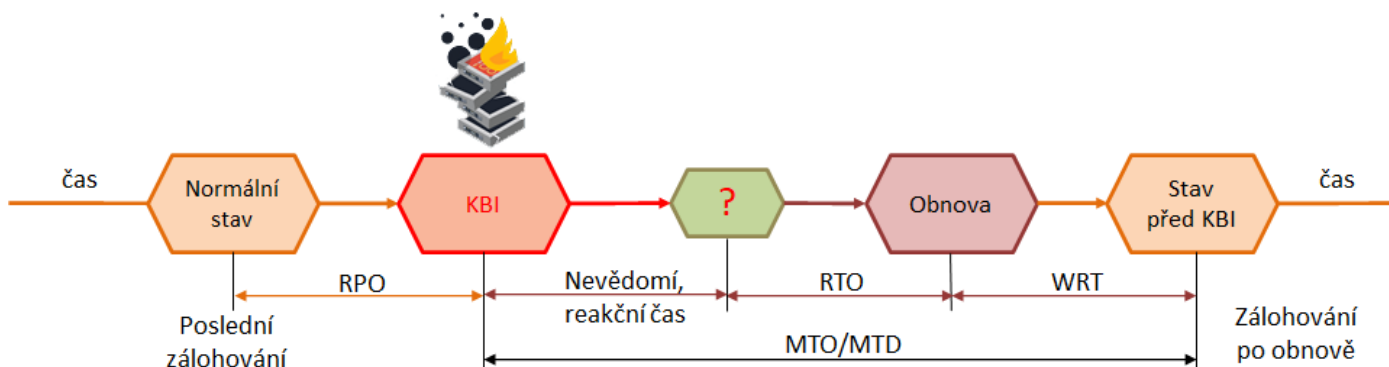
Vztah BCP a DRP



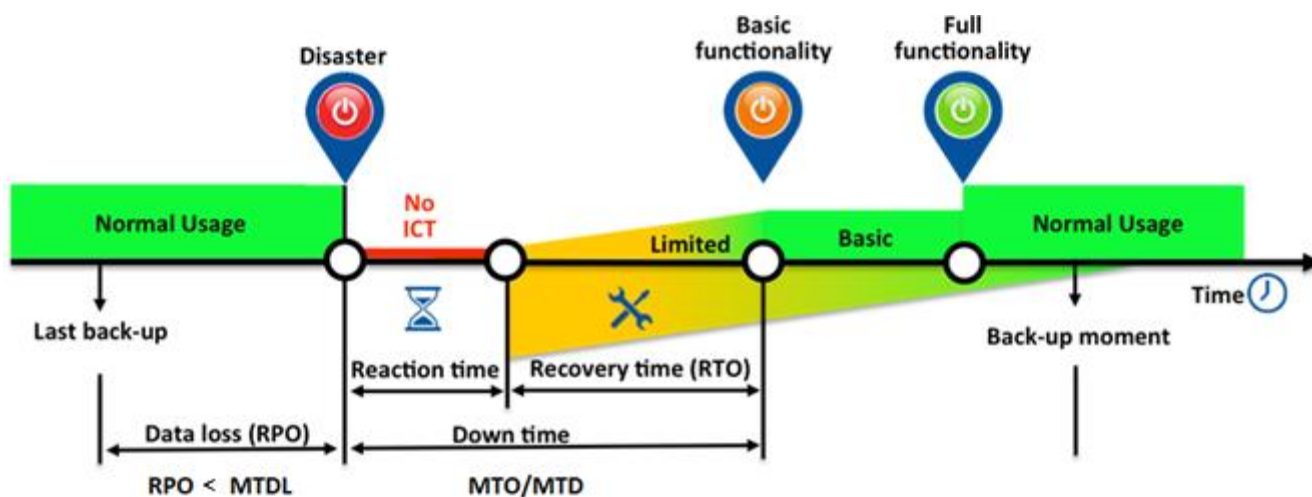
BIA proces (vstupy, zpracování, výstupy)



Parametry nezbytné pro zajištění kontinuity činností IS na časové ose



Vyjádření limitované, minimální a standardní úrovně poskytování služeb



Čas versus náklady

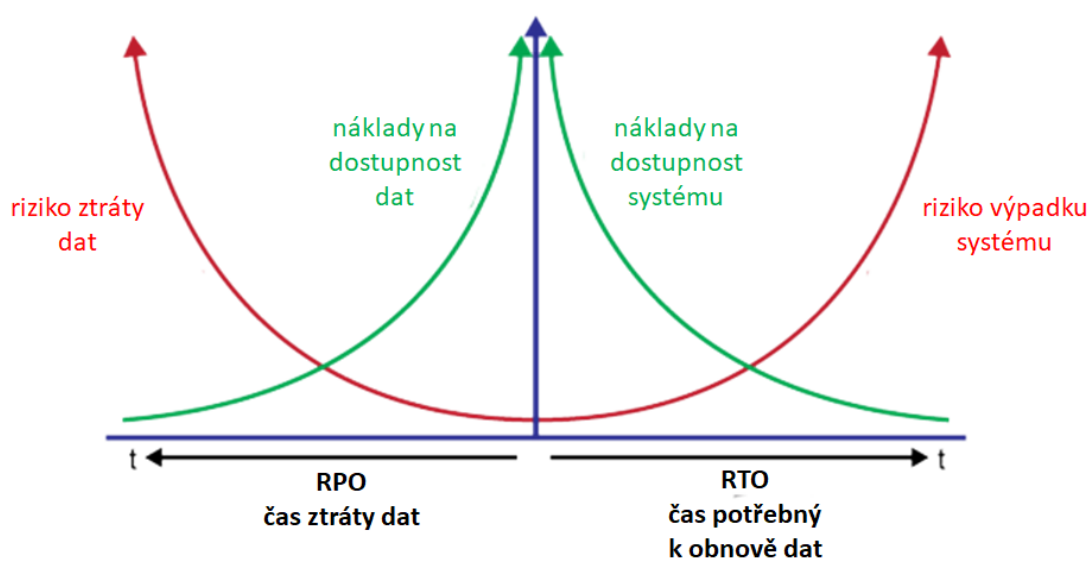
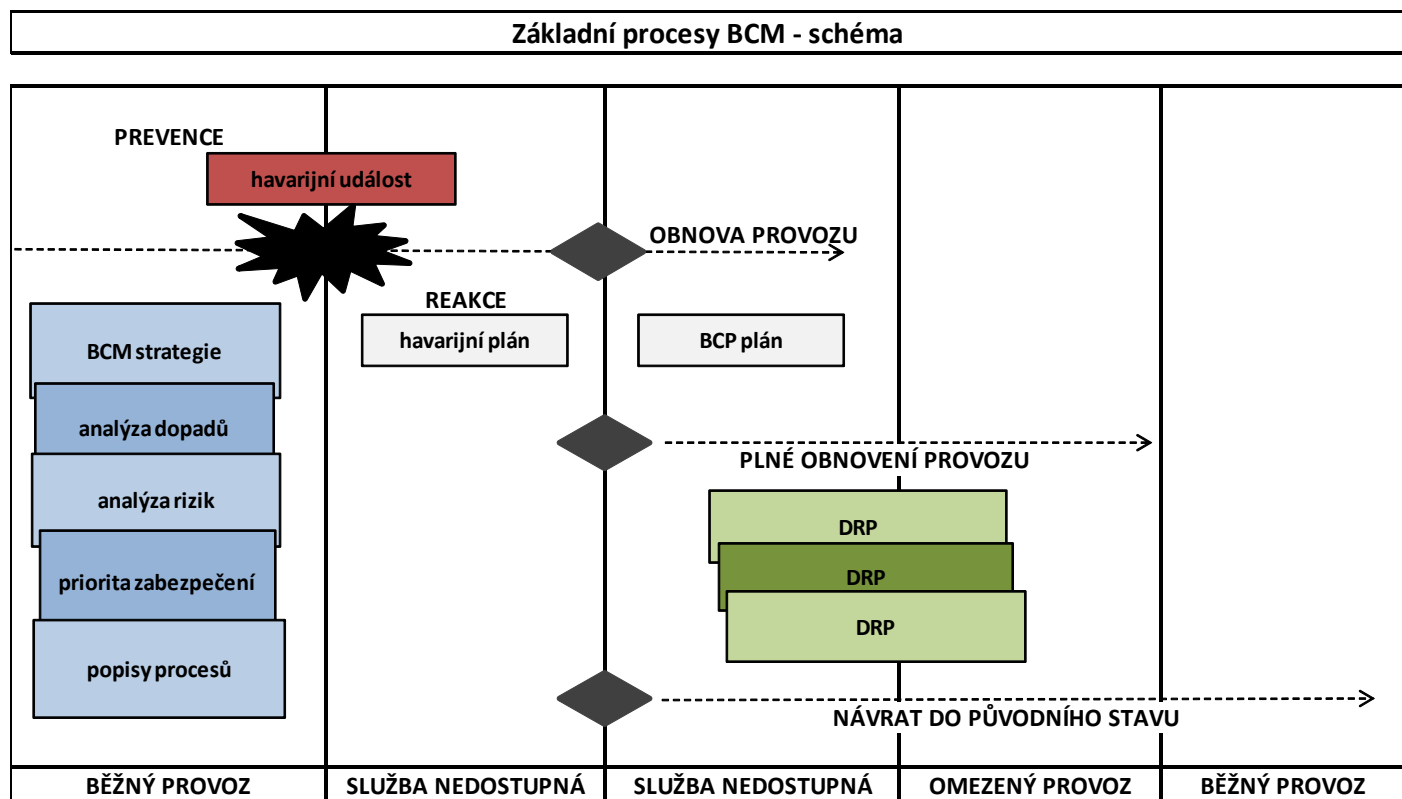


Schéma základních procesů BCM



Výňatek z ČSN EN ISO 22301-2020

Bezpečnost a odolnost — Systémy managementu kontinuity podnikání — Požadavky

Tento dokument specifikuje strukturu a požadavky pro implementaci a udržování systému managementu kontinuity podnikání (BCMS³), jež organizace může nebo nemusí po narušení přijmout. BCMS rozvíjí kontinuitu podnikání přiměřeně velikosti a typu následků.

Výstupy udržování BCMS jsou formovány právními, správními, organizačními a průmyslovými požadavky organizace, poskytovanými produkty a službami, použitými procesy, velikostí a strukturou organizace a požadavky jejích zainteresovaných stran.

8.4.4.1 Organizace musí dokumentovat a udržovat plány a postupy kontinuity podnikání. Plány kontinuity podnikání musí poskytovat pokyny a informace, které pomáhají týmům reagovat na narušení a pomáhají organizaci s reakcí a zotavením.

8.4.4.2 Plány kontinuity podnikání musí souhrnně obsahovat

a) podrobnosti o opatřeních, která týmy podniknou,

tak aby

- 1) prioritní činnosti pokračovaly nebo byly obnoveny v předem stanovených časových rámcích;
- 2) sledovaly dopad narušení a reakce organizace na něj;
- b) odkaz na předem definovanou prahovou hodnotu (hodnoty) a postup pro aktivaci reakce;
- c) postup umožňující dodávku produktů a služeb v dohodnuté kapacitě;
- d) podrobnosti o řízení bezprostředních následků narušení a uložení povinností s ohledem na
 - 1) prospěch jednotlivců;
 - 2) prevenci další ztráty nebo nedostupnost prioritních činností;
 - 3) dopad na životní prostředí.

8.4.4.3 Každý plán musí zahrnovat

- a) účel, rozsah a cíle;
- b) role a odpovědnosti týmu, který bude plán implementovat;
- c) opatření k implementování řešení;
- d) podpůrné informace potřebné pro aktivaci (včetně aktivačních kritérií), provozování, koordinaci a komunikaci opatření týmu;
- e) interní a externí vzájemné závislosti;
- f) požadavky na zdroje;
- g) požadavky na reporting;
- h) proces odstavení.

Každý plán musí být v případě potřeby použitelný a dostupný v jakémkoli čase a na jakémkoli místě.

³ BCMS – Business Continuity Management System – Systém řízení kontinuity činností

ZoKB – vybrané pasáže vztažené ke kontinuitě činností

HLAVA II

SYSTÉM ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

Bezpečnostní opatření

§ 4

(1) Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a **dostupnosti a spolehlivosti** služeb a sítí elektronických komunikací v kybernetickém prostoru.

§ 5

(1) Bezpečnostními opatřeními jsou

- a) organizační opatření a
- b) technická opatření.

(2) Organizačními opatřeními jsou

- 1) **řízení kontinuity činností**

VyKB – vybrané pasáže vztažené ke kontinuitě činností

§ 4

Řízení aktiv

(1) Povinná osoba v rámci řízení aktiv

e) hodnotí a eviduje primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní.

§ 15

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

- a) stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
- b) pomocí hodnocení rizik a analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika související s ohrožením kontinuity činností,
- c) na základě výstupů hodnocení rizik a analýzy dopadů podle písmene b) stanoví cíle řízení kontinuity činností formou určení
 1. minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,
 2. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému, a
 3. bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
- d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c),
- e) vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a havarijní plány související s provozováním informačního a komunikačního systému a souvisejících služeb a
- f) realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti a vychází při tom z požadavků podle § 27.

§ 27

Zajišťování úrovně dostupnosti informací

Povinná osoba zavede opatření pro zajišťování úrovně dostupnosti, kterými zajistí

- a) dostupnost informačního a komunikačního systému pro splnění cílů podle § 15,
- b) odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost,
- c) dostupnost důležitých technických aktiv informačního a komunikačního systému a
- d) redundanci aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému.

Příloha č. 1 k vyhlášce č. 82/2018 Sb.

Hodnocení aktiv

Tab. 3: Stupnice pro hodnocení dostupnosti

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

B - Praktická část

10 Input 1 - Právní normy

10.1 Hierarchie právních norem podle právní síly

Společnost Copy&Print s.r.o. je zřízena na území České republiky. Na tomto území existují platné zákonné normy, které jsou součástí běžného života každého státního útvaru.

10.1.1 Právní normy jsou hierarchicky členěny podle právní síly. Zde uvedené typy právních norem spojte spojnicí od norem s nejvyšší právní silou po nejnižší s níže umístěnou pyramidou:

Čas na zpracování odpovědi: 15'



10.2 Zákony ČR a právo EU

10.2.1 Proč jsou zákony ČR ovlivněny právními akty EU?

Čas na zpracování odpovědi: 15‘

ČR je součástí EU.

Ústavní zákon č. 1/1993 Sb., Ústava České republiky

Čl. 1

(2) Česká republika dodržuje závazky, které pro ni vyplývají z mezinárodního práva.

Čl. 10

Vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, jsou součástí právního řádu; stanoví-li mezinárodní smlouva něco jiného než zákon, použije se mezinárodní smlouva.

Viz hierarchie právních hodnot podle právní síly... 4 – mezinárodní smlouvy a až pod tím 5 – zákony.

10.2.2 Jaké typy EU právních aktů ovlivnily ZoKB, VyKB a OOÚ?

Čas na zpracování odpovědi: 15‘

A. Nařízení – je od data účinnosti závazné pro členské státy EU.

Příklad:

OOÚ

GDPR - NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

KB

CSA - Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

B. Směrnice – je transponována do zákonných norem členských států EU.

Příklad:

KB

NIS1⁴ -> novelizace jak ZoKB, tak i VyKB.

⁴ NIS1 - Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

11 Input 2 – Vybrané pasáže ze ZoKB, VyKB a příslušné normy vzhledem k BCMS

11.1 ZoKB

11.1.1 Definujte pojem „bezpečnostní opatření“ s uvedením čísla paragrafu.

Čas na zpracování odpovědi: 5‘

HLAVA II

SYSTÉM ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

Bezpečnostní opatření

§ 4

(1) Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a *dostupnosti a spolehlivosti* služeb a sítí elektronických komunikací v kybernetickém prostoru.

11.1.2 Uveďte, jak jsou bezpečnostní opatření rozdělena

Čas na zpracování odpovědi: 5‘

§ 5

(1) Bezpečnostními opatřeními jsou

- a) organizační opatření a
- b) technická opatření.

11.1.3 Jaká organizační opatření směřují ke kontinuitě činností?

Uveďte paragraf, odstavec, písmeno

Čas na zpracování odpovědi: 5‘

§ 5

(2) Organizačními opatřeními jsou

- 1) *řízení kontinuity činností*

11.2 VyKB

11.2.1 Jaký paragraf, odstavec a písmeno v rámci řízení aktiv u těchto hodnotí i jejich dostupnost?

Čas na zpracování odpovědi: 5‘

§ 4

Řízení aktiv

(1) Povinná osoba v rámci řízení aktiv

e) hodnotí a eviduje primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní.

11.2.2 Vyjmenujte cíle řízení kontinuity činností

Čas na zpracování odpovědi: 10‘

§ 15

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

b) stanoví cíle řízení kontinuity činností formou určení

1. minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,
2. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému, a
3. bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,

11.2.3 Uved'te hodnoty a označení úrovní u stupnice pro hodnocení dostupnosti

Čas na zpracování odpovědi: 5‘

- 1 – Nízká
- 2 – Střední
- 3 – Vysoká
- 4 – Kritická

11.3 ČSN EN ISO 22301

11.3.1 Specifikujte význam pojmu BCMS

Čas na zpracování odpovědi: 10‘

Tento dokument specifikuje strukturu a požadavky pro implementaci a udržování systému managementu kontinuity podnikání (BCMS), jež organizace může nebo nemusí po narušení přijmout. BCMS rozvíjí kontinuitu podnikání přiměřeně velikosti a typu následků.

Výstupy udržování BCMS jsou formovány právními, správními, organizačními a průmyslovými požadavky organizace, poskytovanými produkty a službami, použitými procesy, velikostí a strukturou organizace a požadavky jejich zainteresovaných stran.

11.3.2 Co musí plány kontinuity podnikání souhrnně obsahovat?

Čas na zpracování odpovědi: 10‘

8.4.4.2 Plány kontinuity podnikání musí souhrnně obsahovat

- a) podrobnosti o opatřeních, která týmy podniknou, tak aby
 - 1) prioritní činnosti pokračovaly nebo byly obnoveny v předem stanovených časových rámcích;
 - 2) sledovaly dopad narušení a reakce organizace na něj;
 - b) odkaz na předem definovanou prahovou hodnotu (hodnoty) a postup pro aktivaci reakce;
 - c) postup umožňující dodávku produktů a služeb v dohodnuté kapacitě;
 - d) podrobnosti o řízení bezprostředních následků narušení a uložení povinností s ohledem na
 - 1) prospěch jednotlivců;

- 2) prevenci další ztráty nebo nedostupnost prioritních činností;
- 3) dopad na životní prostředí.

11.3.3 Co musí každý plán kontinuity podnikání obsahovat a kdy a kde musí být k dispozici?

Čas na zpracování odpovědi: 10‘

8.4.4.3 Každý plán musí zahrnovat

- a) účel, rozsah a cíle;
- b) role a odpovědnosti týmu, který bude plán implementovat;
- c) opatření k implementování řešení;
- d) podpůrné informace potřebné pro aktivaci (včetně aktivačních kritérií), provozování, koordinaci a komunikaci opatření týmu;
- e) interní a externí vzájemné závislosti;
- f) požadavky na zdroje;
- g) požadavky na reporting;
- h) proces odstavení.

Každý plán musí být v případě potřeby použitelný a dostupný v jakémkoli čase a na jakémkoli místě, kde je to požadováno.

12 INPUT 3 BCMS

12.1 Pojmy z oblasti BCMS

12.1.1 Popište níže uvedené zkratky – anglický název a český ekvivalent

Čas na zpracování odpovědi: 20‘

- BCMS
Business Continuity Management System – Systém řízení kontinuity činností
- BCP
Business Continuity Plan – Plán kontinuity činností
- DRP
Disaster Recovery Plan – Plán obnovy činností
- BIA
Business Impact Analysis – Analýza dopadu na podnikání
- RA
Risk Assessment – Posouzení rizik
- RPO
Recovery Point Objective – Cíl bodu obnovy činností
- RTO
Recovery Time Objective - Cíl doby obnovy činností
- WRT
Workout Recovery Time – Čas kontrolních činností po obnově
- MTO/MTD
Maximum Tolerable Outage/Maximum Tolerable Downtime – Přípustný maximální čas odstávky.
- SLA
Service Level Agreement – Úroveň poskytovaných služeb
- MRSL
Minimum Required Service Level – Minimální úroveň poskytovaných služeb
- MTDL
Maximum Tolerable Data Loss – Maximální přípustná ztráta dat.

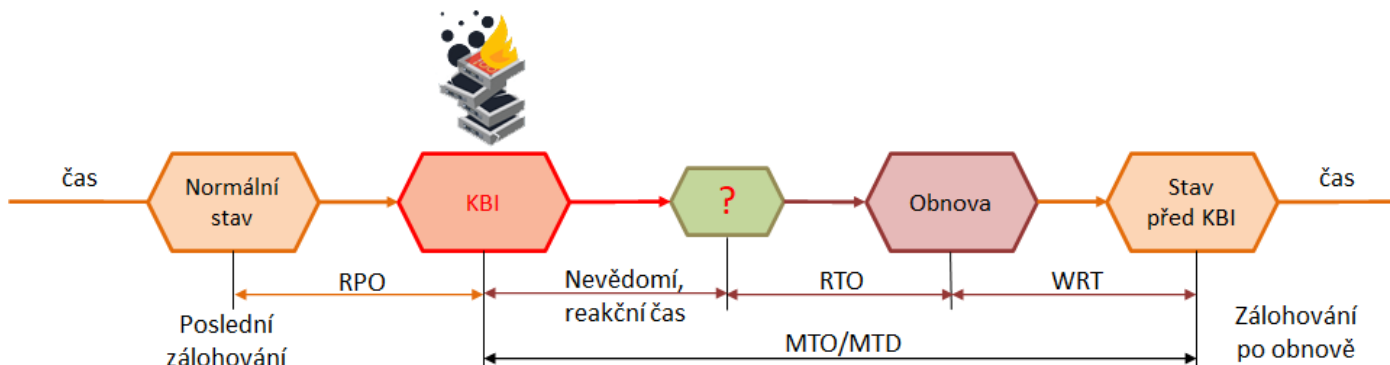
12.1.2 Popište význam BIA

Čas na zpracování odpovědi: 10‘

BIA kvantifikuje dopady přerušení na poskytování služeb, rizika pro poskytování služeb a cíle doby obnovy (RTO) a cíle bodů obnovy (RPO). Tyto požadavky na obnovu se pak používají k vývoji strategií, řešení a plánů.

12.1.3 Na níže uvedené ose doplňte příslušné parametry

Čas na zpracování odpovědi: 15'



12.1.4 Uveďte a zdůvodněte vztah parametrů RPO – MTDL, RTO – MTD

Čas na zpracování odpovědi: 10'

$RTO < MTD$

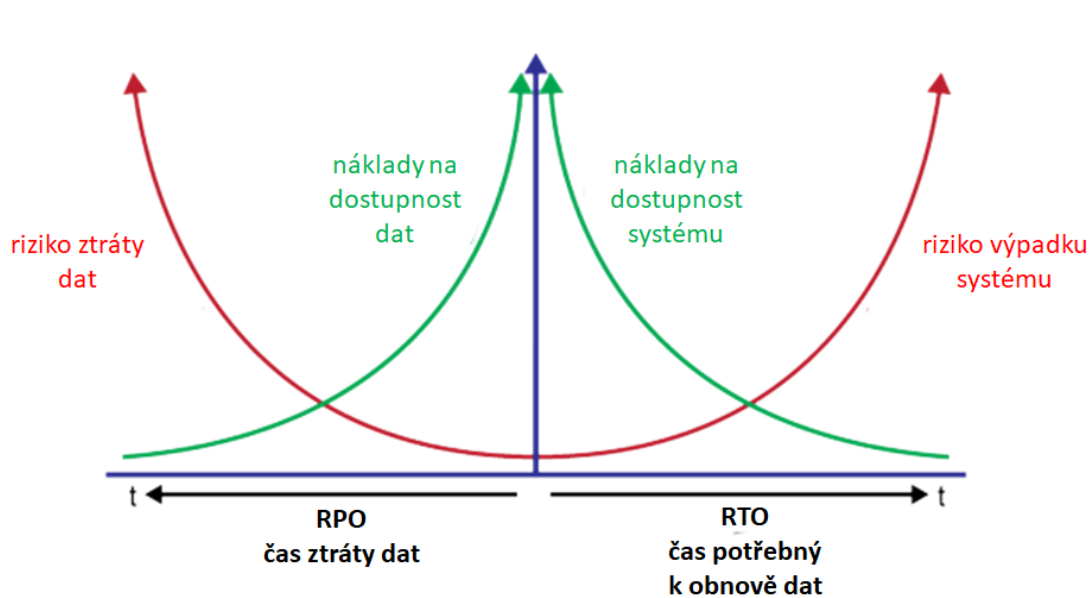
Cíl doby obnovy činností nesmí zahrnout vyšší čas nežli přípustná doba odstávky.

$RPO < MTDL$

Cíl bodu obnovy činností nesmí zahrnout delší čas, než je maximální přípustná ztráta dat (časově).

12.1.5 Graficky vyjádřete vztah RPO a nákladů na dostupnost dat, s uvedením rizika ztráty dat a RTO a nákladů na dostupnost systému s uvedením rizik výpadku systému

Čas na zpracování odpovědi: 10'

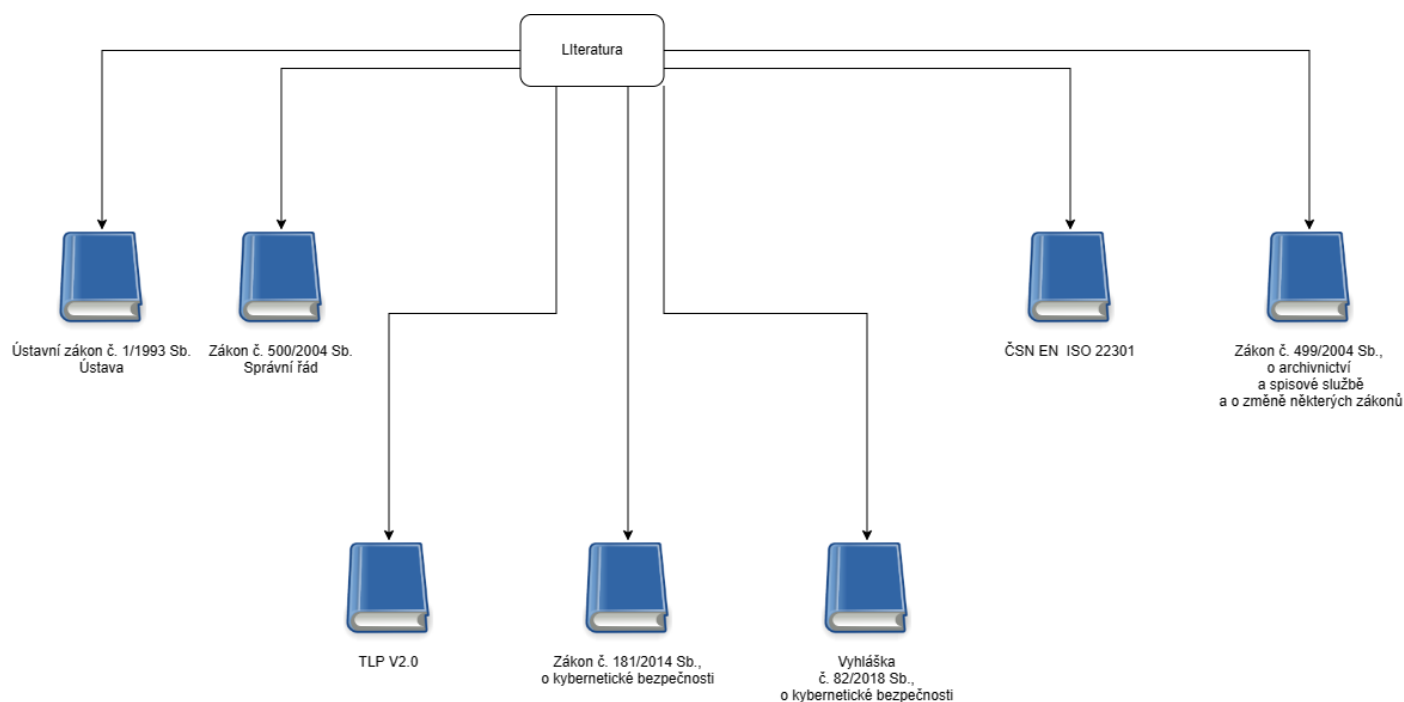


Shrnutí a závěr

Po absolvování tohoto cvičení budou studenti schopni:

- Pochopit důležitost a smysl hierarchie právních norem podle právní síly s vazbou na interní předpisy v jakékoli organizaci.
- Pochopit strukturu právních předpisů.
- Pochopit způsoby aplikace práva EU do legislativy ČR.
- Pochopit pojmy a vztahy v rámci BCMS.
- Prakticky ověřit, že pro každou právnickou osobu je nezbytné z pohledu jejího fungování zajištění jak provozních/technologických, tak i procesních aspektů s vazbou na lidský faktor, ale taktéž i zajištění bezpečnostní vrstvy ve smyslu zajištění informační a kybernetické bezpečnosti a kontinuity byznysu.

Seznam použitých zdrojů



Odkazy na použité zákonné předpisy:

Zákonné předpisy a standardy

- Zákony pro lidi

<https://www.zakonyprolidi.cz>

- Ústava ČR - ústavní zákon č. 1/1993 Sb.
<https://www.zakonyprolidi.cz/cs/1993-1>
- Zákon č. 372/2011 Sb., zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
<https://www.zakonyprolidi.cz/cs/2011-372>
- Zákon č. 500/2004 Sb., správní řád
<https://www.zakonyprolidi.cz/cs/2004-500>
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
 - <https://www.zakonyprolidi.cz/cs/2014-181>
 - <https://www.zakonyprolidi.cz/cs/2017-205>
 - <https://www.zakonyprolidi.cz/cs/2022-226>
- Zákon č. 205/2017 Sb., zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony
 - <https://www.zakonyprolidi.cz/cs/2017-205>
- Zákon č. 226/2022 Sb., zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
 - <https://www.zakonyprolidi.cz/cs/2022-226>

- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
 - <https://www.zakonyprolidi.cz/cs/2018-82>
- ČSN EN ISO 22301 Bezpečnost a odolnost - Systémy managementu kontinuity podnikání - Požadavky

Úřad - NÚKIB

- Web Úřadu - NÚKIB: <https://www.nukib.cz/>
- Doporučení NÚKIB: <https://www.nukib.cz/cs/infoservis/doporuceni/>
- TLP: <https://www.nukib.cz/cs/infoservis/doporuceni/1862-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci-2/>
- Podpůrné materiály:
 - <https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>
 - https://www.nukib.cz/download/publikace/podpurne_materialy/ZKB_blokove_schema.pdf
 - https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_povinnosti.pdf
 - https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_lhuty.pdf
 - https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_rozhodovani_PZS_v2.1.pdf
 - https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_PZS.pdf
 - https://www.nukib.cz/download/publikace/podpurne_materialy/Neprimerene-naklady_v2.1.pdf
- Výkladový slovník kybernetické bezpečnosti: https://www.nukib.cz/download/publikace/podpurne_materialy/vykladovy_slovník_KB_3_vydani.pdf

EU

- **Typy právních aktů EU:** https://ec.europa.eu/info/law/law-making-process/types-eu-law_cs
- **CSA:** <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32019R0881&from=CS>
- **NIS1:** <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016L1148&from=cs>

GDPR:

- <https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32016R0679>

Použitá literatura:

ČADOVÁ, Barbara, Jana PETRŽELOVÁ a Miroslava ČERMÁKOVÁ. *Maturitní otázky -občanský a společenskovední základ*. 1. vyd. Fragment, 2008, 224 s. ISBN 978-80-253-0600-0.

Důvěrnost informací v souladu s TLP 2.0

Barva

Podmínky použití

TLP:RED

Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.

TLP:AMBER

Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta.

TLP:AMBER+STRICT

Informace je sdílena pouze s organizací.

TLP:GREEN

Informace může být sdílena v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.

TLP:CLEAR

Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Příklady použití:

TLP:RED – Od zahraničních partnerů jsme získali informaci, že útočník má přístup do vaší sítě a plánuje spustit ransomware útok. Doporučujeme tedy provést následující protiopatření...

TLP:AMBER – Z našich zjištění vyplývá, že je ve vaší síti používána zranitelná verze firewallu. Doporučujeme co nejdříve provést jeho aktualizaci. Tuto informaci můžete předat správci nebo dodavateli FW.

TLP:AMBER+STRICT – Z našich zjištění vyplývá, že je ve vaší síti používána zranitelná verze firewallu. Doporučujeme co nejdříve provést jeho aktualizaci. Tuto informaci je možné předat pouze v rozsahu vaší organizace.

TLP:GREEN – V České republice nyní probíhá phishing kampaň zaměřující se na zdravotnická zařízení, poučte své uživatele na možná rizika.

TLP:CLEAR – GovCERT.CZ za poslední rok řešil 126 incidentů, z toho 26 závažných.

Pro více informací o protokolu sledujte oficiální stránky FIRST: <https://www.first.org/tlp/>