Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Plánovanie kontinuity činností

Michal Bubák

KPMG
cutting through complexity™

Agenda

- Pojmy, ciele a terminológia
- Procesný cyklus BCM
  - Riadenie BCM
  - Ohodnotenie
  - Plánovanie
  - Implementácia
  - Monitorovanie
- Požiadavky na plánovanie kontinuity činnosti v legislatívnych aktoch SR a medzinárodných štandardoch

Základné pojmy

Plánovanie kontinuity činností - Business continuity planning
Business continuity management (BCM)

Proces podporovaný vedením organizácie, ktorý identifikuje potenciálne dopady a ktorého cieľom je vytvoriť také postupy a prostredie, ktoré umožní zabezpečiť kontinuitu a obnovu kritických procesov a činností organizácie na vopred stanovenú úroveň v prípade ich narušenia alebo straty.

Nosnou aktivitou je príprava, implementácia a udržiavanie plánov kontinuity činností a plánov obnovy.

Prečo sa zaoberať s BCM?

- **Dostupnosť** IKT je jedna zo základných požiadaviek IB.
- Možnosti narušenia dostupnosti IKT a následne aj procesov organizácie sú veľmi široké (požiar, povodeň, epidémia, krádež, terorizmus).
- Možnosti organizácie zamedziť výskytu takýchto udalostí sú obmedzené.
- Potenciálne následky sú katastrofálne.

Východiskový stav

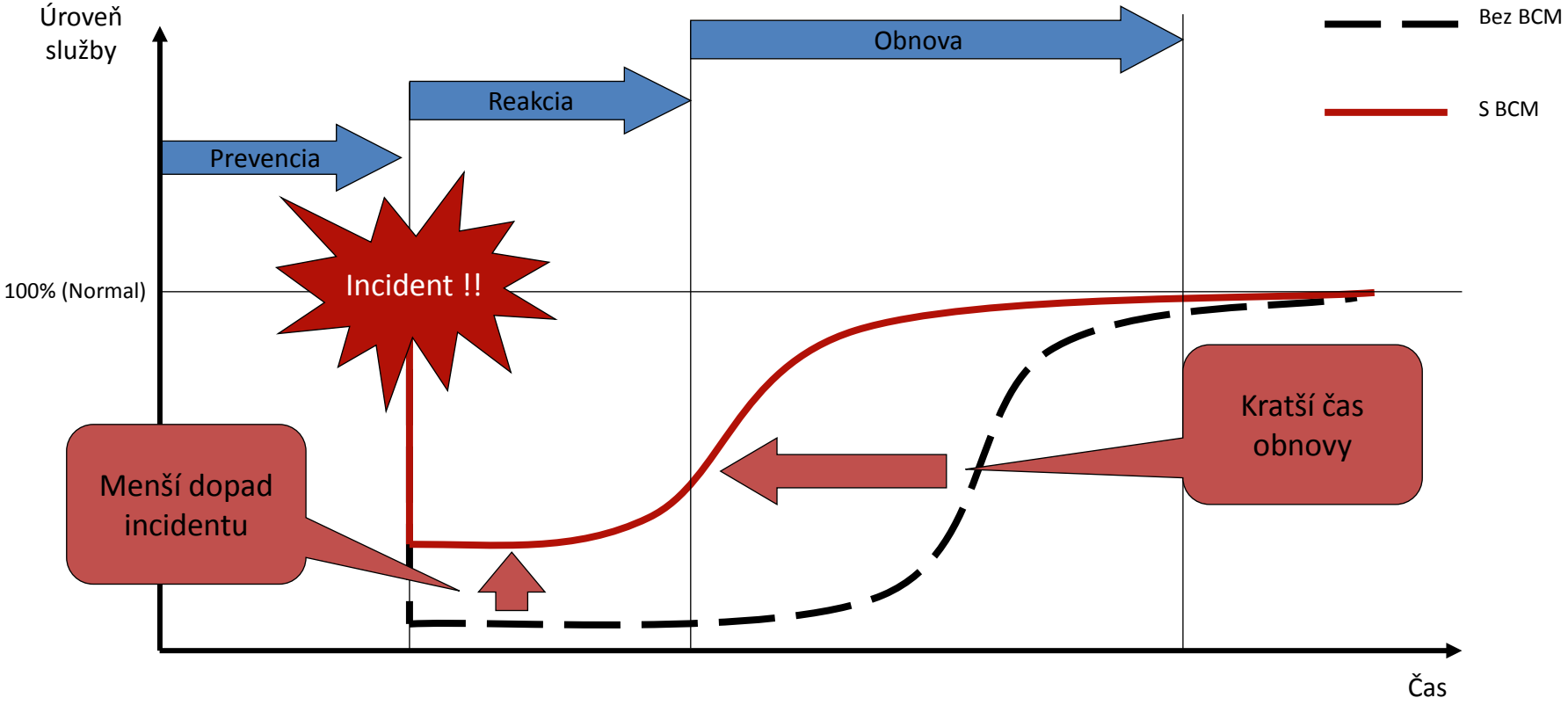
Pred výskytom incidentu

- Pravidelné zálohovanie údajov
- Ukladanie záloh v inej geografickej lokalite
- Dohody s dodávateľmi hardvéru
- Dohody o podpore s dodávateľmi aplikácií
- Ďalšie špecifické prípravné opatrenia väčšinou **absentujú**

Po výskyte incidentu

- Obnova údajov zo zálohy (ak sú dostupné dáta a infraštruktúra)
- Pri zložitejších úkonoch obnovy sa predlžuje doba obnovy
- Pri incidente väčšieho rozsahu môže byť problém s prioritizáciou obnovy

Prínosy BCM


Úroveň služby
Bez BCM
S BCM
Obnova
Reakcia
Prevencia
Incident !!
100% (Normal)
Menší dopad incidentu
Kratší čas obnovy
Čas

Terminológia 1/3

Plán kontinuity činností - Business Continuity Plan (BCP)

Sada dokumentovaných postupov a informácií, ktoré sú pripravené a udržiavané aktuálne pre použitie v prípade výskytu incidentu a ktoré umožnia organizácii obnovu a prevádzku **kritických aktivít** na akceptovateľnej preddefinovanej úrovni.

Plán obnovy - Disaster Recovery Plan (DRP)

Sada dokumentovaných postupov a informácií, ktoré sú pripravené a udržiavané aktuálne pre použitie v prípade výskytu incidentu a ktoré umožnia organizácii obnovu a prevádzku **zdroja/prostriedku**, ktorý je využívaný kritickým procesom.

Terminológia 2/3

Maximálna doba výpadku – Maximum tolerable outage (MTO)
Maximum tolerable period of disruption (MTPD)

Najdlhšia možná doba výpadku procesov alebo služieb organizácie, po ktorej uplynutí nastanú pre organizáciu neakceptovateľné dopady.

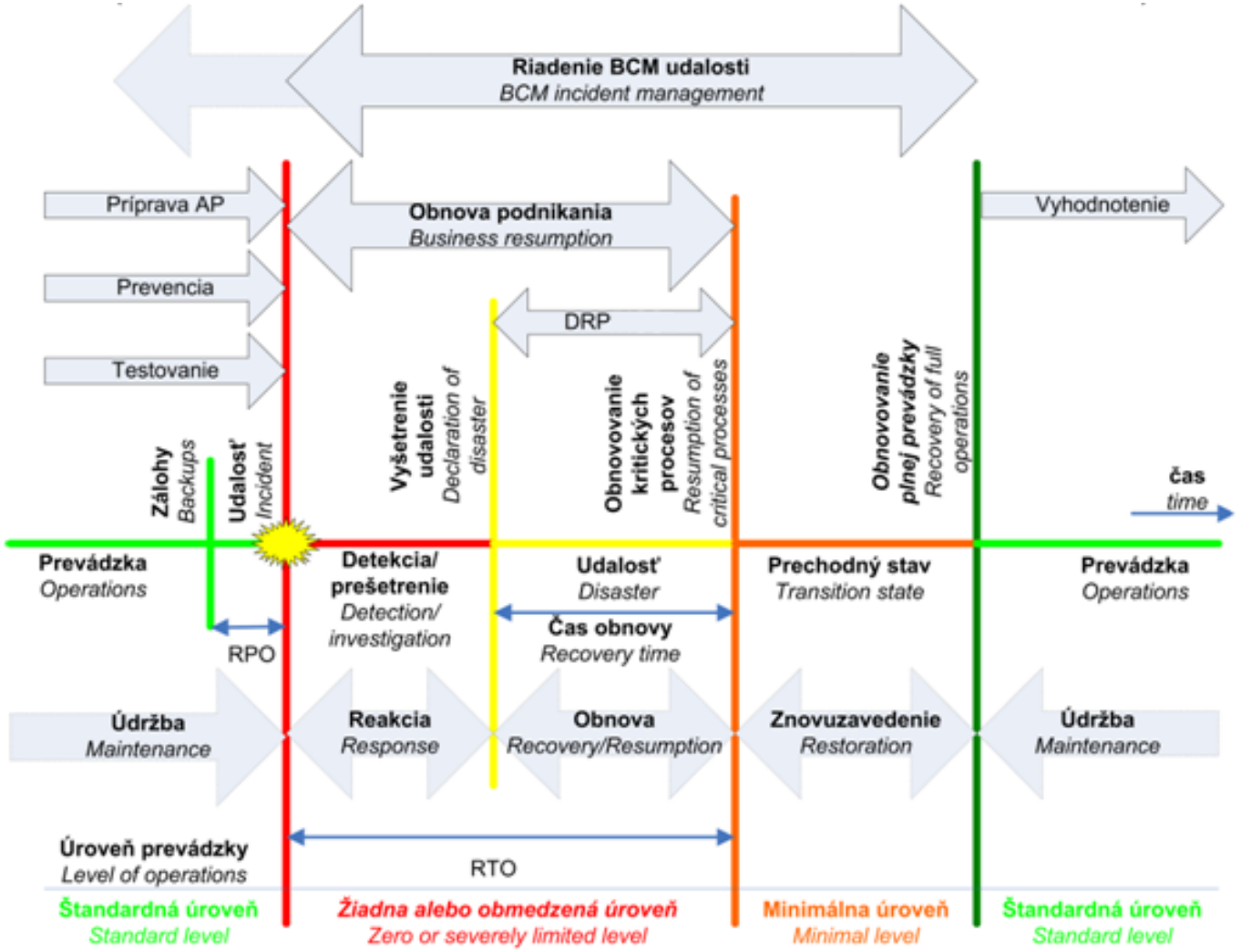
Cieľový čas obnovenia - Recovery Time Objective (RTO)

Maximálny prípustný čas pre obnovenie procesu alebo služby po jej prerušení. Poskytovaná úroveň môže byť nižšia, ako je normálna cieľová úroveň.

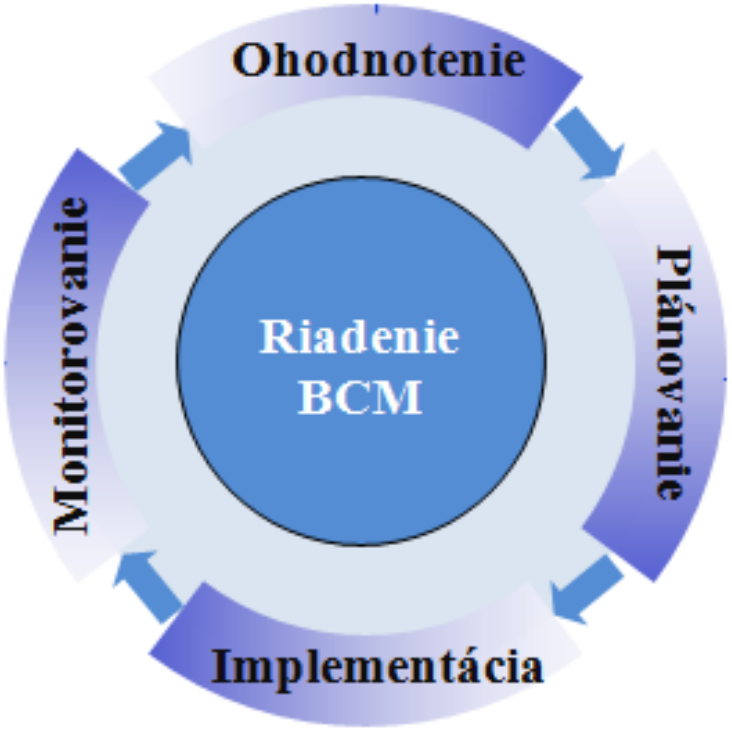
Cieľový bod obnovenia - Recovery Point Objective (RPO)

Maximálne množstvo dát, ktoré môže byť stratené, kým je proces alebo služba obnovená po jej prerušení. Je vyjadrený ako dĺžka času pred výpadkom.

Terminológia 3/3



Procesný cyklus BCM



Fáza 0 – Riadenie BCM
- Organizačný rámec
- Základné dokumenty – Politika, Metodika

Fáza 1 – Ohodnotenie
- Analýza rizík, analýza dopadov
- Určenie priorít a závislostí

Fáza 2 – Plánovanie
- Výber opatrení na zabezpečenie kontinuity a obnovy

Fáza 3 - Implementácia
- Zavádzanie opatrení
- Príprava akčných plánov (BCP a DRP)
- Školenia

Fáza 4 - Monitorovanie
- Testovanie a udržiavanie pripravenosti organizácie zabezpečiť kontinuitu a obnovu

Fáza 0 - Riadenie BCM 1/2

Organizačné zabezpečenie – roly a zodpovednosti

- Vedenie organizácie/Komisia pre IB
- Manažér informačnej bezpečnosti (BCM Koordinátor)
- Vlastníci procesov
- Správcovia prostriedkov a zdrojov
- Audit

Školenia a povedomie

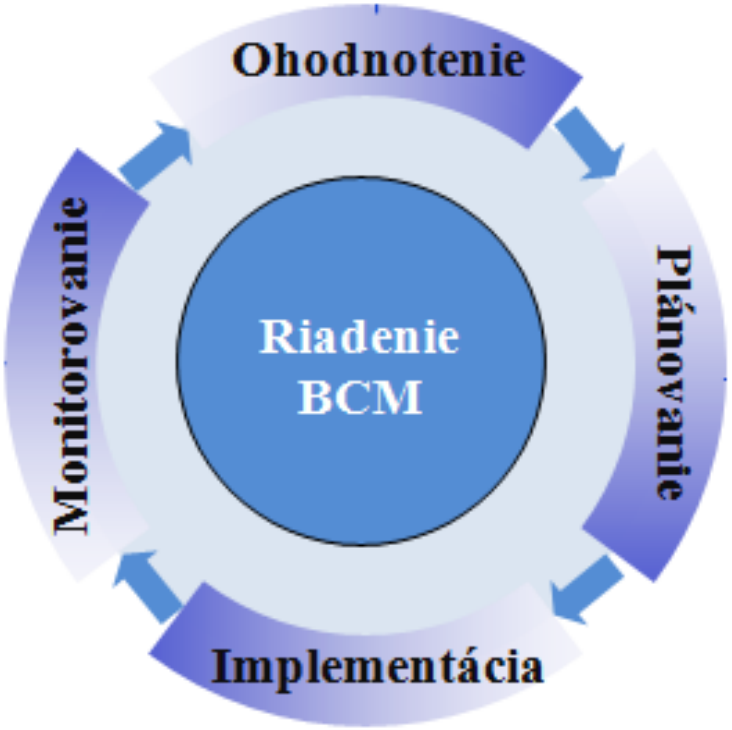
Fáza 0 - Riadenie BCM 2/2

BCM dokumenty

- Formalizujú BCM v organizácii
- Východiskom je **bezpečnostná politika** organizácie
- Politika BCM
  - Ciele v oblasti BCM
  - Záväzok vedenia organizácie
  - **Rozsah**
  - **Definícia rolí a zodpovedností**

- Metodika BCM
  - Konkrétne postupy realizácie BCM procesov
  - Spôsob prípravy akčných plánov
  - Spôsob testovania akčných plánov

Procesný cyklus BCM



Fáza 0 – Riadenie BCM
- Organizačný rámec
- Základné dokumenty – Politika, Metodika

Fáza 1 – Ohodnotenie
- Analýza rizík, analýza dopadov
- Určenie priorít a závislostí

Fáza 2 – Plánovanie
- Výber opatrení na zabezpečenie kontinuity a obnovy

Fáza 3 - Implementácia
- Zavádzanie opatrení
- Príprava akčných plánov (BCP a DRP)
- Školenia

Fáza 4 - Monitorovanie
- Testovanie a udržiavanie pripravenosti organizácie zabezpečiť kontinuitu a obnovu

Fáza 1 - Ohodnotenie

Aktivity - Analýza Rizík, Analýza Dopadov (Business Impact Assessment - BIA)

- Identifikácia a popis kritických funkcií a procesov
- Identifikácia závislostí medzi procesmi
- Určenie maximálnej doby výpadku (MTO) procesov a zdrojov
- Definovanie cieľov pre dosiahnutie požadovaného stavu odolnosti (RTO, RPO)
- Identifikácia kritických zdrojov
- Identifikácia hrozieb, zraniteľností a rizík ohrozujúcich dostupnosť
- Určenie priorít

Roly a zodpovednosti

- Manažér IB
- Vlastníci procesov
- Správcovia zdrojov

Analýza rizík - pripomenutie

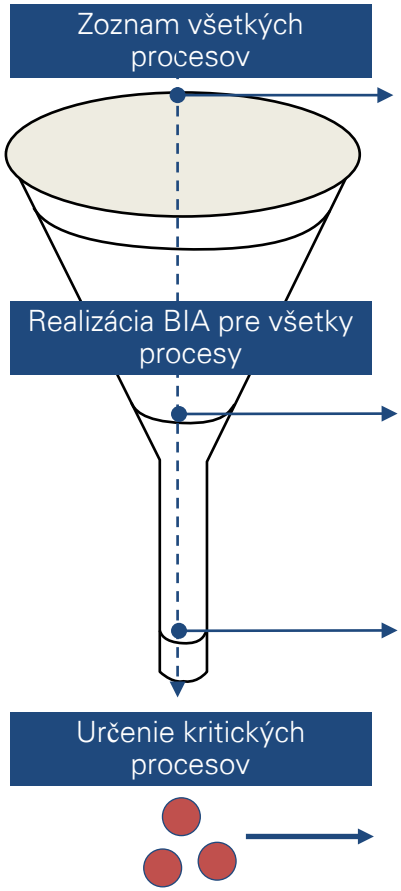
Odhad rizík

Základné prístupy:

- Kvantitatívny (číselné vyjadrenie)
- Kvalitatívny (slovné vyjadrenie)

riziko = pravdepodobnosť * dopad hrozby

Analýza dopadov 1/7



- Krok 1.
- **Získať údaje o procese (biznis kontext)**

- Krok 2.
- **Určiť dopady pri nedostupnosti procesu:**
  - Reputačné
  - Prevádzkové
  - Právne
  - Finančné

- Krok 3.
- **Prioritizácia procesov**

- Krok 4.
- **Určenie MTO procesov**

Analýza dopadov 2/7

Príprava zoznamu procesov a určenie vlastníctva procesov

- Identifikácia činností, ktoré organizácia realizuje na plnenie svojho poslania (procesov) a informácií spracovávaných v rámci procesov

- Vlastník procesu je osoba, ktorá má konečnú zodpovednosť za vykonávanie procesu a zároveň určuje spôsob vykonávania procesu

- Východiská - organizačná štruktúra a organizačný poriadok

Analýza dopadov 3/7

Ohodnotenie dopadov

Kľúčový element – časové rozsahy

Časové rozsahy výpadku narastajú od momentu výpadku

Musia byť prispôsobené podľa potrieb spoločnosti

	Časové rozsahy							
	0 h – 0.5 h	0.5 h – 2 h	2 h – 4 h	4 h – 8 h	8 h – 1 Deň	1 Deň – 5 Dní	5 Dní– 14 Dní	Viac ako 14 Dní
Dopad	Nízky	Nízky	Nízky	Stredný	Stredný	Stredný	Vysoký	Vysoký

Analýza dopadov 4/7

Hodnota	Popis dopadu	Prevádzkový dopad	Legislatívny dopad	Finančný dopad (v €)	Reputačný dopad
0	Žiaden dopad	-	-	-	-
1	zanedbateľný vplyv, strata	interne, útvar	disciplinárne konanie	0 - 5 000	interná nespokojnosť v rámci útvaru
2	malý vplyv, strata	interne, viacero útvarov	zmena vnútornej legislatívy	5 000 - 100 000	interná nespokojnosť v rámci viacero útvarov
3	značný vplyv, strata	interne, divízia/časť spoločnosti	začatie správneho konania smerujúce k opatreniu na nápravu (nízka pokuta)	100 000 - 1 000 000	interná nespokojnosť v rámci divízie, nepriaznivá publicita
4	významný vplyv, strata	viac divízií	začatie správneho konania smerujúce k opatreniu na nápravu (vysoká pokuta)	1 000 000 - 5 000 000	národná negatívna publicita
5	katastrofický vplyv, strata	dopad na celú spoločnosť	začatie správneho konania na EÚ úrovni smerujúce k opatreniu na nápravu (vysoká pokuta)	> 5 000 000	medzinárodná negatívna publicita

ILUSTRATÍVNA TABUĽKA DOPADOV

Analýza dopadov 5/7

Identifikácia závislostí medzi procesmi

- Závislosti na iných „biznis“ procesoch
  - Prípadné korekcie na základe závislostí
- Závislosti na podporných procesoch
  - Určenie hodnoty podporných procesov na základe hodnoty „nadradených“ podporovaných procesov

Analýza dopadov 6/7

Určenie MTO, RTO a RPO

Maximálna doba výpadku - Maximum tolerable outage

Najdlhšia možná doba výpadku procesov alebo služieb organizácie, po ktorej uplynutí nastanú pre organizáciu neakceptovateľné dopady.

Cieľový čas obnovenia - Recovery Time Objective

Maximálny prípustný čas pre obnovenie procesu alebo služby po jej prerušení.

Cieľový bod obnovenia - Recovery Point Objective

Maximálne množstvo dát, ktoré môže byť stratené, kým je proces alebo služba obnovená po jej prerušení.

Analýza dopadov 7/7

Identifikácia potrebných zdrojov a prostriedkov, prenesenie hodnôt

Príklady zdrojov a prostriedkov – model aktív

- Aplikácie (informačné systémy)
- Databázy
- Operačné systémy
- Hardvér
- Sieťová infraštruktúra
- Lokality (výpočtové strediská, kancelárske priestory)
- Ľudské zdroje
- Tretie strany (dodávatelia)

Cvičenie

Zadanie: Pripravte a vysvetlite vhodné časové rozsahy a tabuľku dopadov vo Vašej organizácii.

Cvičenie

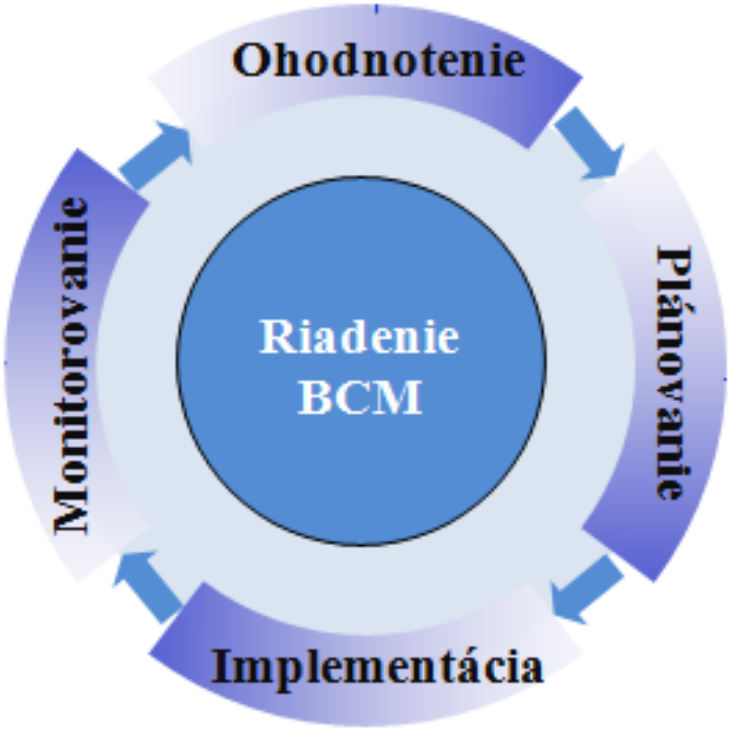
Časové rozsahy

Do	**Od .....** **Do .....**	**Od .....** **Do .....**	**Viac ako .....**

Tabuľka dopadov

Dopad	**Finančný**	**Legislatívny**	**Prevádzkový**	**Reputačný**
Nízky				
Stredný				
Vysoký				

Procesný cyklus BCM



Fáza 0 – Riadenie BCM
- Organizačný rámec
- Základné dokumenty – Politika, Metodika

Fáza 1 – Ohodnotenie
- Analýza rizík, analýza dopadov
- Určenie priorít a závislostí

Fáza 2 – Plánovanie
- Výber opatrení na zabezpečenie kontinuity a obnovy

Fáza 3 - Implementácia
- Zavádzanie opatrení
- Príprava akčných plánov (BCP a DRP)
- Školenia

Fáza 4 - Monitorovanie
- Testovanie a udržiavanie pripravenosti organizácie zabezpečiť kontinuitu a obnovu

Analýza rizík - pripomenutie

Vyhodnotenie/ohodnotenie rizík

- Porovnanie odhadnutej hodnoty rizík s kritériami na ohodnotenie rizík

Ošetrovanie rizík

- Redukcia, Prijatie, Vyhnutie sa, Prenesenie

Fáza 2 - Plánovanie

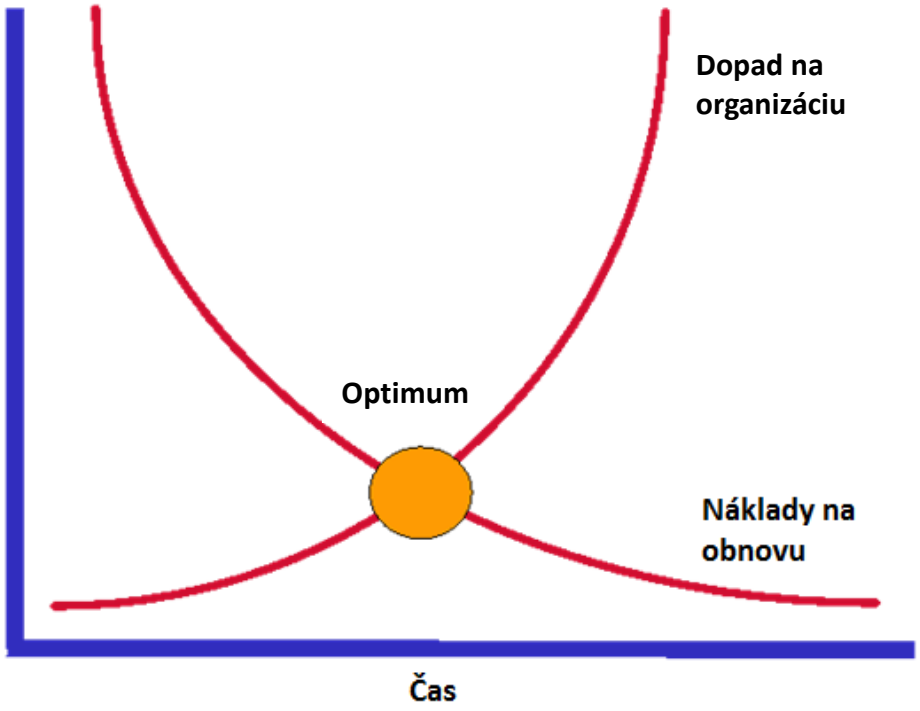
Cieľ: Ošetrovanie rizík, ktorých hodnota prevyšuje akceptovateľnú úroveň a zároveň, pri ktorých sa dopad hrozby prejaví v narušení dostupnosti procesov a činností organizácie.

Možnosti na ošetrovanie rizík v rámci BCM

- redukcia – zavádzanie predovšetkým korekčných opatrení
- prenášanie rizika

Výber vhodných opatrení závisí od **typu aktíva**, na ktorý pôsobí hrozba príslušného rizika a od ekonomickej efektívnosti.

Analýza ekonomickej efektívnosti



Niektoré opatrenia z oblasti BCM ošetrujú viacero individuálnych rizík.

Opatrenia pre IKT prvky a údaje 1/3

Základné opatrenie je pravidelné zálohovanie a následná obnova zo zálohy

Dôležité faktory:

- rozsah zálohovania – určujúce sú závislosti procesov na prostriedkoch
- frekvencia zálohovania – určujúce je RPO
- umiestnenie záloh - určujúca je výška potenciálnych dopadov

Kľúčová je pripravenosť/dostupnosť záložných alebo náhradných IKT prvkov a ich umiestnenie.

Opatrenia pre IKT prvky a údaje 2/3

Varianty pripravenosti záložných IKT prvkov:

- **Postupná obnova** (angl. Cold Site alebo Cold Standby): Dopredu pripravené prenosné alebo trvalé priestory primeranej veľkosti, ktoré majú zavedené napájanie elektrickou energiou a telekomunikačné pripojenie. Inštalácia a konfigurácia hardvéru a softvéru a obnova údajov sa vykoná dodatočne.

- **Strednodobá obnova** (angl. Warm Site alebo Warm Standby): Obsahuje to isté čo predchádzajúci bod, plus navyše nenakonfigurovaný hardvér, softvér a sieťové komponenty. Konfigurácia hardvéru a softvéru a obnova údajov sa vykoná dodatočne.

Opatrenia pre IKT prvky a údaje 3/3

Varianty pripravenosti záložných IKT prvkov:

- **Rýchla obnova** (angl. Hot Site alebo Hot Standby): Navyše oproti predchádzajúcemu bodu obsahuje nakonfigurovaný a pripravený hardvér aj softvér. Potreba obnovy údajov zo zálohy.

- **Riešenia vysokej dostupnosti** (angl. High Availability Clusters): obnova bez akejkoľvek straty služby.) Využíva technológie ako zrkadlenie (angl. mirroring) a rozloženie výkonu na viac prvkov (angl. load balancing)

Opatrenia pre ľudské zdroje 1/3

Ľudské zdroje sú špecifický typ aktíva, keď na jednej strane vykonávajú všetky neautomatizované procesy organizácie a na druhej strane sú nositeľmi schopností a znalostí.

Nedostupnosť ľudských zdrojov môže byť spôsobená udalosťami na úrovni jednotlivcov (choroba, zranenie, smrť) alebo väčších skupín (epidémia), pričom priebeh konkrétneho scenára je veľmi individuálny. Zároveň použiteľnosť jednotlivých opatrení je rôzna pre jednotlivé organizačné jednotky organizácie, respektíve pre jednotlivé osoby.

Je veľmi náročné vybrať jedno správne opatrenie, ktoré pomôže vo všetkých prípadoch. Opatrenia je vhodné kombinovať.

Opatrenia pre ľudské zdroje 2/3

- **Navýšenie počtu pracovníkov oproti skutočným potrebám**: Toto opatrenie umožní vykryť neočakávané výpadky (práceneschopnosť) a zároveň zvyšuje flexibilitu pri plánovaní pracovných úloh.

- **Dokumentácia postupov a znalostí**: Aktuálna a prehľadná dokumentácia pracovných postupov, znalostí a skúseností umožní v prípade výpadku rýchlejší a efektívnejší nástup náhradných ľudských zdrojov.

- **Prekrývajúce sa pracovné pozície**: Rozsah jednotlivých pracovných pozícií nie je izolovaný, ale existujú medzi nimi prieniky. Prípadný výpadok je potom možné vykryť zo zostávajúcich zdrojov.

Opatrenia pre ľudské zdroje 3/3

- **Zastupiteľnosť / Plánovanie nástupníctva:** Na konkrétnu pracovnú pozíciu pripadá viac osôb, ktoré sa v prípade výpadku vedia zastúpiť.

- **Rotácia zamestnancov:** Pravidelnou rotáciou zamestnancov sa docielia širšie znalosti a širší záber jednej osoby, ako je jej aktuálna pozícia. Prípadný výpadok je potom možné vykryť zo zostávajúcich zdrojov, ktoré danú prácu v minulosti vykonávali.

- **Použitie tretích strán:** Ak to dovoľuje povaha prác, jednou z náhradných alternatív sú externí zamestnanci. Pri použití tejto stratégie je odporúčané nájsť vhodného dodávateľa a dohodnúť s ním podmienky vopred. Vzťah s dodávateľom môže byť postavený na kontrakte typu SLA, t.j. je presne stanovená úroveň služby, ktorú musí dodávateľ dodržať.

Opatrenia pre priestory 1/2

Uvedené opatrenia sú zamýšľané pre pracovné priestory, nie pre výpočtové centrá.

- **Práca z domu**: Ak je to technicky realizovateľné a dovoľuje to povaha prác, je možné nariadiť pracovníkom prácu z domu.

- **Alternatívne priestory v rámci organizácie**: Organizácia disponuje niekoľkými lokalitami, ktoré sú od seba geograficky vzdialené a majú voľné kapacity s pripravenými pracovnými priestormi. V prípade nedostupnosti niektorej z lokalít sa pracovníci presunú do druhej lokality podľa poradia priority ich procesov.

Opatrenia pre priestory 2/2

- **Alternatívne priestory poskytnuté treťou stranou**: Organizácia uzavrie dohodu o poskytnutí náhradných pracovných priestorov s treťou stranou. Môže ísť o recipročnú dohodu, kedy poskytovanie priestorov nie je primárnou činnosťou tretej strany a poskytuje ich za prísľub rovnakej pomoci v prípade nedostupnosti jej vlastných priestorov. Druhá možnosť je dohoda na komerčnom základe, keď tretia strana poskytuje alternatívne priestory za odplatu ako svoju primárnu činnosť.

Alternatívne priestory by nemali byť príliš blízko pri hlavných, aby nepodliehali rovnakému riziku a zároveň by nemali byť príliš ďaleko, aby to nesťažovalo presun a logistiku.

Opatrenia pre dodávateľov

Príkladom dodávateľmi poskytovaných služieb môžu byť telekomunikačné služby, vývoj a údržba softvéru, právne poradenstvo, spracovanie miezd a pod.

- **Zvýšenie počtu dodávateľov**: Aktívne využívanie niekoľkých dodávateľov na ten istý druh služby. Pri výpadku jedného dodávateľa sa rozložia dodávky na ostatných.

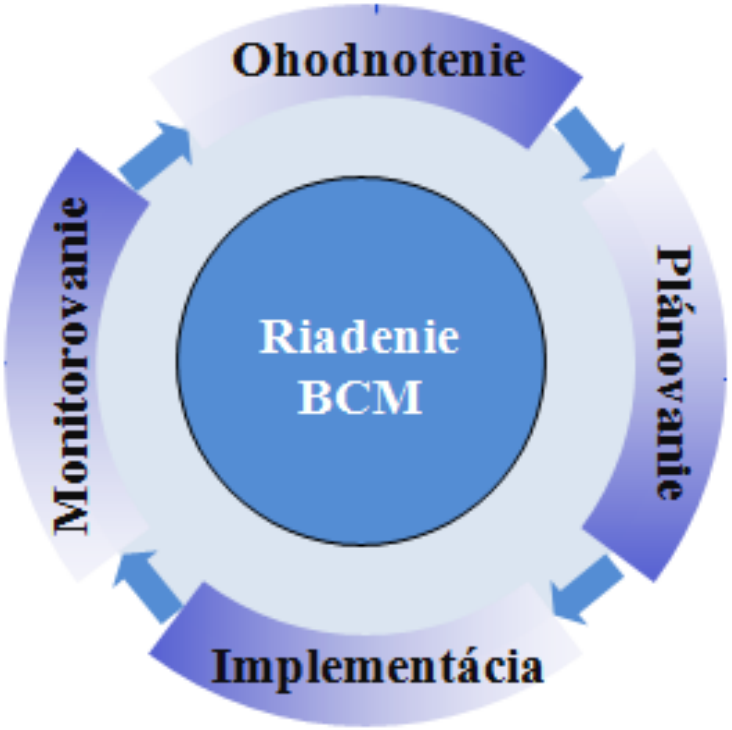
- **Identifikácia vhodných alternatívnych dodávateľov**: Organizácia si vopred vyhľadá vhodných náhradných dodávateľov a prípadne dohodne podmienky dodávky služieb, ktoré využije až v momente výpadku hlavného dodávateľa.

Opatrenia pre dodávateľov

- **Dohody o úrovni poskytovaných služieb (SLA)**: Zaviazanie dodávateľa k dodržaniu stanovených úrovní služieb. Príkladom parametrov môže byť dostupnosť služby v percentách, maximálna doba reakcie na mimoriadnu situáciu, maximálna doba na vyriešenie mimoriadnej situácie a obnovu služieb a pod. Stanovenie sankcií a povinnosti nahradiť škodu pri nedodržaní stanovených úrovní služieb.

- **Požiadavky na zabezpečenie BCM na strane dodávateľa**: Súčasťou požiadaviek na dodávateľa môže byť požiadavka preukázať primeranú schopnosť obnovy. Dodávateľ sa môže napríklad preukázať certifikátom na svoj systém riadenia kontinuity činností vydaný nezávislou certifikačnou autoritou, alebo umožní organizácii vykonať externý audit.

Procesný cyklus BCM



Fáza 0 – Riadenie BCM
- Organizačný rámec
- Základné dokumenty – Politika, Metodika

Fáza 1 – Ohodnotenie
- Analýza rizík, analýza dopadov
- Určenie priorít a závislostí

Fáza 2 – Plánovanie
- Výber opatrení na zabezpečenie kontinuity a obnovy

Fáza 3 - Implementácia
- Zavádzanie opatrení
- Príprava akčných plánov (BCP a DRP)
- Školenia

Fáza 4 - Monitorovanie
- Testovanie a udržiavanie pripravenosti organizácie zabezpečiť kontinuitu a obnovu

Fáza 3 - Implementácia

Aktivity

- Zavádzanie opatrení vybraných vo fáze plánovania
- Príprava akčných plánov (BCP a DRP)
- Školenia

Výstupy

- Implementované opatrenia
- Individuálne akčné plány – Plány kontinuity činností a plány obnovy špecifikujúce alternatívne procedúry pre kritické procesy a techniky obnovy pre kritické zdroje
- Vyškolený personál schopný používať akčné plány

Akčné plány - štruktúra

Štruktúra akčných plánov podľa štandardu BSI Standard 100-4: Business Continuity Management:

- **Plán okamžitej reakcie** (Immediate measures plan) popisuje kroky na prvoradé zabezpečenie bezpečnosti a ochrany osôb.

- **Príručka krízového tímu** (Crisis team guide) spolu s **plánom krízovej komunikácie** (Crisis communication plan) dávajú návod na zvládnutie krízového stavu a popisujú riadenie komunikácie počas krízového stavu.

Akčné plány - štruktúra

Štruktúra akčných plánov podľa štandardu BSI Standard 100-4: Business Continuity Management:

- **Plány kontinuity činností** (Business continuity plans) popisujú reakciu organizácie na výpadok kritických procesov spôsobený bezpečnostným incidentom. Plán kontinuity činností tvorí sada dokumentovaných postupov a informácií, ktoré umožnia organizácii obnovu a prevádzku kritických procesov na akceptovateľnej preddefinovanej úrovni.

- **Plány obnovy** (Recovery plans) obsahujú dokumentované postupy a informácie, ktoré umožnia organizácii obnovu a prevádzku zdroja/prostriedku. Plány obnovy dopĺňajú plány kontinuity činností.

Akčné plány - štruktúra

Štruktúra akčných plánov podľa štandardu NIST Special Publication 800-34 Rev. 1:

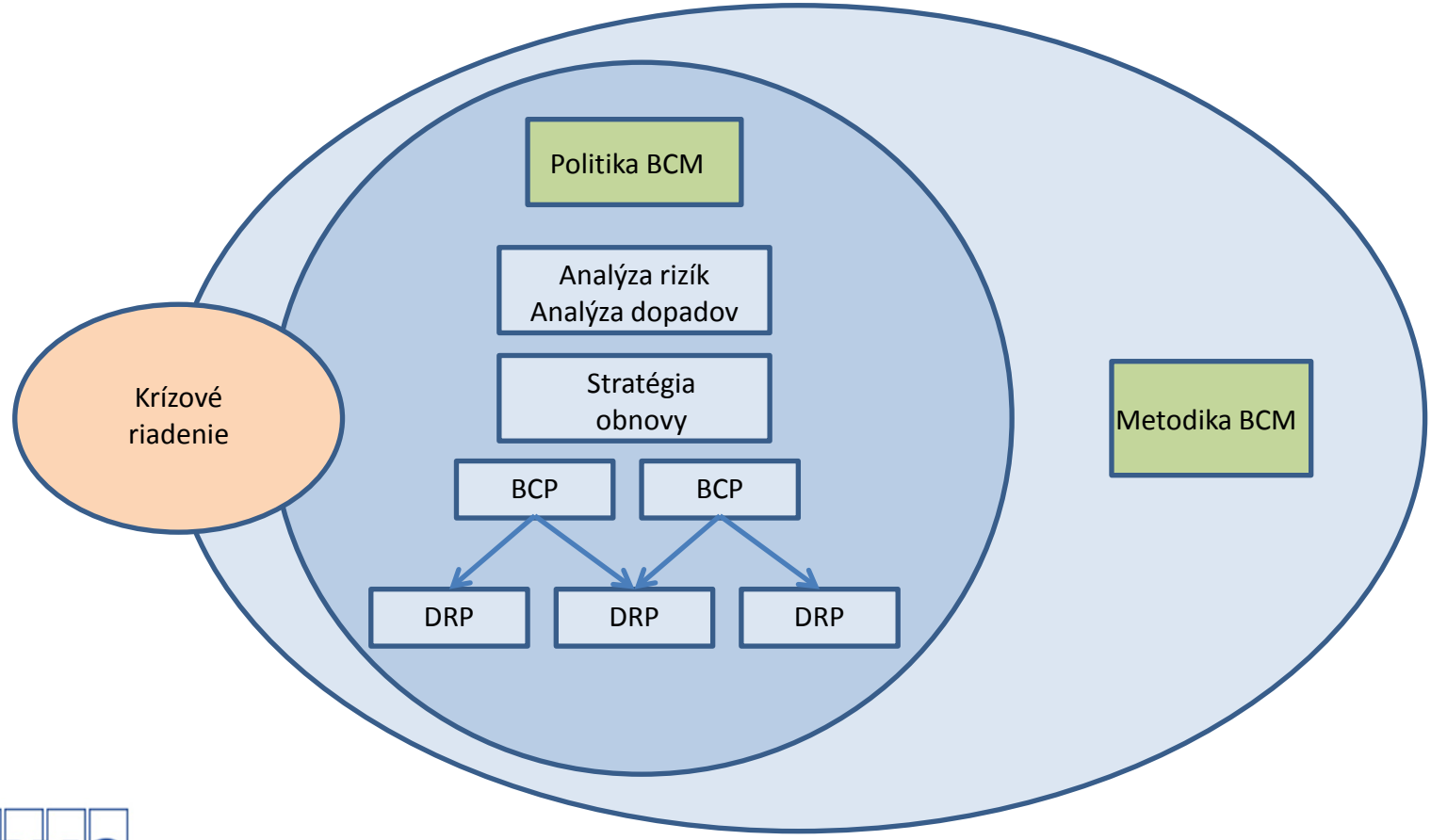
- **Business Continuity Plan** – Popisuje procedúry na udržanie biznis prevádzky počas obnovy po výpadku.
- **Continuity of Operations Plan** – Popisuje procedúry a návod na udržanie kritických činností v záložnej lokalite po dobu do 30 dní (požadované federálnou legislatívou).
- **Crisis Communications Plan** - Popisuje procedúry na zvládnutie internej a externej komunikácie, prostriedky na poskytovanie informácií o kritickom stave a zvládnutie šírenia „klebiet“.
- **Critical Infrastructure Protection Plan** – Popisuje politiky a procedúry na ochranu prvkov národnej kritickej infraštruktúry v súlade s Plánom ochrany národnej infraštruktúry.

Akčné plány - štruktúra

Štruktúra akčných plánov podľa štandardu NIST Special Publication 800-34 Rev. 1:

- **Cyber Incident Response Plan** - Popisuje procedúry na zvládnutie kybernetického útoku ako napríklad vírus, červ alebo trójsky kôň.
- **Disaster Recovery Plan** - Popisuje procedúry na premiestnenie prevádzky informačných systémov do alternatívnej lokality.
- **Information System Contingency Plan** - Popisuje procedúry a vybavenie na obnovu informačného systému.
- **Occupant Emergency Plan** - Popisuje procedúry na minimalizáciu strát na životoch alebo ujmy na zdraví a na ochranu majetku v dôsledku fyzickej hrozby.

Vzťahy medzi dokumentmi BCM



Akčné plány - príprava

Akčné plány sú pripravované pre procesy a zdroje/prostriedky v závislosti od ich priority určenej vo fáze ohodnotenia a v súlade s opatreniami určenými vo fáze plánovania.

Na príprave akčných plánov sa na jednej strane podieľajú

- **Vlastníci a vykonávatelia procesov** - znalosti a skúsenosti s daným procesom
- **Správcovia zdrojov a prostriedkov** - znalosti a skúsenosti s daným zdrojom / prostriedkom
- **Manažér IB** (BCM koordinátor) - súlad akčných plánov s požiadavkami na obnovu, ktoré majú naplniť, súlad s celkovým kontextom BCM v organizácii a konzistentnú formu

Pripravené akčné plány musia byť **schválené vedením organizácie**

Plán kontinuity činností 1/11

Štruktúra

- Údaje o dokumente plánu
- Popis procesu
- Pravidlá aktivácie plánu
- Popis scenáru/scenárov
- Obmedzenia/predpoklady
- Kontaktné údaje všetkých osôb uvedených v pláne

Štruktúra pre každý scenár

- Prípravné úlohy
- Identifikácia problému
- Fáza reakcie
- Alternatívny proces
- Obnovovacie postupy
- Kontrolné úlohy
- Úlohy po obnovení

Plán kontinuity činností 2/11

Údaje o dokumente plánu

- Kto plán vytvoril
- Kto plán schválil
- Vlastník plánu / osoba zodpovedná za jeho aktualizáciu
- Distribúcia a umiestnenie plánu (ktoré osoby k plánu majú prístup a kde sú umiestnené jeho elektronické a papierové kópie)
- Referencie na iné dokumenty

Plán kontinuity činností 3/11

Popis procesu

- Popis procesu z analýzy dopadov
- Vlastník procesu a jeho zástupcovia
- Parametre procesu – MTO, RTO, RPO
- Zdroje využívané procesom
  - Aplikácie
  - Infraštruktúra
  - Údaje (vo fyzickej aj logickej podobe)
  - Ľudské zdroje
  - Lokality
  - Dodávatelia

Plán kontinuity činností 4/11

Pravidlá aktivácie plánu - popis kritérií, ktoré musia byť splnené na aktiváciu plánu a určenie osoby alebo osôb s právomocou rozhodnúť o aktivácii plánu

Príklady scenárov

- Nedostupnosť aplikácie
- Obmedzenie funkčnosti aplikácie
- Nedostupnosť budovy
- Výpadok podporných služieb (elektrina, voda, kúrenie)
- Výpadok služieb dodávateľa
- Nedostupnosť ľudských zdrojov

Obmedzenia/predpoklady

Plán kontinuity činností 5/11

Prípravné úlohy:

Všetky aktivity, ktoré majú byť vykonané pred tým, ako je plán použitý pri realizácii negatívneho scenára.

Príklady:

- Zabezpečenie náhradných priestorov
- Zabezpečenie náhradnej techniky
- Príprava internej a externej komunikácie
- Dohodnutie SLA s dodávateľom
- Aktívny monitoring

Plán kontinuity činností 6/11

Identifikácia problému:

Akým spôsobom zistíme, že nastal negatívny scenár.

Príklady:

- Automatické notifikácie
- Identifikácia zamestnancami IT
- Hlásenie dodávateľa
- Identifikácia používateľmi (zamestnancami)
- Identifikácia zákazníkmi

Dôležitá je kontaktná osoba!

Plán kontinuity činností 7/11

Fáza reakcie:

Reakcia na incident (súčasťou témy Riadenie incidentov)

Príklady:

- Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér IB)
- Potvrdenie scenára
- Aktivácia krízového riadenia
- Aktivácia plánu obnovy
- Rozhodnutie o alternatívnom procese
- Informovanie ďalších osôb (call centrum, interní používatelia)

Plán kontinuity činností 8/11

Alternatívny proces:

Alternatívne spôsoby výkonu procesu (ak existujú)

Príklady:

- Realizácia procesu v alternatívnych priestoroch
- Práca z domu
- Realizácia procesu náhradným personálom
- Použitie kancelárskeho softvéru namiesto aplikácie
- Manuálne spracovanie namiesto automatizovaného
- Informovanie na web stránke, call centre, sociálnych sieťach
- „Čakanie“

Plán kontinuity činností 9/11

Obnovovacie postupy :

Kroky na obnovenie plnej prevádzky

Príklady:

- Realizácia plánu obnovy
- Obnova údajov zo zálohy
- Reštart IKT systémov
- Realizácia krokov, ktoré nie sú v pláne obnovy, alebo ak pre dané aktívum neexistuje plán obnovy
- Obnova v spolupráci s dodávateľom

Plán kontinuity činností 10/11

Kontrolné úlohy:

Aktivity vykonávané na uistenie pred prechodom do plnej prevádzky

Príklady:

- Kontrola dostupnosti a funkčnosti IKT systémov
- Kontrola obnovy a aktuálnosti údajov
- Kontrola dostupnosti priestorov
- Potvrdenie dostupnosti personálu

Plán kontinuity činností 11/11

Úlohy po obnovení:

Aktivity „upratovacieho“ charakteru, ktoré je možné vykonať až po obnovení, respektíve nie je nevyhnutné ich vykonať v rámci obnovy

Príklady:

- Vysporiadanie sa s údajmi, ktoré nemohli byť spracované počas výpadku alebo boli spracovanými alternatívnym spôsobom
- Odstránenie informácie o výpadku z web stránky, kontaktného centra
- Informovanie relevantných osôb – vlastník procesu, manažér IB
- Informovanie ďalších osôb - kontaktné centrum, interní používatelia

Plán obnovy 1/10

Štruktúra

- Údaje o dokumente plánu
- Popis zdroja (systému)
- Popis scenáru/scenárov
- Obmedzenia/predpoklady
- Kontaktné údaje všetkých osôb uvedených v pláne

Štruktúra pre každý scenár

- Prípravné úlohy
- Identifikácia problému
- Fáza reakcie
- Obnovovacie postupy
- Kontrolné úlohy
- Úlohy po obnovení

Plán obnovy 2/10

Údaje o dokumente plánu

- Kto plán vytvoril
- Kto plán schválil
- Vlastník plánu / osoba zodpovedná za jeho aktualizáciu
- Distribúcia a umiestnenie plánu (ktoré osoby k plánu majú prístup a kde sú umiestnené jeho elektronické a papierové kópie)
- Referencie na iné dokumenty

Plán obnovy 3/10

Popis zdroja

- Popis zdroja
- Vlastník/IT gestor zdroja a jeho zástupcovia
- Zoznam podporovaných procesov
- Požiadavky na obnovu (MTO, RTO, RPO)
- Stratégia obnovy

Plán obnovy 4/10

Príklady scenárov

- Obnova údajov zo zálohy
- Obnova konfigurácie aplikácie/databázy/operačného systému
- Opätovná inštalácia aplikácie/ databázy/ operačného systému
- Výmena hardvérového komponentu
- Opätovná inštalácia celého hardvéru

Obmedzenia/predpoklady

- Kvalifikácia personálu
- Vhodné priestory – riadne alebo náhradné
- Dostupná sieťová infraštruktúra - pripojenie do lokálnej siete/na Internet

Plán obnovy 5/10

Prípravné úlohy:

Všetky aktivity, ktoré majú byť vykonané pred tým ako je plán použitý pri realizácii negatívneho scenára.

Príklady:

- Udržiavanie konfiguračnej databázy
- Predpripravený „image“ systému
- Zabezpečenie náhradného hardvéru
- Dohodnutie SLA s dodávateľom hardvéru
- Aktívny monitoring

Plán obnovy 6/10

Identifikácia problému:

Akým spôsobom zistíme, že nastal negatívny scenár.

Príklady:

- Aktivácia DRP z nadradeného BCP
- Automatické notifikácie
- Identifikácia zamestnancami IT oddelenia
- Hlásenie dodávateľa
- Identifikácia používateľmi (zamestnancami)
- Identifikácia zákazníkmi

Plán obnovy 7/10

Fáza reakcie:

Reakcia na incident (súčasťou témy Riadenie incidentov)

Príklady:

- Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér IB)
- Potvrdenie scenára
- Výber scenára obnovy

Plán obnovy 8/10

Obnovovacie postupy :

Kroky na obnovenie zdroja/prostriedku podľa zvoleného scenára

Príklady scenárov:

- Obnova údajov zo zálohy
- Obnova konfigurácie aplikácie/databázy/operačného systému
- Opätovná inštalácia aplikácie/ databázy/ operačného systému
- Výmena hardvérového komponentu
- Opätovná inštalácia celého hardvéru

Plán obnovy 9/10

Kontrolné úlohy:

Aktivity vykonávané na uistenie pred prechodom do plnej prevádzky

Príklady:

- Kontrola dostupnosti a funkčnosti IKT systémov
- Kontrola obnovy a aktuálnosti údajov
- Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér IB)

Plán obnovy 10/10

Úlohy po obnovení:

Aktivity „upratovacieho“ charakteru, ktoré je možné vykonať až po obnovení, respektíve nie je nevyhnutné ich vykonať v rámci obnovy

Príklady:

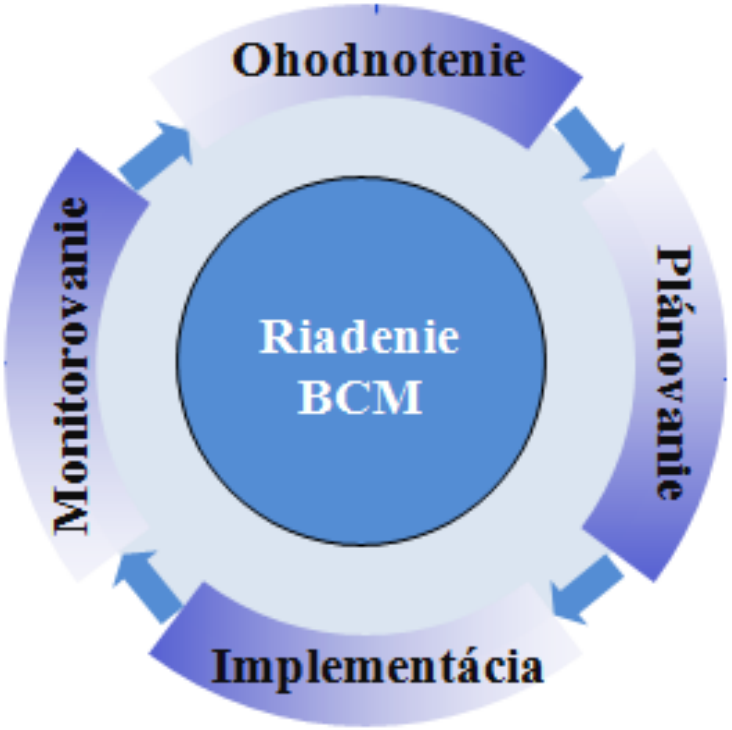
- Vysporiadanie sa s údajmi, ktoré nemohli byť spracované počas výpadku
- Informovanie relevantných osôb – vlastník procesu, manažér IB
- Informovanie ďalších osôb - kontaktné centrum, interní používatelia

Školenia

- Po príprave a schválení akčných plánov je potrebné vyškoliť osoby zahrnuté do akčných plánov tak, aby boli schopné akčné plány používať a dosiahnuť požadované výsledky.

- Za prípravu a realizáciu školení je zodpovedný manažér IB (BCM koordinátor). S obsahovou časťou školení mu pomôžu vlastníci procesov a správcovia zdrojov, ktorí sa podieľali na príprave plánov

Procesný cyklus BCM



Fáza 0 – Riadenie BCM
- Organizačný rámec
- Základné dokumenty – Politika, Metodika

Fáza 1 – Ohodnotenie
- Analýza rizík, analýza dopadov
- Určenie priorít a závislostí

Fáza 2 – Plánovanie
- Výber opatrení na zabezpečenie kontinuity a obnovy

Fáza 3 - Implementácia
- Zavádzanie opatrení
- Príprava akčných plánov (BCP a DRP)
- Školenia

Fáza 4 - Monitorovanie
- Testovanie a udržiavanie pripravenosti organizácie zabezpečiť kontinuitu a obnovu

Fáza 4 - Monitorovanie

Aktivity

- Testovanie úplnosti, efektívnosti a realizovateľnosti pripravených akčných plánov
- Vyhodnotenie testovania akčných plánov
- Previerka BCM funkcie
- Aktualizácia s ohľadom na identifikované nedostatky

Výstupy

- Výsledky testovania akčných plánov
- Výsledky previerky BCM funkcie
- Identifikované nedostatky a odporúčania na zlepšenie
- Aktualizované BCM procesy a akčné plány

Testovanie akčných plánov 1/10

Prínosy testovania:

- Odhalenie prípadných nedostatkov a nepresností v plánoch
- Zvýšenie informovanosti a povedomia
- Zručnosti a efektívnejšie použitie plánov
- Zvýšená istota, že sa môžeme na akčné plány spoľahnúť

Za organizáciu testovania, výkon testovania a následnú aktualizáciu akčných plánov zodpovedá **manažér IB** (BCM koordinátor).

Pri organizácii testovania musí brať do úvahy viacero faktorov:

- Priorita procesov a zdrojov/prostriedkov
- Náklady na testovanie (času zainteresovaných pracovníkov)
- Riziká spojené s jednotlivými typmi testov

Testovanie akčných plánov 2/10

Testovanie akčných plánov je potrebné vykonávať **v opakovaných cykloch** minimálne na ročnej báze.

Jeden cyklus obsahuje nasledovné kroky:

- Príprava a schválenie plánu testovania na celý cyklus (napríklad rok)
- Príprava a schválenie jednotlivých testov
- Výkon testovania v dohodnutom čase
- Dokumentácia priebehu a výsledkov testovania
- Analýza a vyvodenie záverov

Testovanie akčných plánov 3/10

Manažér IB je zodpovedný za prípravu **plánu testovania akčných plánov** a **detailného návrhu** každého testu.

Vyhodnotené musia byť nasledovné oblasti

- Kritickosť procesov
- Prepojenie s ostatnými procesmi
- Predchádzajúce plány testovania
- Vhodné typy testov
- Možné negatívne dopady testu na prevádzku a funkčnosť činností organizácie
- Dostupnosť zdrojov potrebných na vykonanie plánovaných testov

Plán testovania a návrhy jednotlivých testov musia byť následne schválené vedením organizácie.

Testovanie akčných plánov 4/10

Manažér IB je zodpovedný za **realizáciu jednotlivých testov** v stanovenom termíne podľa plánu testovania a za **zabezpečenie dokumentácie priebehu testovania** (napr. vo forme protokolu z testovania).

Po ukončení testu je manažér IB zodpovedný za vykonanie **analýzy priebehu a výsledkov** testovania v spolupráci s relevantnými účastníkmi testu. Analýza by sa mala zamerať na:

- Vyhodnotenie vhodnosti a primeranosti obnovovacích postupov.
- Vyhodnotenie vhodnosti a primeranosti alternatívnych postupov.
- Vyhodnotenie časového trvania jednotlivých krokov akčného plánu.
- Vyhodnotenie internej a externej komunikácie.
- Vyhodnotenie potreby preškolenia jednotlivých zamestnancov.

Testovanie akčných plánov 5/10

Príklad štruktúry protokolu z testovania:

- Referencia na akčný plán
- Kto test schválil
- Cieľ testu
- Typ testu
- Vedúci testu
- Účastníci testu
- Dátum a čas konania testu
- Trvanie testu
- Miesto výkonu testu
- Výsledky testu – zistené nedostatky
- Návrh nápravných aktivít

Testovanie akčných plánov 6/10

Test „od stola“ (angl. Desk check)

- Preverenie aktuálnosti údajov v pláne a prípadne ich doplnenie alebo oprava.
- Zložitosť: nízka
- Odporúčaná frekvencia: ročne
- Účastníci: manažér IB

Testovanie akčných plánov 7/10

Rekapitulácia (angl. Walk-through)

- Teoretické prejdenie akčného plánu bod po bode bez jeho skutočnej realizácie. Diskusia o jednotlivých bodoch plánu medzi účastníkmi testu s cieľom poukázať na nezrovnalosti a kritické časti akčného plánu.
- Vzhľadom na teoretickú realizáciu testu je potrebné, aby osoba, ktorá test vedie (napr. BCM koordinátor) na začiatku vysvetlila všetky zjednodušenia a náhrady (napr. kto reprezentuje osoby a subjekty, ktoré sa na teste nezúčastňujú, ale sú uvedené v pláne).
- Zložitosť: nízka
- Odporúčaná frekvencia: ročne
- Účastníci: manažér IB a osoby definované v akčnom pláne

Testovanie akčných plánov 8/10

Simulácia

- Účastníci testu vykonávajú všetky aktivity popísané v akčnom pláne, avšak v pripravenom „umelom“ prostredí, napr. mimo bežného pracovného času, v náhradnej lokalite a s informačnými systémami v testovacom prostredí bez použitia produkčných údajov. Podobne ako pri rekapitulácii je potrebné vysvetliť všetky zjednodušenia a náhrady.
- Zložitosť: stredná
- Odporúčaná frekvencia: raz za 1 - 2 roky
- Účastníci: manažér IB a osoby definované v akčnom pláne

Testovanie akčných plánov 9/10

Testovanie vybraných kritických aktivít

- Realizuje sa podobne ako test plánu v plnom rozsahu v "ostrom" prostredí, ale niektoré aktivity sú vynechané, respektíve zrealizované v testovacom prostredí (napr. interakcia s treťou stranou).
- Zložitosť: stredná
- Odporúčaná frekvencia: raz za 2 – 3 roky
- Účastníci: manažér IB a osoby definované v akčnom pláne

Testovanie akčných plánov 10/10

Realizácia akčného plánu v plnom rozsahu

- Realizácia plánu v plnom rozsahu, t.j. vykonanie všetkých krokov podľa plánu v "ostrej" prevádzke. Plán sa iniciuje napr. vyhlásením nedostupnosti budovy, vypnutím informačného systému alebo odpojením dodávky elektrickej energie. Podľa cieľu testu účastníci môžu aj nemusia byť informovaní o tom, že sa jedná o test.
- Zložitosť: vysoká
- Odporúčaná frekvencia: raz za 2 – 3 roky
- Účastníci: manažér IB a všetci zamestnanci ovplyvnení výpadkom

Previerka BCM funkcie

Predmet previerky:

- Organizačný rámec BCM
- Dokumenty - politika BCM, metodika
- Proces, výsledky a aktuálnosť analýzy rizík a analýzy dopadov
- Návrhy a implementácia opatrení
- Stav a pokrytie akčných plánov (BCP, DRP)
- Realizácia plánu testovania akčných plánov

Požiadavky na plánovanie kontinuity činnosti v legislatívnych aktoch SR

Dôležité legislatívne akty z pohľadu BCM

- Výnos MFSR č. 312/2010 o štandardoch pre ISVS
- Zákon č. 45/2011 Z.z. o kritickej infraštruktúre
- Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

- Zákon č.351/2011 Z. z. o elektronických komunikáciách
  všeobecne záväzný právny predpis - opatrenie č. O-30/2012
- Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov

Výnos o štandardoch pre ISVS 1/3

§ 30 Manažment rizík pre oblasť informačnej bezpečnosti

d) **analyzovanie procesov povinnej osoby**, ktoré sú podstatné pre plnenie činnosti povinnej osoby z hľadiska ich závislosti od informačných systémov verejnej správy, a určenie procesov, ktoré nemôžu prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných informačných systémov verejnej správy; tieto procesy sú **kritickými procesmi**

e) **analyzovanie rizík** vyplývajúcich z hrozieb pre informačné systémy verejnej správy, od ktorých závisia kritické procesy; tieto informačné systémy sú **kritickými informačnými systémami** verejnej správy

f) vypracovanie **plánov na obnovu** činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov verejnej správy

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Výnos o štandardoch pre ISVS 2/3

§ 34 Fyzická bezpečnosť a bezpečnosť prostredia

f) zabezpečenie, aby boli existujúce **záložné kapacity informačného systému** verejnej správy, zabezpečujúce funkčnosť alebo náhradu informačného systému verejnej správy, umiestnené v **sekundárnom zabezpečenom priestore**, dostatočne vzdialenom od zabezpečeného priestoru

i) stanovenie parametrov pre informačné systémy verejnej správy, ktoré definujú **maximálnu prípustnú dobu výpadku** informačného systému verejnej správy a vytvorenie a zavedenie opatrení, ktoré sú zamerané na **riešenie obnovy prevádzky v prípade výpadku** informačného systému verejnej správy

KPMG
cutting through complexity™

Výnos o štandardoch pre ISVS 3/3

§ 36 Monitorovanie a manažment bezpečnostných incidentov

§ 38 Zálohovanie

d) zabezpečenie vykonania **testu obnovy** informačného systému verejnej správy a údajov z prevádzkovej zálohy najmenej **raz za jeden rok**

§ 39 Fyzické ukladanie záloh

b) fyzické ukladanie druhej kópie archivačnej zálohy **v inom objekte**, ako sa nachádzajú technické prostriedky informačného systému verejnej správy, ktorého údaje boli archivované tak, aby bolo minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy

Zákon č. 45/2011 o kritickej infraštruktúre

§ 9 Povinnosti prevádzkovateľa

Prevádzkovateľ je povinný ochraňovať prvok pred narušením alebo zničením. Na ten účel prevádzkovateľ je povinný:

b) zaviesť bezpečnostný plán

- popis možných spôsobov hrozby narušenia alebo zničenia prvku
- zraniteľné miesta prvku
- **bezpečnostné opatrenia na jeho ochranu**

c) prehodnocovať priebežne bezpečnostný plán

d) oboznámiť svojich zamestnancov v nevyhnutnom rozsahu s bezpečnostným plánom

e) **precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku**

Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Vyhláška o rozsahu a dokumentácii bezpečnostných opatrení:

§ 4

Bezpečnostná smernica podľa § 19 ods. 2 zákona obsahuje :

e) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností **efektívnej obnovy stavu pred haváriou**, poruchou alebo inou mimoriadnou situáciou

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Požiadavky na plánovanie kontinuity činnosti v medzinárodných štandardoch

KPMG
cutting through complexity™

Normy ISO/IEC rady 270xx

ISO/IEC 27002 — Code of practice for information security management

Kapitola 14. Manažment kontinuity činnosti spoločnosti

Cieľ riadenia: Zabrániť prerušeniam podnikových aktivít a chrániť kritické podnikové procesy pred vplyvmi závažných zlyhaní alebo havárií informačných systémov a zabezpečiť ich včasnú obnovu.

Opatrenia:

- Zahrnutie informačnej bezpečnosti do procesu manažmentu kontinuity činnosti
- Kontinuita činnosti a ohodnotenie rizík
- Zostavovanie a implementovanie plánov kontinuity činnosti vrátane informačnej bezpečnosti
- Štruktúra plánovania kontinuity činnosti
- Testovanie, údržba a prehodnocovanie plánov kontinuity činnosti

Normy ISO/IEC rady 270xx

ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

- Popisuje procesy na prevenciu, predikciu a riadenie udalostí týkajúcich sa IKT, ktoré môžu narušiť kontinuitu činností organizácie.

ISO/IEC 27005 — Information security risk management

- Niektoré usmernenia sa dajú využiť pri realizácii analýzy dopadov.

ISO/IEC TR 27008 — Guidance for auditors on ISMS controls

- Usmernenia pre audit kontrolných opatrení, vrátane BCM oblasti.

ISO 22301:2012 Societal security – Business continuity management systems – Requirements

- Samostatná ISO norma, ktorá sa venuje manažmentu kontinuity činností
- Založený na prístupe na rovnakom prístupe (PDCA cyklus) ako systém manažmentu IB podľa normy ISO/IEC 27001
- Definuje, čo treba robiť, ale nie ako
- Možnosť certifikácie organizácie

Národné štandardy 1/3

Britský inštitút pre štandardy (British Standards Institution)

BS 25999-1:2006 Business Continuity Management. Code of Practice
BS 25999-2:2007 Specification for Business Continuity Management

- Základ pre ISO 22301
- Založený na prístupe PDCA
- Možnosť certifikácie organizácie

Národné štandardy 2/3

Americký národný inštitút pre štandardy a technológie (National Institute of Standards and Technology)

NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

Štruktúrovaný návod a odporúčania na zavedenie procesu plánovania kontinuity pre obnovu informačných systémov po havárii

Národné štandardy 3/3

Nemecký BSI (Federal Office for Information Security)

BSI Standard 100-4: Business Continuity Management

Popisuje, ako vyvinúť, zaviesť a udržiavať v organizácii systém na riadenie kontinuity činnosti

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™