Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Plánovanie kontinuity činností

Michal Bubák

Jún 2013

KPMG
cutting through complexity™

Agenda

- Pojmy, ciele a terminológia
- Životný cyklus BCM
  - Spustenie BCM programu
  - 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)

Kontext

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.

Ciele

Ciele implementácie BCM sú:

- Vytvorenie systému riadenia zameraného na minimalizáciu finančných, prevádzkových, legislatívnych a reputačných dopadov spôsobených negatívnymi udalosťami prerušujúcich prevádzku procesov organizácie.
- Identifikovať kritické biznis funkcie a zdroje potrebné pre prevádzku organizácie a analyzovať možnosti na udržanie kritických funkcií a zdrojov na požadovanej úrovni.
- Identifikovať možné negatívne udalosti, ktoré môžu spôsobiť závažné výpadky a uskutočniť kroky na zmiernenie týchto hrozieb.
- Definovať organizačnú štruktúru, procesy a zdroje na podporu dosiahnutia požadovanej úrovne odolnosti.
- Testovanie a udržiavanie definovanej štruktúry, procesov a zdrojov na zaistenie tejto odolnosti v akomkoľvek čase.

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.

Havarijný plán - Disaster Recovery Plan (DRP)

Postup obnovy zdrojov.

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.

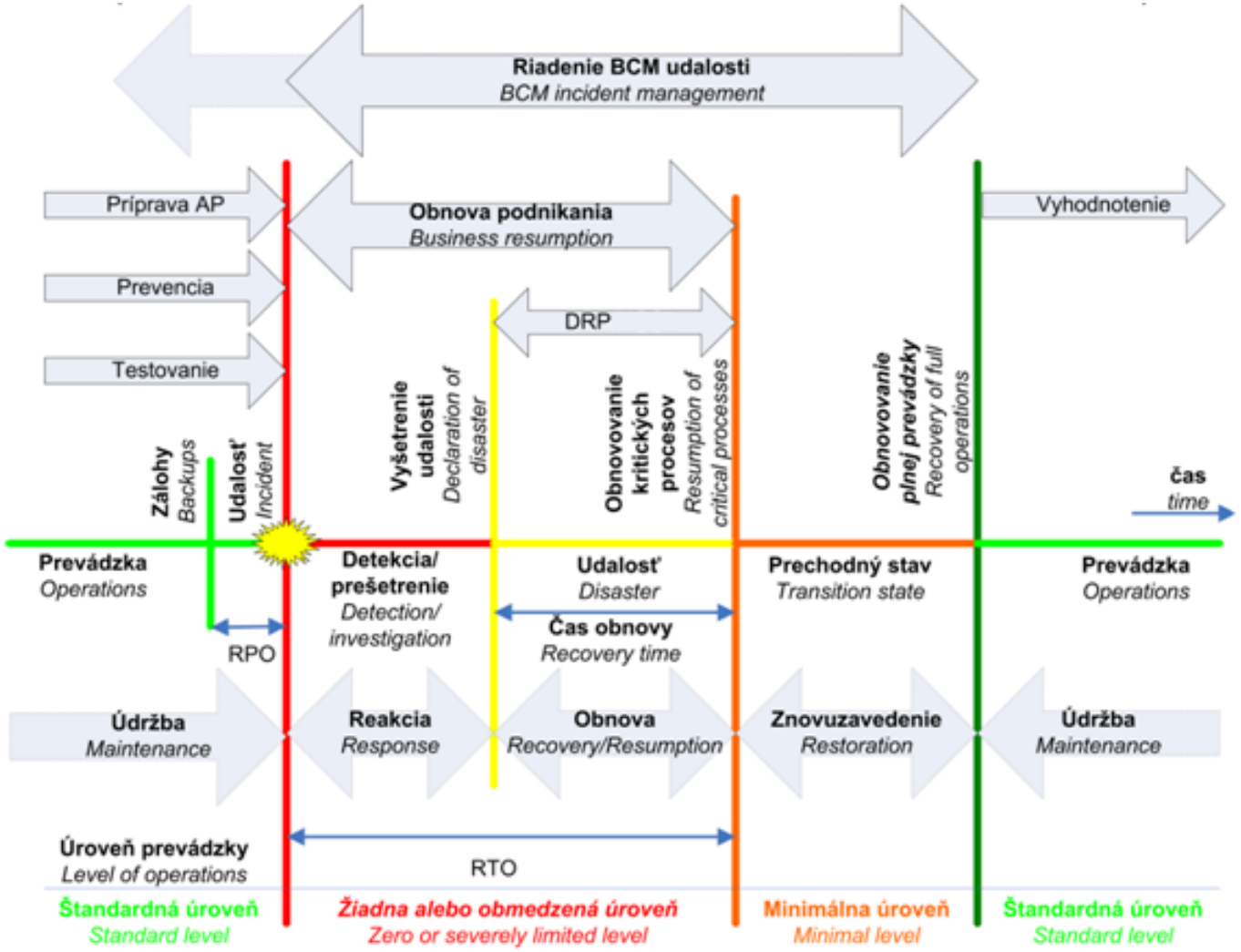
Cieľový čas obnovenia - Recovery Time Objective (RTO)

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)

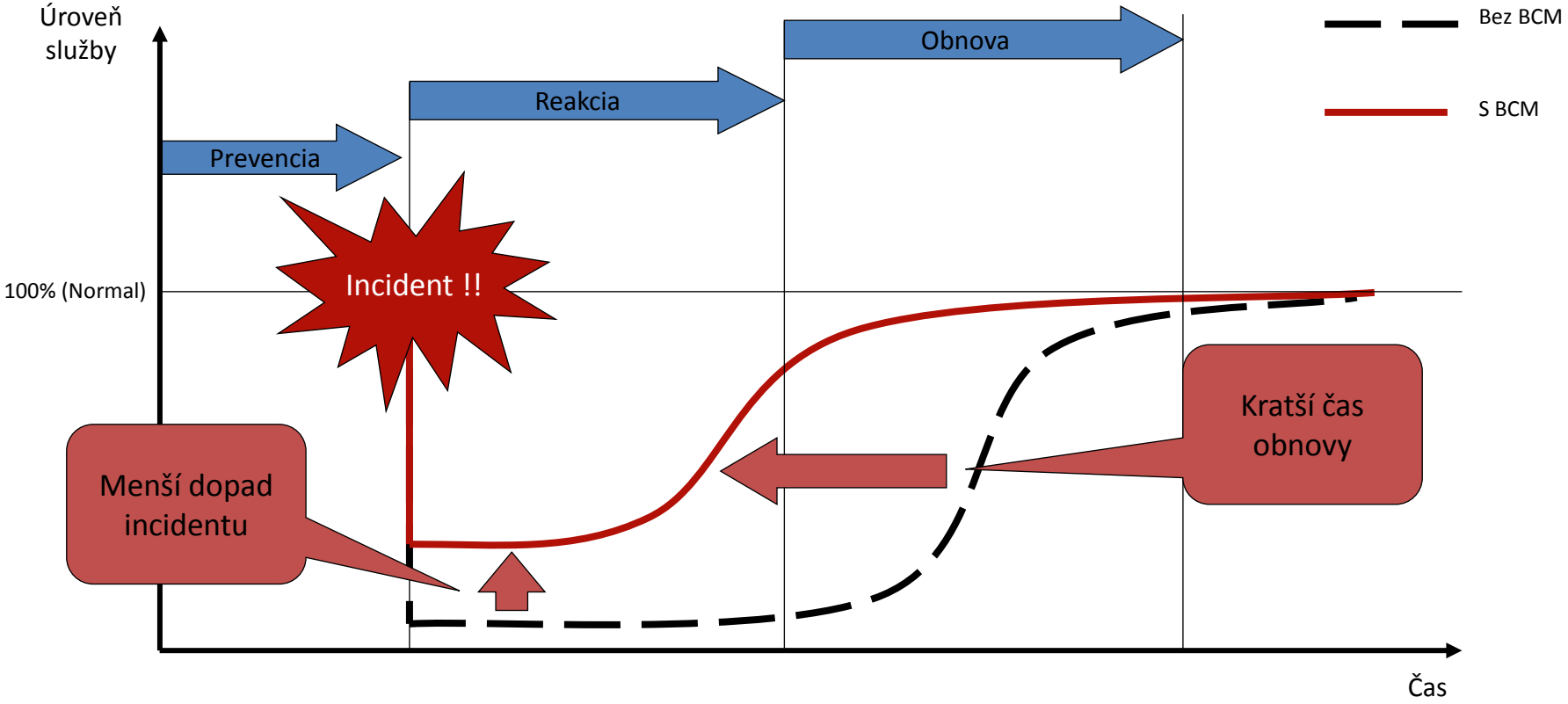
Maximálne množstvo dát, ktoré môže byť stratené, kým je proces alebo služba obnovená po jej prerušení. Je vyjadrený ako dĺžka času pred výpadkom.

Terminológia 3/3

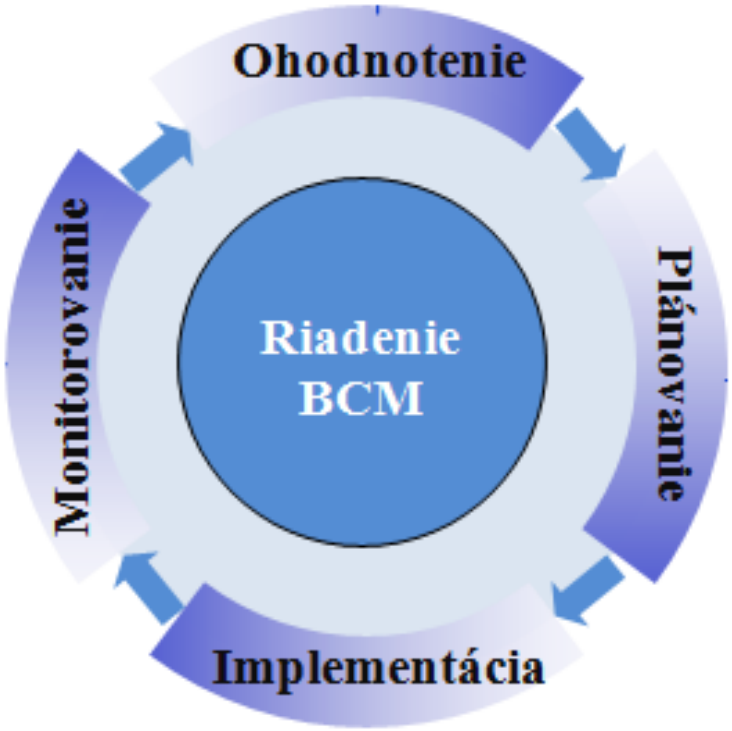


KPMG
cutting through complexity™

Prínosy BCM


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

Životný cyklus BCM



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

Fáza 1 - Ohodnotenie
- Analýza rizík
- Analýza dopadov

Fáza 2 - Plánovanie
- Rozdielová analýza (gap analysis)
- Návrh stratégie obnovy

Fáza 3 - Implementácia
- Vytvorenie plánov kontinuity činnosti
- Vytvorenie havarijných plánov

Fáza 4 - Monitorovanie
- Testovanie
- Monitorovanie výkonnosti
- Zaznamenávanie výsledkov

Fáza 0 - Spustenie BCM programu

Aktivity

- Ustanovenie BCM tímu:
  - Sponzor BCM
  - Riadiaca komisia pre BCM (Bezpečnostná komisia)
  - BCM Koordinátor (Manažér bezpečnosti)
- Príprava Politiky BCM
- Príprava metodických dokumentov

Výstupy

- Tím BCM
- Politika BCM
- Metodika BCM

Fáza 1 - Ohodnotenie

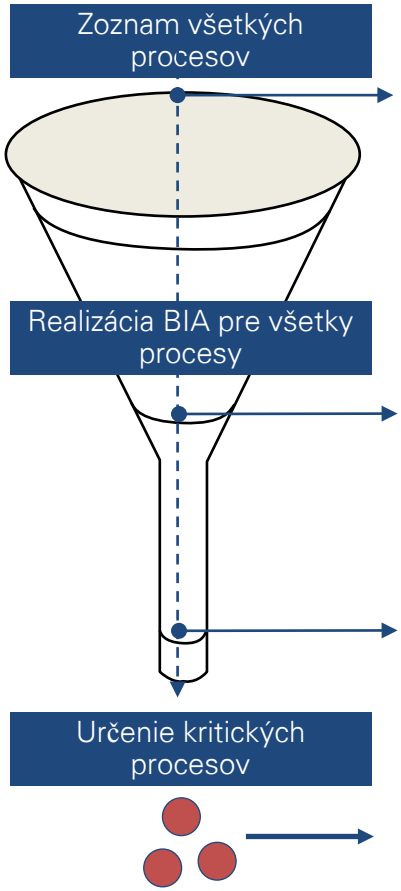
Aktivity

- Identifikácia kritických funkcií a procesov
- Identifikácia kritických zdrojov
- Identifikácia aktuálnych rizík ohrozujúcich kontinuitu
- Definovanie cieľov pre dosiahnutie požadovaného stavu odolnosti (RTO, RPO)

Výstupy

- Analýza Dopadov (BIA) – Identifikácia kritických procesov, ich závislosť na zdrojoch a požiadavky na obnovu
- Analýza Rizík – identifikácia zraniteľností kritických procesov a zdrojov, a potenciálnych hrozieb ohrozujúcich tieto procesy a zdroje

Analýza dopadov 1/4



- 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**

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Analýza dopadov 2/4

Kľúčový element – časové rozsahy

Časové rozsahy výpadku narastajú od momentu výpadku
Musia byť prispôsobené podľa potrieb spoločnosti

Tabuľka dopadov		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
	Reputačný	Nízky	Nízky	Nízky	Stredný	Stredný	Stredný	Vysoký	Vysoký

KPMG
cutting through complexity™

Analýza dopadov 3/4

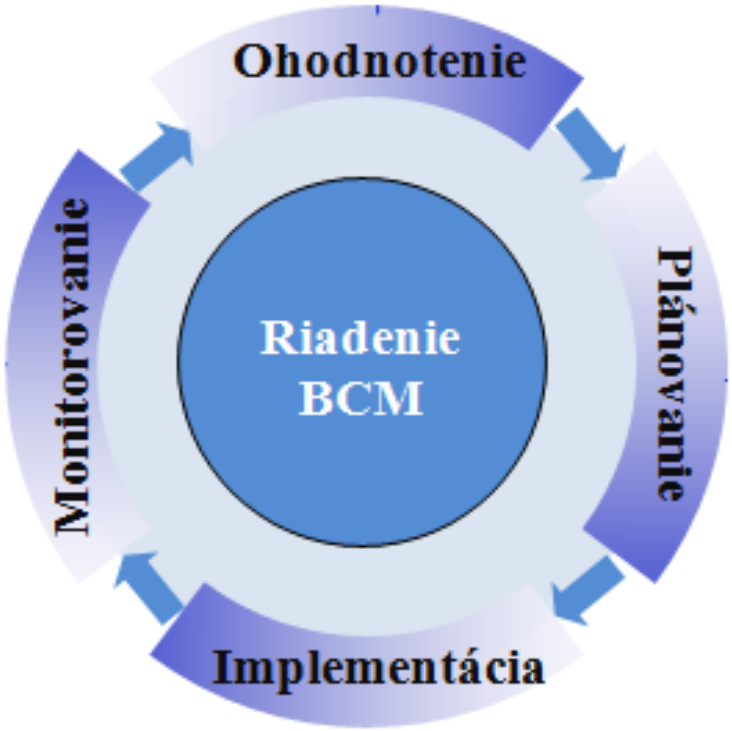
Hodnota	Popis dopadu	Prevádzkový dopad	Legislatívny dopad	Finančný dopad (v €)	Reputačný dopad
0	Žiaden dopad	-	-	-	-
1	zanedbateľný vplyv, strata	interne, útvar	disciplinárne konanie	0 - 5 000	interná nespokojnosť v rámci útvaru
2	malý vplyv, strata	interne, viacero útvarov	zmena vnútornej legislatívy	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

Analýza dopadov 4/4

Závislosti procesov

- Na iných „biznis“ procesoch a aktivitách
- Na podporných procesoch
- Na zdrojoch – hierarchický model
  - Aplikácie (informačné systémy)
  - Infraštruktúra
  - Ľudské zdroje
  - Lokality
  - Tretie strany (dodávatelia)

Životný cyklus BCM



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

Fáza 1 - Ohodnotenie
- Analýza rizík
- Analýza dopadov

Fáza 2 - Plánovanie
- Rozdielová analýza (gap analysis)
- Návrh stratégie obnovy

Fáza 3 - Implementácia
- Vytvorenie plánov kontinuity činnosti
- Vytvorenie havarijných plánov

Fáza 4 - Monitorovanie
- Testovanie
- Monitorovanie výkonnosti
- Zaznamenávanie výsledkov

Fáza 2 - Plánovanie

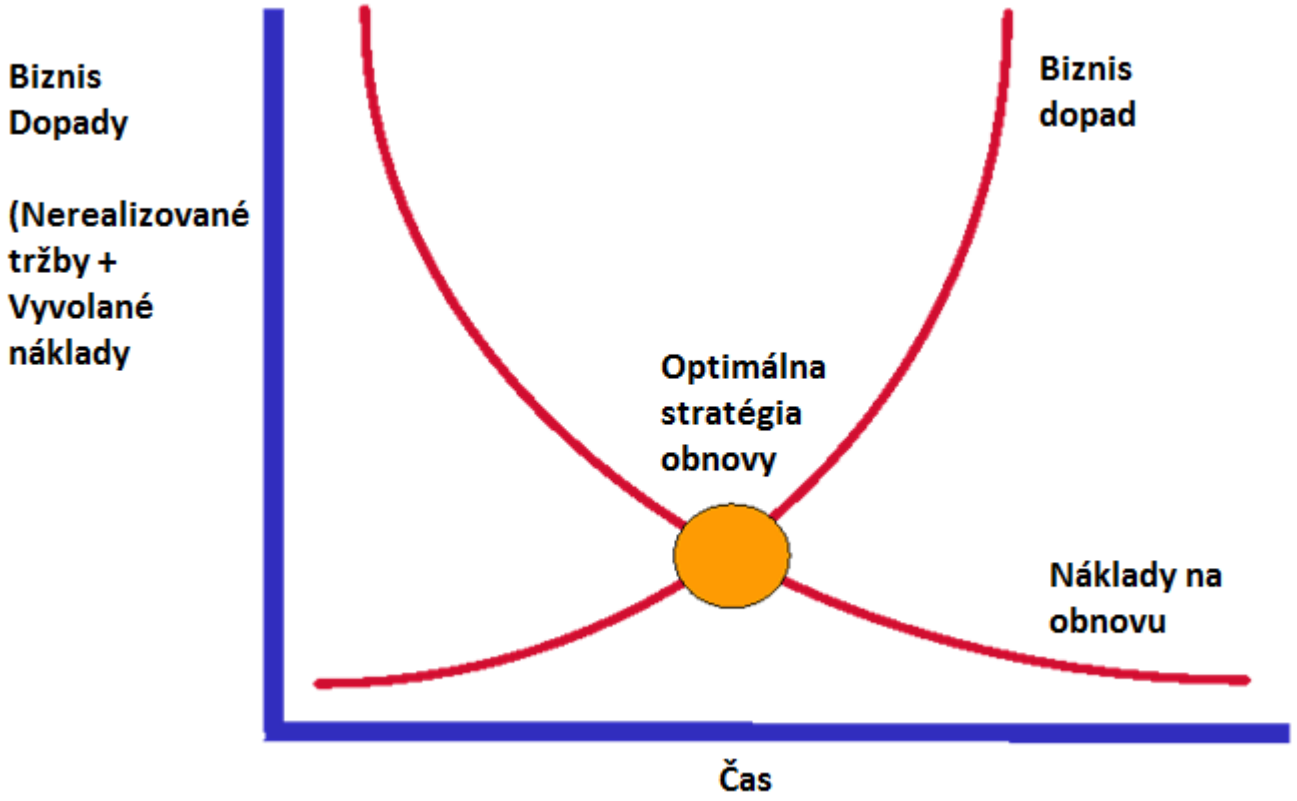
Aktivity

- Analýza rozdielov medzi biznis požiadavkami a kapacitami pre obnovu z existujúcich zdrojov
- Príprava optimálnej architektúry procesov, zdrojov, technológii a stanovenie požiadaviek na požadovaný stav

Výstupy

- Rozdielová analýza – identifikácia nesúladu medzi biznis požiadavkami na obnovu a možnosťami súčasných zdrojov na obnovu
- Stratégia obnovy – identifikácia strategických cieľov obnovy a definícia prístupu k obnove

Stratégia obnovy



Stratégia obnovy pre technológie 1/2

Spôsoby obnovy, ako reagovať na prerušenie služby:

- Nekonať
- Manuálne náhradné riešenie (workaround)
- Postupná obnova (Cold Standby) - viac ako 72 hodín
  - prenosné, alebo trvalé priestory, ktoré majú podporné vybavenie a sieťovú kabeláž, ale nie počítačové systémy. Hardvér a softvér sú inštalované dodatočne.
- Strednodobá obnova (Warm Standby) – 24 – 72 hodín
  - Priestory majú počítačové systémy a sieťové komponenty. Nutná konfigurácia hardvéru a softvéru a taktiež obnova dát.

Stratégia obnovy pre technológie 2/2

Spôsoby obnovy, ako reagovať na prerušenie služby:

- Rýchla obnova – menej ako 24 hodín
  - Vyhradené pevné priestory s počítačovými systémami, softvér nakonfigurovaný a pripravený. Potreba obnovy údajov zo zálohy.
- Okamžitá obnova (Hot Standby) – obnova bez akejkoľvek straty služby
  - Používa zrkadlenie (mirroring) , rozdelenie výkonu (load balancing) a rozdelenie umiestnenia technológií.
  - Riešenia vysokej dostupnosti (High Availability Clusters)

Stratégia obnovy pre ľudské zdroje

Opatrenia v rámci stratégie obnovy pre personál:

- Dokumentácia pracovných postupov
- Prekrývajúce sa pracovné pozície
- Zastupiteľnosť / Plánovanie nástupníctva
- Rotácia zamestnancov
- Použitie tretích strán

Stratégia obnovy pre priestory

Opatrenia v rámci stratégie obnovy pre priestory:

- Alternatívne priestory v rámci organizácie
- Alternatívne priestory poskytnuté treťou stranou (recipročné alebo komerčné dohody)
- Práca z domu

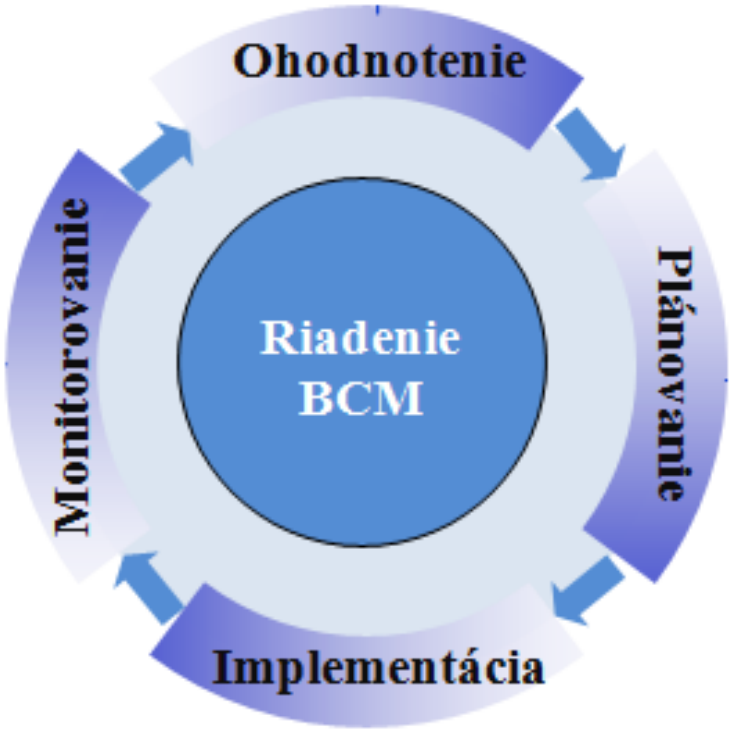
Alternatívne priestory by nemali byť príliš blízko pri hlavných, aby nepodliehali rovnakému riziku a zároveň by nemali byť príliš ďaleko, aby to nesťažovalo presun a logistiku.

Stratégia obnovy pre dodávateľov

Opatrenia v rámci stratégie obnovy pre dodávateľov :

- Zvýšenie počtu dodávateľov
- Identifikácia vhodných alternatívnych dodávateľov
- Požiadavky na preukázateľné a overiteľné zabezpečenie BCM na strane dodávateľa
- Dohody o úrovni poskytovaných služieb (SLA)

Životný cyklus BCM



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

Fáza 1 - Ohodnotenie
- Analýza rizík
- Analýza dopadov

Fáza 2 - Plánovanie
- Rozdielová analýza (gap analysis)
- Návrh stratégie obnovy

Fáza 3 - Implementácia
- Vytvorenie plánov kontinuity činnosti
- Vytvorenie havarijných plánov

Fáza 4 - Monitorovanie
- Testovanie
- Monitorovanie výkonnosti
- Zaznamenávanie výsledkov

Fáza 3 - Implementácia

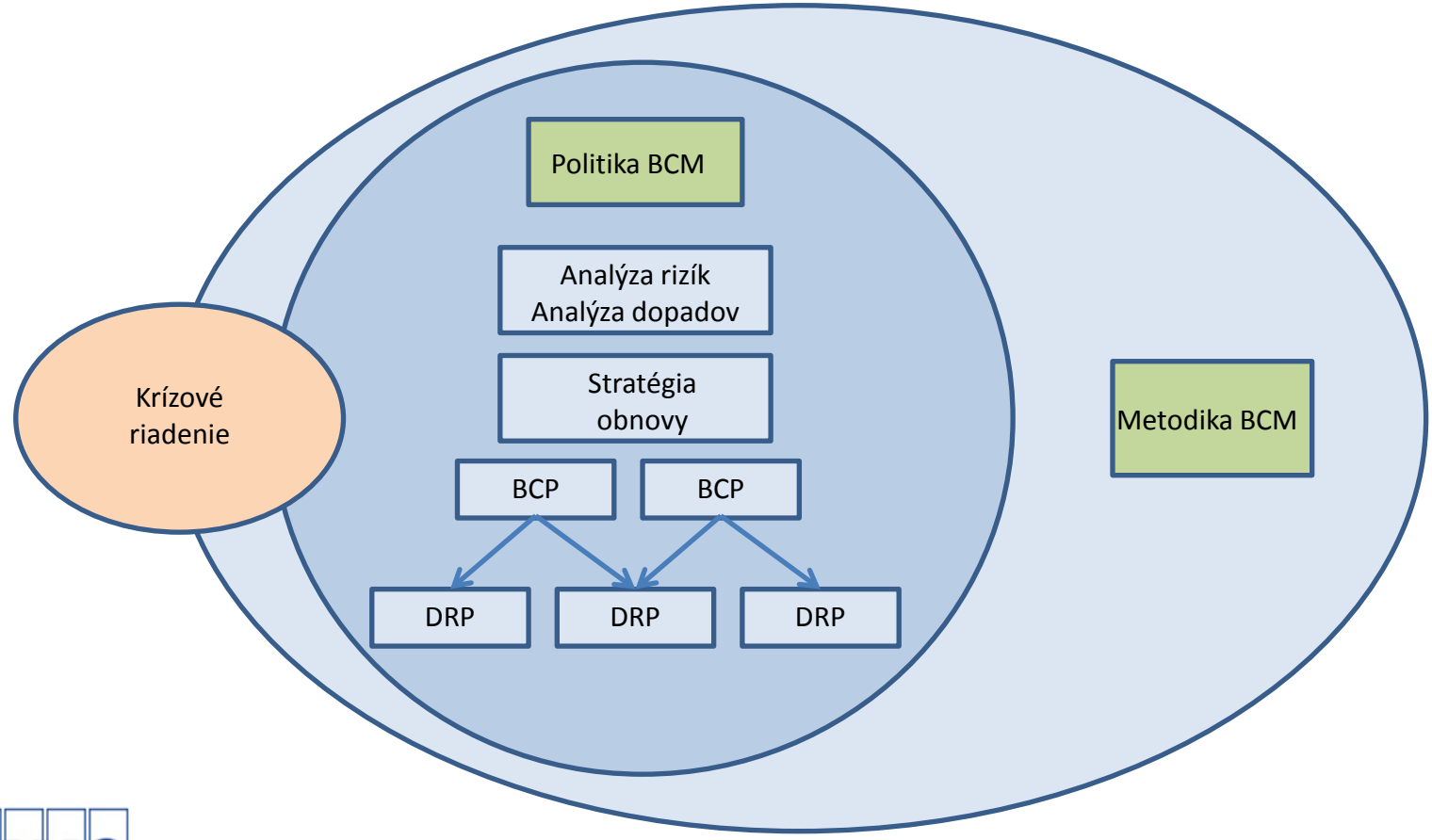
Aktivity

- Príprava akčných plánov (BCP a DRP)
- Školenia

Výstupy

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

Vzťahy medzi dokumentmi BCM



Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Plán kontinuity činností 1/9

Štruktúra

- Popis procesu
- 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

KPMG
cutting through complexity™

Plán kontinuity činností 2/9

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 3/9

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 4/9

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 5/9

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 6/9

Fáza reakcie:

Reakcia na incident (súčasťou témy Riadenie incidentov)

Príklady:

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

Plán kontinuity činností 7/9

Alternatívny proces:

Alternatívne spôsoby výkonu procesu (ak existujú)

Príklady:

- Realizácia procesu v alternatívnych priestoroch
- „Home office“
- 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 8/9

Obnovovacie postupy :

Kroky na obnovenie plnej prevádzky

Príklady:

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

Plán kontinuity činností 9/9

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
- Odstránenie informácie z web stránky, call centra
- Informovanie relevantných osôb (vlastník, BCM koordinátor, manažér IB)
- Informovanie ďalších osôb (call centrum, interní používatelia)

Havarijný plán 1/8

Štruktúra

- 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

Havarijný plán 2/8

Popis zdroja

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

Havarijný plán 3/8

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

Havarijný plán 4/8

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

Havarijný plán 5/8

Identifikácia problému:

Akým spôsobom zistíme, že nastal negatívny scenár.

Príklady:

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

Havarijný plán 6/8

Fáza reakcie:

Reakcia na incident (súčasťou témy Riadenie incidentov)

Príklady:

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

Havarijný plán 7/8

Obnovovacie postupy :

Kroky na obnovenie plnej prevádzky 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

Havarijný plán 8/8

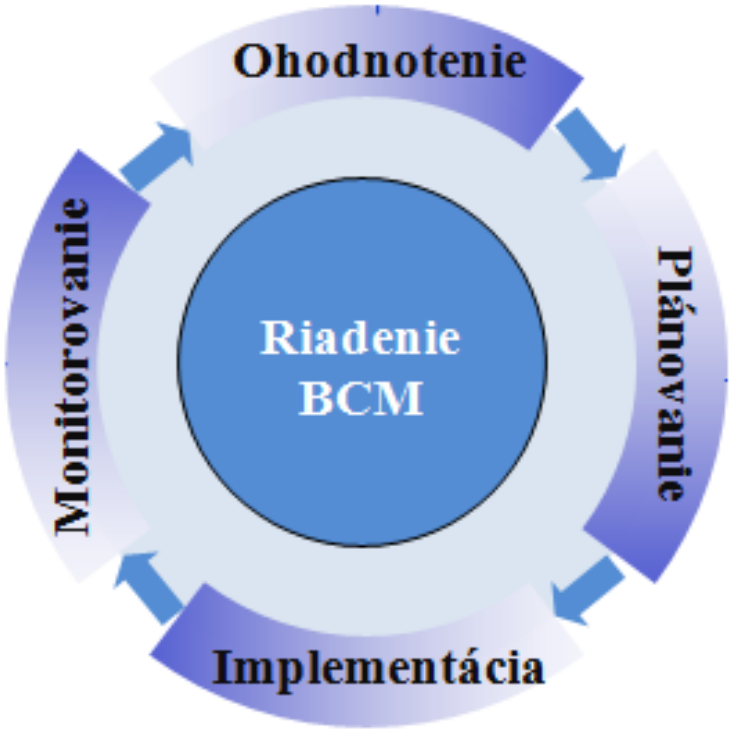
Kontrolné úlohy:

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)

Životný cyklus BCM



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

Fáza 1 - Ohodnotenie
- Analýza rizík
- Analýza dopadov

Fáza 2 - Plánovanie
- Rozdielová analýza (gap analysis)
- Návrh stratégie obnovy

Fáza 3 - Implementácia
- Vytvorenie plánov kontinuity činnosti
- Vytvorenie havarijných plánov

Fáza 4 - Monitorovanie
- Testovanie
- Monitorovanie výkonnosti
- Zaznamenávanie výsledkov

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 1/3

Postupnosť krokov:

- Príprava a schválenie (ročného) plánu testovania
- Príprava individuálnych testov
- Schválenie a akceptácia testov
- Výkon testovania v dohodnutom čase
- Dokumentácia priebehu a výsledkov testovania
- Analýza výsledkov, príprava finálnej správy
- Aktualizácia akčných plánov

Ministerstvo financií Slovenskej republiky

EFQM Recognised for excellence 5 star - 2012

Testovanie akčných plánov 2/3

Zložitosť	Typ testu	Cieľ/Aktivity	Frekvencia
Nízka	Test „od stola“ (Desk check)	Previerka/doplnenie obsahu	Aspoň raz ročne
Stredná	Rekapitulácia (Walk-through)	Kritický pohľad na obsah; Zvýšenie povedomia	Ročne
	Simulácia	Overenie plánu v „testovacom“ prostredí	Ročne alebo 2 krát ročne
	Iba kritické aktivity	Vybrané kroky plánu v ostrej prevádzke	Ročne alebo menej
Vysoká	Realizácia plánu v plnom rozsahu	Realizácia všetkých krokov plánu v ostrej prevádzke	Ročne alebo menej

KPMG cutting through complexity™

Testovanie akčných plánov 3/3

Protokol 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

Previerka BCM funkcie

Predmet previerky:

- Organizačný rámec BCM
- Dokumenty - politika BCM, metodika
- Aktuálnosť analýzy rizík/analýzy dopadov
- Stratégie obnovy
- Stav a pokrytie akčných plánov (BCP, DRP)
- Realizácia plánu testovania akčných plánov

Spôsoby realizácie previerky:

- Nezávislý audit
- Sebahodnotenie (Self-assessment)

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

„Fáza 5“ - Posilňovanie BCM v rámci organizačnej kultúry

Dôležité faktory:

- Vedenie a podpora zo strany vrcholového manažmentu
- Prehľadné a jednoznačné priradenie zodpovedností
- Zladené očakávania
- Pravidelné školenia, budovanie povedomia
- Testovanie akčných plánov

Dôsledky pozitívnej BCM kultúry:

- Efektívnejšia realizácia BCM programu
- Väčšia sebaistota zainteresovaných osôb
- Rýchlejšia obnova

KPMG
cutting through complexity™

Požiadavky na plánovanie kontinuity činnosti v legislatívnych aktoch SR a medzinárodných štandardoch

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™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

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

KPMG
cutting through complexity™

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**

ISO/IEC 27002

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

BS 25999 / ISO 22301

BS 25999-1:2006 Business Continuity Management. Code of Practice

BS 25999-2:2007 Specification for Business Continuity Management

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

- Nahrádza BS 25999
- Založený na prístupe PDCA
- Možnosť certifikácie organizácie

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™