

Mgr. Lukáš Limberk; Mgr. Monika Johaníková; Ing. Ondřej Bos

Business Continuity Management a jeho životní cyklus

Anotace

Příspěvek je věnován popisu jednotlivých fází cyklu řízení kontinuity činností a vysvětlení provázanosti dílčích kroků, přičemž autoři demonstrují cyklus aplikací modelu PDCA. Pro přiblížení náplně částí cyklu řízení kontinuity činností je využita česká verze britské normy BS 25999-1:2006 Management kontinuity činností organizace – Část 1: Soubor zásad. Závěrem je zmíněno několik nových poznatků a přístupů, s nimiž se lze, v souvislosti s životním cyklem řízení kontinuity činností, v současnosti setkat.

Klíčová slova

Řízení kontinuity činností, životní cyklus, Plánuj-Udělej-Zkontroluj-Jednej.

Summary

The article contains description of phases of Business Continuity Management cycle and explanation of ongoing steps by application of PDCA model, as authors demonstrate. To concentrate on some practical aspects of the business continuity management cycle is utilized the Czech version of the British Standard BS 25999-1:2006 Business Continuity Management of the Organization – Part 1: The policy file. Finally are mentioned several new knowledge and approaches which can currently take place in relation to the life cycle of business continuity management.

Keywords

Business Continuity Management, life cycle, Plan-Do-Check-Act.

1. Životní cyklus Business Continuity Management

Business Continuity Management (BCM) je možné implementovat do všech organizací bez ohledu na velikost nebo na ekonomickém sektoru, v němž organizace provozuje svou činnost. Základem životního cyklu BCM je řízení programu BCM, které je bráno jako kontinuální proces. Předmět a struktura programu BCM se může lišit, v závislosti na potřebách jednotlivých organizací.

Management programu

Jádrem životního cyklu BCM je management programu. Program BCM by měl vést k dosažení cílů stanovených politikou kontinuity činností organizace. Management programu BCM se sestává ze tří kroků:¹

- stanovení odpovědností;
- implementace kontinuity činností do organizace;
- nepřetržitý management kontinuity činností organizace.

Plánovací cyklus BCM v rámci normy BS 25999 – 1

Norma BS 25999 – 1 ustavuje proces, principy a terminologii managementu kontinuity činností organizace. Účelem této normy je poskytnout základní podklady pro porozumění, vytváření a implementaci kontinuity činností a zajistit důvěru ve vztazích organizace se zákazníky a ostatními organizacemi. Tato norma poskytuje systém založený na příkladech dobré praxe (good practice) a je určena komukoli, kdo nese odpovědnost za chod organizace nebo poskytování služeb. Od vrcholového vedení, přes všechny úrovně organizace, od organizací s místní působností až po globální hráče. Je určena samostatným obchodníkům, malým a středním podnikům i společnostem zaměstnávající tisíce lidí. Norma se ale netýká činností spojených s nouzovým plánováním, ani témat vztahujících se ke stavům civilní nouze. Bez ohledu na velikost úsilí nebo zdroje vloženého do managementu kontinuity činností organizace může organizace stále čelit kombinaci incidentů, které nepředvídala.

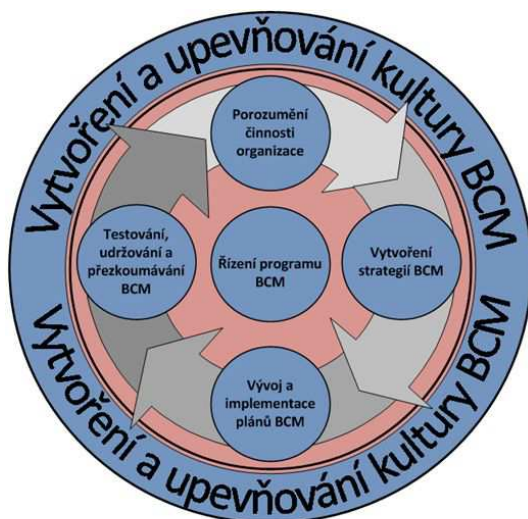
Norma BS 25999 – 1 popisuje řízení kontinuity jako kontinuální cyklický proces začínající stanovením programu BCM, který vychází z politiky managementu kontinuity, na který následně navazují vzájemné propojené fáze. Jednotlivé fáze životního cyklu BCM jsou následující:

- Pochopení činností organizace (různé analytické aktivity);
- Vytvoření strategie;
- Tvorba a implementace plánů;
- Testování, udržování a přezkoumávání BCM;
- Vytvoření a upevňování kultury BCM.

¹ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 16.

Těmto základním fázím životního cyklu BCM předchází samotné stanovení programu a politiky BCM. Rozhodující vliv na úspěšné zavedení systému plánování kontinuity činností v organizaci má vytvoření a upevňování kultury BCM a její zahrnutí do celkového řízení. Implementaci systému řízení kontinuity činností (BCMS – Business Continuity Management System) popisuje druhá část normy BS 25999. BS 25999 – 2, která prosazuje procesní přístup založený na základě Demingovu cyklu PDCA (Plan – Do – Check – Act).

Ilustrace: Životní cyklus BCM.²



Životní cyklus BCM [BS 25999-1:2006]

Životní cyklus BCM³

Stanovení odpovědností

Management společnosti by měl určit osobu zodpovědnou za politiku a implementaci BCM do organizace. Jednat by se mělo o osobu s příslušnou autoritou, jak přirozenou tak formální. Je nezbytné, aby tato osoba (např. vlastník, předseda představenstva, zvolený představitel apod.) měla plnou odpovědnost za zajištění trvalého úspěchu BCM v oblasti jeho způsobilosti. Dále je potřeba určit osobu popřípadě celý tým pro implementaci a udržování programů BCM. Tyto osoby mohou být z různých částí organizace v závislosti na její velikosti a složitosti organizační struktury. Pokud to struktura organizace vyžaduje, je možné určit v jednotlivých odděleních osobu nebo osoby, které budou nápomocny při implementaci BCM. Veškeré odpovědnosti, pravomoci a role všech těchto určených osob by měly být uvedeny v popisech práce a kompetenčních profilech. Zároveň by tyto svěřené kompetence a odpovědnosti měly být předmětem auditů a organizace by měla zajistit jejich zakotvení v politice hodnocení a odměňování.

² British Standards Institution, překlad a interpretaci pro prostředí v České republice vytvořila společnost Risk Analysis Consultants.

³ Business Continuity Institute <http://www.thebci.org/>

Implementace kontinuity činností do organizace

Při implementaci programu kontinuity činností organizace by veškeré činnosti měly zahrnovat návrh, tvorbu a implementaci programu. Je třeba, aby organizace komunikovala o programu se zainteresovanými stranami, zajistila zaměstnancům příslušné školení v této problematice a procvičovala způsobilost kontinuity činností organizace. Pro efektivní řízení implementace je možné zavést některou metodu projektového managementu.⁴

Nepřetržitý management

Všechny součásti způsobilosti kontinuity činností je třeba neustále přezkoumávat a přehodnocovat. Je potřeba je tedy pravidelně revidovat, testovat a aktualizovat dle potřeby. Navíc by opatření a plány kontinuity činností měly být přezkoumávány a aktualizovány při výskytu závažné změny v operačním prostředí, procesech, technologiích nebo v zaměstnancích (např. fluktuace zaměstnanců) a také vždy když testování nebo incident odhalí nedostatky.

Jsou činnosti, které je nutné vykonávat jak na počátku, tak neustále. Patří sem:

- stanovení rozsahu kompetencí a rolí ve vztahu k BCM;
- určení konkrétní osoby nebo týmu, pro dosažení neustálé způsobilosti BCM;
- udržování aktuálnosti programu kontinuity činností organizace prostřednictvím správné praxe;
- podporování kontinuity činností uvnitř i vně organizace;
- správa programů procvičování;
- pravidelné přezkoumávání a aktualizace způsobilosti kontinuity činností organizace, včetně přezkoumání a aktualizace relevantních rizik a analýzy dopadů;
- správa dokumentace;
- monitorování výsledků způsobilosti kontinuity činností organizace;
- řízení nákladů, ustanovení režimů managementu změn a managementu úspěchů ve vztahu ke kontinuitě činností organizace.

Vrátíme se k výše zmiňované **dokumentaci BCM**. Tuto dokumentaci by měly vytvořit a spravovat osoby pověřené udržováním kontinuity činností organizace. Dokumentace by měla zahrnovat:⁵

- politiku BCM;
 - o prohlášení o předmětu BCM;
 - o působnost BCM;
- analýzu dopadů;
- posuzování rizik a hrozeb;
- strategii BCM;

⁴ Projektový management je disciplína zahrnující plánování, organizování a řízení, která směřuje k úspěšnému zvládnutí a dosažení plánovaných specifických cílů.

⁵ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 19.

- programy připravenosti;
- programy školení a výcviku;
- plány managementu incidentů;
- plány kontinuity činností organizace;
- plány obnovy činností organizace;
- rozvrhy a záznamy o testování;
- dohody a smlouvy o úrovni služeb.

Porozumění organizaci

Cílem této fáze životního cyklu BCM je porozumění činnostem organizace prostřednictvím identifikace klíčových produktů nebo služeb a stanovení činností a zdrojů, které je zajišťují. Díky této části je program BCM v souladu s cíli, závazky, povinnostmi a zákony, jimiž je organizace vázána. Tato fáze životního cyklu se skládá ze dvou částí, **analýzy dopadů** a **analýzy rizik**. Výstupy z těchto dvou analytických činností slouží jako poklad pro výběr nejefektivnější strategie.

Analýza dopadů

Analýza dopadů (Business impact analysis – BIA) je společně s analýzou rizik nejdůležitější fáze životního cyklu kontinuity podnikání. Jen BIA umožní organizaci definovat procesy, které jsou pro ni kritické a pro zachování fungování naprosto nezbytné. S tím souvisí i definování dalších vlastností procesů jako je stanovení:

- a) cílové doby obnovy aktivity (Recovery time objective – RTO);
- b) maximální doby výpadku (MAO ~ MTPD);
- c) nezbytných zdrojů pro zachování kritických procesů (lidské zdroje, znalosti, technické zdroje);
- d) maximální ztrátu dat (MTDL) / cílový bod obnovy (RPO);
- e) kritického období procesu (časovou citlivost);
- f) interních i externích závislostí posuzovaných aktivit;
- g) požadavků na potřebné softwarové vybavení technických zdrojů a další.

Naproti tomu, analýza rizik nám umožní poznat hrozby, kterým mohou organizace čelit a které mohou mít za následek přerušení činností organizace.

Každá firma si vytváří svou vlastní analýzu dopadů na základě své velikosti, zaměření a možností. Analýza dopadů tedy není typ dokumentu one-size-fits all, ale musí respektovat typ a velikost organizace. Mezinárodní norma BS 25999-1 vymezuje vstupy, které mají být při provádění analýzy dopadů vzaty v úvahu (např. obchodní cíle organizace, zájmy a cíle zainteresovaných stran), následně poté v bodě 6.2.2 popisuje požadované výstupy (např. maximální doba přerušení, minimální úroveň služeb, která musí být v případě výpadku dodržena, maximální doba k návratu k normálu organizace aj.). Nicméně, již dále neuvádí, jakým způsobem ji provádět.⁶

⁶ Tuto situaci se snaží částečně napravit nová ISO norma 22313 i Good Practice Guideline 2013.

Prvním krokem k úspěšné analýze dopadů **je tvorba správné metodologie**. Metodologie analýzy dopadů přesně popisuje proces provádění, odpovědnosti v procesu sběru a zpracování dat jakož i celkové nakládání s dokumentací (aktualizace, přístupnost jen vybraných osobám apod.). Jak již bylo zmíněno výše, neexistuje jeden univerzální dokument pro všechny organizace, ale musí se vycházet z podmínek, v jakých jednotlivá organizace působí a vytvořit metodologii ušitou přesně na míru jejich potřeb⁷. Správně nastavená metodologie zajistí komplexnost a konzistentnost sesbíraných dat.

Při vytváření metodologie se musí originátor rozhodnout, zda pro hodnocení dopadů využije metodu kvalitativní, kvantitativní popřípadě kombinaci obou. Při kvalitativní analýze hodnotitel vychází především ze svých zkušeností a při hodnocení dopadu si vystačí s označení dopadu „nízký“, „střední“, „vysoký“ a „velmi vysoký“. Při kvantitativním způsobu hodnocení dopadů vstupují do analýzy i konkrétní finanční částky (ztráty z důvodu nedostupnosti procesu, aktivit nebo poskytování produktu)⁸. V metodologii ať již kvantitativní nebo kvalitativní je velmi důležité stanovení vhodného časového rámce pro hodnocení dopadů výpadku aktivity. Tzn., že hodnotitel bude hodnotit velikost dopadu v předem definovaném časovém úseku např. 1 hodina od výpadku, 4 hodiny od výpadku, 8 hodin, 2 dny, 1 týden atd. Časový úsek se liší od typu organizace. Například finanční společnosti jsou velmi citlivé na výpadky a vysoký dopad může mít i výpadek, který trvá velmi krátkou dobu. Naproti tomu u některých výrobních společností může být rámec definován v delších časových úsecích například 1 den, 1 týden, 2 týdny, 1 měsíc, 2 měsíce⁹.

Metodologie musí také definovat způsob a kategorie hodnocení kritičnosti. Obecně je pro stanovení kategorií kritičnosti procesů a aktivit doporučení definovat 3 až 4 kategorie (např. „velmi důležitý“, „důležitý“, „vedlejší“, „nedůležitý“)¹⁰.

Dále je v metodologii nezbytné definovat způsob sběru informací. Existuje několik doporučených způsobů, například formou interview s vedoucími pracovníky odpovědnými za konkrétní činnost, dotazníků, workshopů nebo mohou být využity jiné interní i externí zdroje¹¹. Na závěr musí metodologie definovat, jak budou shromážděné informace dále zpracovány, zda organizace využije některý speciální softwarový nástroj pro řízení kontinuity činností nebo zda si vystačí např. MS Office Excel, požadavky na aktualizaci a určení způsobu finální validace vedením společnosti.¹²

⁷ KOSUTIC, Dejan, Becoming Resilient: The Definitive Guide to ISO 22301 Implementation, EPPS Services Ltd, Zagreb 2013, ISBN 978-953-57452-3-5.

⁸ Záleží na organizaci, co všechno zahrne do ztrát, zdali jen ztrátu vyplývající z nedodání produktů a s tím spojené sankce, nebo zahrne i další související náklady jako jsou například náklady na pronájem náhradních prostor, náhradních zařízení, případně započte i možné sankce od regulátorů.

⁹ Zde je potřeba brát v úvahu Service Level Agreement (SLA) společnosti. V některých případech mohou být i výrobní podniky velmi citlivé na výpadky.

¹⁰ Anglicky psaná odborná literatura uvádí pojmy např. Mission-Critical, Vital, Important, Minor apod.

¹¹ BIRD, Lyndon, Good Practice Guidelines 2010: Global Edition, The Business Continuity Institute, London 2010, s. 51.

¹² Doporučeno je aktualizovat minimálně jednou ročně nebo při významné změně v organizaci.

Způsob sběru dat

Jak je již zmíněno výše, můžeme pro sběr informací využít interview, dotazník, workshop nebo jiné interní a externí zdroje. Každá metoda má své výhody, ale i nevýhody. V následujícím odstavci se pokusím zhodnotit klady i zápory všech zmíněných způsobů.

Interview

Osoba odpovědná za oblast business continuity (např. BC manažer) provádí interview se všemi vedoucími pracovníky, kteří jsou odpovědní za aktivity určené k implementaci řízení kontinuity.¹³ Na začátku interview BC manažer uvede vedoucího pracovníka do problematiky řízení kontinuity i analýzy dopadů a vysvětlí mu důvody a přínos této fáze, následně je proveden (polo)strukturovaný rozhovor. Rozhovor by měl vycházet z předem vytvořeného dotazníku nebo seznamu otázek. Po ukončení interview a zpracování odpovědí do výstupní zprávy je nezbytná validace hodnotitele. Výhodou je osobní kontakt hodnotitele a vedoucího pracovníka, naopak nevýhodou této metody je velká časová náročnost.

Dotazník

Pokud BC manažer využije ke sběru dat metodu dotazníku, musí počítat s tím, že vytvoření samotného dotazníkového formuláře může zabrat spoustu času. Otázky v něm musí být relevantní, jasné, stručné a dotazník musí být velmi jednoduchý na vyplnění. BC manažer může vytvořit dotazník na webovém rozhraní a odpovědným vedoucím poslat pouze odkaz (i s připomínkou termínu odeslání zpět) nebo může rozeslat dotazník v papírové formě. Jelikož nedochází k osobnímu kontaktu mezi BC manažerem a hodnotitelem, je nezbytné uvést i kontakt, na koho se mohou hodnotitelé v případě nejasností nebo nepochopení otázky obrátit. Tímto se částečně zmírní riziko nepochopení otázky, zaujaté nadhodnocení aktivit apod. Po zpracování dotazníků je vhodné a užitečné seznámit hodnotitele se zjištěnými výsledky.

Workshop

Je společné setkání BC manažera (který plní roli facilitátora) se všemi vedoucími pracovníky (hodnotiteli) procesů a aktivit, při němž je, stejně jako u interview, podrobně a názorně vysvětlena celá metodologie analýzy včetně praktických ukázek. I při tomto způsobu sběru dat je nezbytné vytvoření seznamu otázek, které jsou součástí agendy workshopu.

Jiné interní i externí zdroje

Může se jednat například o analýzu obchodních smluv, interních dokumentů, instrukcí, zákonů, nařízení a dalších. Tento způsob je však považován za pouze za podpůrný k výše uvedeným.

¹³ Nebo všech aktivit v organizaci – tento předpoklad musí být definován v metodologii BIA, případně v Politice nebo Programu BCM.

Jednotlivé fáze analýzy dopadu

Analýzu dopadu lze obecně rozdělit do následujících kroků:¹⁴

- 1) Identifikace a ohodnocení oblastí.
- 2) Identifikace procesů a podprocesů v každé oblasti.
- 3) Hodnocení procesů a podprocesů.
- 4) Vyhodnocení analýzy.
- 5) Zpráva z BIA.

Ad 1) Identifikace a ohodnocení oblastí:

Definování jednotlivých oblastí, jejich procesů a podprocesů je jedním ze základních stavebních kamenů analytické fáze. První krok představuje stanovení jednotlivých oblastí, které budou hodnoceny. Analýza dopadů se zpravidla vykonává plošně pro celou organizaci a v převážné většině případů se oblasti posuzují na základě organizační struktury organizace¹⁵, které zodpovídají za procesy v jednotlivých oblastech (například oddělení lidských zdrojů; marketingu; obchodu; informačních technologií, logistiky atd.)

Ad 2) Identifikace procesů a podprocesů v každé oblasti:

Každé oddělení v organizaci by mělo mít vlastní přehled činností a aktivit, které provádějí v rámci svých každodenních aktivit¹⁶. Pro účely hodnocení dopadů lze aktivity rozdělit na strategickou, taktickou a operativní úroveň.

- Pod *strategickou úroveň* můžeme zařadit činnosti, jako jsou například: řízení společnosti, strategické plánování, projektové plánování, rozvoj obchodu apod.
- Pod *taktickou úroveň* řadíme např. IT, lidské zdroje, finance.
- Pod *operativní úroveň* řadíme např. výrobní proces, prodej, logistika, skladování, zákaznický servis, nákup a řízení dodavatelů, další jiné podpůrné služby jakou jsou zajištění bezpečnosti podniku, údržbu objektu apod.¹⁷

Ad. 3) Ohodnocení procesů a podprocesů:

Procesy a podprocesy jsou hodnoceny podle předem vypracované metodologie.

¹⁴ SZABADOS, Ľubomír, et al, Business Continuity Management: Příručka manažera, TATE International Slovakia, Bratislava 2008, s. 115 – 126.

¹⁵ Pokud se jedná o procesně řízenou organizaci, posuzují se jen procesy, bez ohledu na oddělení.

¹⁶ Seznam aktivit je obvykle v organizacích uveden u popisu pracovního místa.

¹⁷ Nejnovější vydání Good Practice Guidelines z roku 2013 také rozděluje BIA na „Strategickou“, „Taktickou“ a „Operativní“. Nicméně již neuvádí konkrétní příklady oddělení, ale jen doporučuje pod strategickou analýzu dopadu zahrnout nejdůležitější procesy a služby organizace, do taktické BIA pak procesy a služby, které jsou vyžadovány pro fungování nejdůležitějších procesů a služeb. V operativní BIA jsou dále rozpracované procesy a služby uvedené v taktické BIA, včetně požadavků na zdroje. Nový GPG navíc ještě definuje „Úvodní“ (Initial BIA), která rozvíjí analytický rámec pro upřesnění BCM programu.

Ad. 4) Vyhodnocení analýzy:

Všechny informace shromážděné napříč organizací je nutné vyhodnotit a zpracovat do výsledné výstupní zprávy. Tato činnost je obvykle určena odpovědné osobě za řízení kontinuity činností v organizaci. Nejčastěji se jedná o BC manažera, který zajišťuje, že informace budou zhodnoceny komplexně, nezaujatě a konzistentně.

Ad. 5) Zpráva z BIA:

Měla by obsahovat záměr organizace, cíle, kritické procesy, finanční a nefinanční dopady způsobené přerušением jednoho nebo více kritických procesů, cíle BCM, minimální požadavky na zdroje, klíčové zákazníky, dodavatele, stanovení cílové doby obnovy (Recovery time objective; RTO), rozpis priorit, profil obnovy zdrojů potřebných na obnovu. Závěrečnou zprávu obvykle zpracovává BC manažer a předkládá ji k finálnímu schválení vedení společnosti.¹⁸

Příklady kvalitativní a kvantitativní vyhodnocení analýzy dopadu

Níže je uveden příklad k posouzení cílové doby obnovy (RTO) a maximální tolerované doby výpadku (MTO) ve výrobní společnosti, která dodává výrobky na základě aktuálního požadavku zákazníka (**oddělení logistika, proces vyřizování objednávek**).

Jak je vidět, v režimu just-in-time jsou přijímány objednávky i několikrát v průběhu dne, tzn., že kritické období nelze přesně časově vymezit (je v podstatě neustále). Již při jedné hodině výpadku vzniká středně vysoký dopad na dodání produktu. S tím souvisí i finanční ztráty z nevyrobených produktů, právní dopady z nedodržení smluvních podmínek i dopady na dobré jméno podniku. Naproti tomu, po celou dobu výpadku procesu přijímání objednávek je dopad na bezpečnost a zdraví zaměstnanců, stejně jako regulační na velmi nízké úrovni.

Cílová doba obnovy je tedy vedoucím pracovníkem (manažerem logistiky) určena do 1 hodiny – nejvyšší prioritou je v tomto případě dodržení smluvních podmínek. Maximální doba výpadku (MTO) je z důvodu vysokého dopadu na doručení produktu definována na 4 hodiny.

Tabulka: Vyhodnocení cílové (RTO) a maximální doby přerušení (MTO) a kritického období

	RTO		MTO				
Vyřizování objednávek	1 hodina	4 hodiny	1 den	3 dny	2 týdny	1 měsíc	Kritické období
Finanční dopad	L	M	M	H	VH	VH	průběžně
Dopad na jméno společnosti	L	M	M	M	M	H	
Dopad na zdraví a bezpečnost zaměstnanců	L	L	L	L	L	L	
Regulační dopad	L	L	L	L	L	L	
Právní dopad	L	M	M	H	H	VH	
Dopad na doručení produktu	M	H	VH	VH	VH	VH	

L – low / nízký M – medium / střední H – high / vysoký VH – very high / velmi vysoký

¹⁸ Nutnost oficiální validace analýzy dopadů i další dokumentace je obvykle předem stanoveno v BCM programu nebo v BCM politice.

Pokud není ve společnosti zpracován popis procesu, pro komplexní zhodnocení procesu je vhodné tyto informace v rámci analýzy dopadu sesbírat. Tím, že definujeme vstupy i výstupy snadněji definujeme interní závislosti.

Tabulka: Popis procesu Vyřizování objednávek

Vyřizování objednávek	odpovědná osoba / minimální počet osob pro zajištění provozu procesu	požadované vstupy	kdo poskytuje vstupy	požadované výstupy	kam směřují výstupy

Tabulka: Vyhodnocení interních a externích závislostí respektive požadavků

Vyřizování objednávek	interní závislosti	externí závislosti	IT požadavky	požadavky na technické zdroje

Popis jednotlivých kategorií:

Interní závislostí představuje závislost na interním procesu, aktivitě nebo službě.
 Externí závislost rozlišujeme na upstream a downstream:

- Upstream = dodávky zboží nebo služeb třetí stranou ve prospěch společnosti.
- Downstream = dodávky zboží a služeb společnosti pro jiné oddělení, pro třetí stranu, pro zákazníka atd.

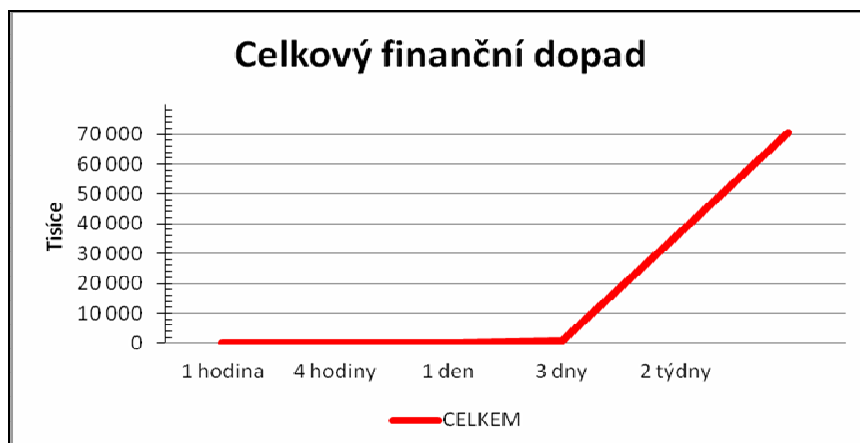
IT požadavky na proces = využívané aplikace a další software pro zajištění procesu.
 Technické zdroje = hardware, telekomunikační zařízení aj.

Tabulka: Finanční dopad – kvantitativní analýza dopadů

Vyřizování objednávek	1 hodina	4 hodiny	1 den	3 dny	2 týdny	1 měsíc
Finanční dopad (ušlý výdělek)	5 000	20 000	250 000	750 000	35 000 000	70 000 000
Finanční dopad (smluvní, regulační pokuty)			20 000	60 000	280 000	560 000
Další náklady						
CELKEM	5 000	20 000	270 000	810 000	35 280 000	70 560 000

Pro komplexní posouzení dopadů je vhodné definovat i finanční ztráty, které mohou vzniknout v případě narušení procesu – vyřizování objednávek.

Tabulka: Grafické vyhodnocení finančních dopadů



Jak je možné vyčíst z grafu, při nedostupnosti aktivity 1 hodiny jsou dopady na nízké úrovni, za 4 hodiny jsou finanční dopady již na úrovni středně vysoké a při výpadku, který potrvá 3 dny, jsou dopady vysoké. Po dvou týdnech finanční dopady dosahují velmi vysoké úrovně. Tyto výše uvedené údaje o procesu slouží pro správné určení prostředků pro zmírnění dopadu i výběru business kontinuity strategií¹⁹.

Závěr

Výše uvedeným způsobem je nutné ohodnotit všechny aktivity a procesy u všech²⁰ oddělení organizace. Poté BC manažer zkonsoliduje výsledky a zpracuje zprávu z BIA, která je **společně s analýzou rizik** využita v dalších částech životního cyklu – **Vytvoření strategie a Implementace odezvy**.

Vytvoření strategií BCM

Poté co byla provedena analýza okolí organizace a identifikace vlivů, které na ni mohou působit, přichází na řadu fáze výběru strategie nebo strategií, s jejichž pomocí bude organizace dosahovat svých cílů.

Při určování strategií BCM je nezbytné, aby byla implementována všechna opatření, která vedou ke snížení pravděpodobnosti vzniku mimořádných událostí nebo alespoň ty, které vedou k redukci jejich možných dopadů. Je třeba zahrnout opatření k zabezpečení odolnosti²¹ a zmírňujících opatření, dále je nutné zajistit kontinuitu kritických činností během i po vzniku přerušení a nesmí být opomenuty ani ty činnosti, které nebyly označeny jako kritické.

Organizace by měla zvážit možnosti strategií pro kritické činnosti a zdroje, které budou nezbytné pro obnovu těchto činností. Výběr nejvhodnějších strategií se bude odvíjet od určujících faktorů, jako jsou maximální tolerovatelná doba přerušení kritických činností,

¹⁹ Více informací v části "Stanovení strategie řízení kontinuity činností".

²⁰ Všechny oddělení nebo jen ty, které byly vybrány pro implementaci kontinuity činností.

²¹ Resilience – odolnost neboli schopnost organizace odolat zasažení incidentem.

náklady nutné pro implementaci strategií a důsledky nečinnosti. Strategie je možné stanovit pro několik „druhů“ zdrojů (viz níže).

Strategie pro lidské zdroje. Měla by být stanovena strategie pro zabezpečení základních dovedností a znalostí, a to nejen u zaměstnanců, ale i u smluvních partnerů a dalších zainteresovaných stran, které mají odborné dovednosti a znalosti, které spoluvytváří hodnoty organizace. Takovéto strategie určené k zajištění těchto dovedností a znalostí mohou zahrnovat:²²

- záznamy o způsobu vykonávání kritických činností;
- školení a výcvik dovedností personálu a smluvních partnerů;
- separaci základních dovedností, tak aby nemohly být ve stejný čas a na stejném místě zasaženy tím samým incidentem (může se jednat například o fyzické rozmístění personálu s těmito dovednostmi nebo zajištění těchto dovedností u více osob);
- využívání třetích stran;
- plány následnictví;
- uchovávání znalostí a management znalostí.

Strategie vztahující se k prostorům provozů. Tyto strategie by měly stanovit přístupy pro snížení dopadů na pracovní prostory a místa. Může se jednat o:²³

- alternativní prostory uvnitř organizace,
- alternativní prostory smluvně zajištěné u jiných organizací,
- alternativní prostory poskytnuté specializovanými třetími stranami,
- umožnění práce z domova a jiných vzdálených přístupů,
- další odsouhlasené vhodné prostory,
- využití alternativní pracovní síly ve stanoveném místě.

Jedná se tedy o náhradní provozovny, které jsou k dispozici, pokud jsou normální provozy nefunkční. Při stanovování těchto prostor je třeba dbát na určité zásady. Prostory by měly být od normálních prostor vzdáleny tak, aby byla minimální pravděpodobnost, že budou oba provozy zasaženy stejnou mimořádnou událostí, avšak musí být v takové vzdálenosti, aby personál byl ochoten a schopen se do nich přemístit. Je dobré si uvědomit, že některé činnosti je mnohem snazší převést na specializované třetí strany (smluvně zajištěné alternativní služby poskytované formou outsourcingu apod.), než přemístit personál do alternativních prostor.

²² ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 26.

²³ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 27.

Strategie vztahující se k technologiím. Tyto strategie se budou odvíjet od podstaty využívané technologie a jejích vazeb na kritické činnosti, ale vždy půjde o jednu nebo o kombinaci těchto strategií vztahující se k:²⁴

- technologiím vyvinuté organizací;
- technologiím poskytovaných nebo pořízených organizací od vnější organizace;
- technologii provozované externí třetí stranou, v rámci služby pronajaté naší organizací.

Technologické strategie, by měly obsahovat geografické rozmístění technologií (např. provoz obdobných technologií na různých místech, resp. ve více provozech, pro redukci rizik), skladování a údržbu staršího vybavení jako záloh a náhrad, zmírnění rizik pro unikátní technologie nebo technologie s dlouhou životností.

Jedny z nejvýznamnějších technologií pro veškeré organizace jsou v současné době informační technologie a ty tudíž vyžadují komplexní strategie kontinuity. Při určování těchto strategií je třeba dbát na:

- cílové doby obnovy IT systémů a jejich aplikací, které zajišťují kritické činnosti;
- umístění a vzdálenosti mezi technologickými lokacemi;
- počet technologických lokací;
- vzdálený přístup a jeho odolnost vůči proniknutí do systémů;
- telekomunikační kanály a redundanci spojů;
- politiku „čistého stolu“ (zamezit personálu opouštět pracovní místa, aniž by se odhlásili ze systému, mít hesla napsané na monitoru PC apod.);
- zapojení třetích stran do této oblasti.

Jak již bylo zmíněno, tato část je v dnešní době velice choulostivá. Proto se jí budeme ještě chvíli věnovat. V případě, že je IT organizace rozmístěna na více místech, je možné stanovit pro ně společné strategie. Obnova může být zajištěna tak, že systémy, síť a paměti na jednotlivých provozech jsou schopny zajistit operace ostatních nad rámec operací vlastních. Je potřeba zajistit ochranu a možnost obnovy dat, důležitých pro chod organizace, v souladu s časovým rámcem určeným během analýzy dopadů. Doporučuje se systém zrcadlového zálohování, během kterého jsou veškerá systémová data duplicitně zálohována automaticky a také zajištění obnovitelnosti dat rozšířením jejich formátu (fyzické formáty a elektronické formáty).

Strategie vztahující se k dodávkám. Je třeba, aby organizace vytvořila a spravovala seznam hlavních dodávek, které jsou nutné pro zajištění kritických činností. V rámci této strategie mohou být zavedena opatření jako:²⁵

- uložení rezervních dodávek na jiném místě;
- smluvní zajištění dodávek s třetími stranami v krátkém časovém úseku;

²⁴ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 28.

²⁵ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 29.

- vytvoření překladišť pro just-in-time dodávky v jiném místě;
- udržování materiálů ve skladištích nebo přepravních místech;
- přemístění operací do náhradního místa, které je blíže ke zdroji dodávek;
- určení alternativ pro dodávky.

Pokud jsou některé kritické činnosti závislé na jedinečných dodávkách, je potřeba, aby organizace identifikovala klíčové dodavatele těchto dodávek. Jestliže není možné zvýšit počet dodavatelů, vzhledem ke specifičnosti dodávek, je třeba od nich vyžadovat zavedení BCM, popřípadě prokázání způsobilosti kontinuity jejich činností. Doporučuje se smluvní zajištění úrovně služeb poskytovaných dodavateli a požadovat zaručení se za poskytování jedinečných dodávek.

Strategie vztahující se k zainteresovaným stranám. Při určování veškerých strategií by organizace měla zohledňovat zájmy klíčových zainteresovaných stran. Zaměstnanci, zákazníci, dodavatelé, partneři, distributoři, investoři, pojišťovny, akcionáři, majitelé, vláda a správní orgány, každá z těchto skupin vyžaduje zvláštní zvážení, každá z nich může vyžadovat specifická opatření k zajištění jejich zájmů. Zvláštní pozornost při tvorbě strategií je nutno věnovat dotčeným správním orgánům. Veškerá opatření a BCM jako takový by měly být minimálně konzultovány s věcně a místně příslušnými orgány veřejné správy.

Vývoj a implementace odezvy BCM

V předchozích fázích cyklu BCM organizace identifikovala své kritické činnosti, stanovila hrozby, které jsou pro tyto činnosti relevantní, určila vhodnou strategii pro snížení pravděpodobnosti a dopadů incidentů, a také pro zajištění kontinuity nebo obnovy kritických činností. Ve fázi vývoje a implementace odezvy BCM se jedná o vytvoření a zavádění příslušných plánů a opatření vedoucích k zajištění kontinuity činností organizace.

Struktura odezvy na incident. Je třeba, aby organizace stanovila takovou strukturu odezvy na mimořádnou událost, která zajistí efektivní odezvu a obnovu po vzniku přerušení. Tyto struktury by měly být jednoduché a rychle utvořitelné, aby v případě incidentu převzala kontrolu nad vzniklou situací, potlačila její následky a byla schopna komunikovat se zainteresovanými stranami. Mluvíme zde o týmu krizového řízení nebo jakkoliv jinak pojmenovaném týmu, který zodpovídá za tyto činnosti. Pro činnost týmu krizového řízení je nutné zajistit plány, procesy a postupy pro řízení mimořádných událostí a ty by měly být podpořeny nástroji kontinuity činností organizace pro zajištění kontinuity činností a jejich obnovy.

Plány. Veškeré plány, které má organizace vypracované, musí být stručné, jasné a přístupné pro všechny, jež mají v těchto plánech stanoveny odpovědnosti. Velikost organizace určuje rozsah plánovacích dokumentů, pokud se jedná o malé podniky, mnohdy postačuje jeden plán, který pokrývá veškeré požadavky na činnosti a celý provoz. U velkých organizací lze očekávat více plánů, které detailně řeší určité činnosti, prostory nebo scénáře.

Pro každý plán musí být top managementem stanoveny a odsouhlaseny účel a předmět. Účel a předmět musí být pochopen těmi, kdo budou provádět plánem stanovené

postupy. Veškeré vazby mezi plány a ostatními dokumenty musí být jasně určeny, také je nezbytné stanovit postupy vedoucí k získání a k přístupu k těmto plánům. Každý plán managementu incidentu, kontinuity činností organizace a obnovení činností organizace má mít prioritně seřazené cíle vzhledem k obnově kritických činností, časovým rámcům pro obnovu, úrovní obnovy potřebným pro každou kritickou činnost a situacím, při kterých je možné plán použít. V plánu musí být jasně stanoveno, kdo má jaké kompetence, role a odpovědnosti při plnění úkolů stanovených plány, tzn. musí být určeny osoby, případně týmy, kterých se to týká.

Vyvolání plánů, resp. metody, kterými jsou aktivovány relevantní plány nebo jejich části, v co nejkratším čase po vzniku incidentu způsobujícího přerušení, je třeba jasně stanovit a zadokumentovat. Také je potřeba určit jedince, kteří mají pravomoc za předem stanovených podmínek vyvolat relevantní plány. Aktivace procesů, které jsou určeny plány, může vyžadovat okamžitou mobilizaci zdrojů organizace, proto je nutné, aby plány obsahovaly přesný popis a určení:²⁶

- jak budou mobilizovány týmy;
- prostor nebo jiných shromažďovacích bodů;
- následných pracovišť pro krizový management, resp. jiná centra odkud budou veškerá opatření a operace koordinována.

Podnik by měl určit osobu, která bude zodpovědná za přezkoumávání, hodnocení, doplňování a aktualizaci plánu, prováděné v pravidelných intervalech. Plány by měly obsahovat kontaktní informace na klíčové pracovníky a zainteresované strany. Při uvádění kontaktů dostupných mimo pracovní dobu, je třeba dbát na ochranu soukromých dat.

Plán managementu incidentu (IMP). Jedná se o plán upravující postupy a opatření prováděná v úvodní fázi incidentu²⁷. Takový plán by měl být flexibilní, proveditelný a relevantní. Musí být přehledný a snadno pochopitelný, a přitom musí poskytovat základ pro řízení všech problémů, které bude muset organizace ihned po vzniku incidentu řešit. Plán musí mít oporu u vrcholového vedení organizace a v neposlední řadě musí být podpořen příslušným rozpočtem pro jeho vývoj, udržování a školení nebo výcvik.²⁸ IMP by měl, kromě výše zmíněných obecných doporučení obsahu, zahrnovat:

- a) **Seznam úkolů a kontrolní seznam činností**, které je nutné zajistit ihned po vzniku přerušení. Úkoly by na prvním místě měly řešit zajištění životů a zdraví osob. Úkoly a činnosti musí vycházet z analýzy dopadů a být konstruovány tak, aby nebyly v přímém rozporu se strategickými a taktickými stanovisky organizace. Dále jimi musí být zajištěno předcházení dalším ztrátám, nepřerušení kritických činností a zdrojů.
- b) **Kontakty pro případ stavu nouze**. Je potřebné zajistit jasné stanovení pravidel a okolností, za kterých bude organizace komunikovat uvnitř a vně podniku. Bude se jednat o protokoly pro komunikaci s médii, zaměstnanci, zainteresovanými stranami, rodinnými příslušníky personálu apod. Seznamy kontaktů je třeba udržovat aktuální

²⁶ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 35.

²⁷ Může se jednat o požární poplachové směrnice, požární evakuační plány aj.

²⁸ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 36.

a dostupné. (Pro tak choulostivou oblast, jako je komunikace s rodinnými příslušníky personálu nebo médií, je vhodné disponovat předem připravenými a vyškolenými pracovníky.).

- c) **Lidské činnosti.** IMP by měl identifikovat osobu zodpovědnou za zajištění evakuace, mobilizaci různých bezpečnostních týmů, týmů první pomoci apod. V rámci plánu by tato osoba měla být zodpovědná za vytvoření a provozování systému, který bude evidovat a lokalizovat, všechny osoby přítomné na pracovišti i v okolí organizace. Také by tato osoba měla zajišťovat bezpečnostní instruktáže a komunikace s personálem, zákazníky a dalšími zainteresovanými stranami. Je také nezbytné určit personál zmocněný ke spojení a komunikaci se složkami integrovaného záchranného systému. Efektivita záchranných a likvidačních prací složek integrovaného záchranného systému může být zlepšena, pokud je nastolena spolupráce mezi organizací a těmito pohotovostními službami.
- d) **Management zainteresovaných stran.** Je třeba, aby se organizace zaměřila na proces identifikace a hierarchické seřazení klíčových zainteresovaných stran. Pokud je to nezbytné, může být vytvořen zvláštní plán managementu zainteresovaných stran k zajištění jejich priorit, případně jim přidělit osobu zodpovědnou za prosazování zájmů těchto stran.
- e) **Místo managementu incidentu.** Jak již bylo zmíněno, je třeba stanovit prostory a místa odkud bude řízena odezva na vzniklou situaci. Tyto prostory musí být vybaveny tak, aby bylo možné v reálném čase sledovat vývoj situace a zároveň vydávat rozhodnutí a opatření. Prostředky pro komunikaci, sdílení a přístup k informacím musí mít kromě primárního i sekundární zajištění. Dobrá komunikace je nezbytná. Z těchto míst by měl být zajištěn přístup ke zdrojům, pomocí kterých tým bez prodlení může zahájit efektivní činnosti managementu incidentu.
- f) **Dodatky.** IMP by měl zahrnovat detaily mobilizace a kontakty na všechny relevantní agentury, organizace a zdroje, nezbytné pro podporu strategií odezvy organizace. Také by měl obsahovat formuláře pro vytvoření záznamů o dění během incidentu (časový průběh, ztráty, učiněná rozhodnutí, náklady, apod.), neboli takové informace, které mohou být důležité pro přezkoumání po incidentu a na jejichž základě může být celý systém vylepšen. V rámci dodatků IMP může jít o mapy, grafy, plány a další vizuálně zjednodušené informace, které mohou být důležité pro řešení incidentu. Také mohou obsahovat dokumentované strategie odezvy schválené třetí stranou (partnery, dodavateli, apod.). Dále mohou být zahrnuty detaily o skladech, vybavení a vyčkávacích prostorách a také požadavky na postupy managementu, které zajišťují, že veškerá pojištění a právní nároky organizace splní požadavky stanovené jim ve smlouvách.

Plány kontinuity činností organizace (BCP). Cílem těchto plánů je, aby byla organizace v případě vzniku přerušení schopna obnovit nebo udržet své činnosti na úrovni běžného provozu.²⁹ Tyto plány jsou zavedeny pro podporu kritických činností, kterými organizace dosahuje svých cílů. Obsah a struktura těchto plánů může být různá v závislosti na velikosti organizace, druhu jejich činností a jejím okolí. Obsahem BCP by měly být:

²⁹ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 39.

a) Plány činností a kontrolní seznamy úkolů. Strukturovaný kontrolní seznam činností a úkolů, které je nutné provést v závislosti na jejich prioritě pro udržení činností v normálním chodu, může celý tento proces výrazně zpřehlednit a usnadnit. Plány činností je nutné zaměřit na:³⁰

- způsob aktivace BCP;
- osobu odpovědnou za učiněná rozhodnutí a vyvolání BCP;
- postupy, které musí být těmito osobami splněny při činění rozhodnutí;
- osobu, se kterou musí být obsah rozhodnutí konzultován před jeho vydáním;
- osobu, kterou je nutné informovat o učiněném rozhodnutí;
- stanovení toho, který personál jde kam a kdy (např. v případě vzniku přerušení je možné některé zaměstnance poslat domů pro zajištění jejich bezpečnosti a zůstávají jen klíčoví zaměstnanci, neboli ti, kteří jsou nezbytní pro zajištění předem stanovené úrovně chodu kritických činností);
- určení dostupnosti služeb, resp. stanovení toho, kde a kdy budou dostupné a také jak organizace mobilizuje externí zdroje a zdroje třetích stran;
- způsoby komunikace a podávání informací v této oblasti;
- pokud je to nutné, objasnit detailní postupy manuálních úkolů a činností, které je nutné učinit pro zotavení systému.

b) Požadavky na zdroje. Veškeré zdroje potřebné pro zajištění kontinuity činností organizace a obnovu těchto činností je nezbytné identifikovat v různých časových bodech. To může zahrnovat:³¹

- lidi neboli jejich bezpečnost, potřeby blaha, pohotovostní výdaje a přepravní logistiku;
- prostory;
- technologie včetně těch, které zajišťují komunikaci;
- informace o financích, záznamech zákazníků, dodavatelích a zainteresovaných stranách;
- právní dokumenty (smlouvy, pojistné smlouvy apod.) a dokumenty, týkající se služeb (dohody o úrovni poskytovaných služeb třetími stranami);
- dodávky;
- management komunikace a komunikace se zainteresovanými stranami.

c) Odpovědné osoby. Opět je nutné určit osoby odpovědné za správné řízení fází kontinuity činností a obnovy činností organizace po přerušení.

d) Formuláře a dodatky. Může se jednat o aktuální kontaktní informace na agentury, organizace a další poskytovatele, kteří mohou být potřební pro podporu organizace. Co se

³⁰ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 40.

³¹ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 41.

týče formulářů, půjde zejména o zajištění záznamů o průběhu zajištění kontinuity činností a obnovy činností organizace po přerušení a o záznam učiněných rozhodnutí pro pozdější přezkoumání.

Další typy plánů, které jsou součástí BCP plánu, řadíme např. IT plány obnovy (DRP plán), Plán obnovy zasažené lokality, Plán k návratu aktivit do původní lokality, Plán pro vypořádání backlogu produkce aj.

Testování, udržování a přezkoumávání opatření BCM

V této fázi BCM zajišťuje organizace validitu provedených opatření, jejich testování a přezkoumání a také to, aby byla tato opatření aktuální. Žádná opatření nemohou být považována za spolehlivá, pokud nebyla testována a není udržována jejich aktuálnost. Testování je také důležité pro rozvinutí týmové spolupráce, odborné způsobilosti a znalostí, které jsou životně důležité při vzniku přerušení v důsledku mimořádné události.

Pro zajištění komplexního systému testování a přezkoumávání BCM by organizace měla vyvinout **program testování**. Ten by měl být navrhnut tak, aby byl schopen zaručit, že v případě potřeby bude plán kontinuity fungovat, jak bylo předpokládáno. Program by měl testovat opatření zavedená v rámci BCM a validovat obnovu technologií a telekomunikací, včetně dostupnosti a přemístění personálu.

Program testování vede ke zlepšení způsobilosti BCM prostřednictvím testování schopnosti obnovení činností organizace po vzniku incidentu a současně vede k ověření, že BCM zahrnuje veškeré kritické činnosti organizace, jejich vzájemné vazby a priority. Také zvyšuje sebedůvěru účastníků testování v oblasti BCM.³² Zveřejnění výsledků testování posiluje povědomí o důležitosti BCM pro organizaci. Vede ke zlepšení způsobilosti také prostřednictvím ověření efektivnosti a včasnosti obnovení kritických činností a prokázání tak odborné způsobilosti týmu BCM.

Testování opatření, kterým budeme ověřovat jejich funkčnost, by mělo být realistické, pečlivě naplánované a odsouhlasené zainteresovanými stranami, aby bylo minimalizováno riziko přerušení činností organizace. Mělo by se také naplánovat tak, aby byla pravděpodobnost vzniku přerušení během testování co nejmenší.³³ Pro testování je třeba určit jejich záměry a cíle. Ihned po ukončení testování by se měla uskutečnit porada, analýza a zhodnocení toho, zda byly záměry a cíle dosaženy.³⁴ Následně by měla být vypracována zpráva s vyhodnocením obsahující doporučení a stanovující časový rozvrh pro zavedení navrhovaných opatření³⁵. V rámci programu testování by také měly být zváženy role všech stran (klíčoví poskytovatelé služeb, outsourcingové firmy apod.), jejichž účast na obnově je nezbytná.

³² ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 43.

³³ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 46.

³⁴ Good Practice Guidelines 2013 označuje tuto aktivitu jako „Hot debrief“.

³⁵ Good Practice Guidelines 2013 označuje tuto aktivitu jako „Formal debrief“.

Existuje řada typů a názvů testů, které jsou kategorizovány podle obsahu, složitosti nebo účastníků. V principu však můžeme rozdělit testy na několik základních kategorií:³⁶

- a) cvičení založené na diskuzi; walk-through test; desk check test; orientační seminář³⁷ a analýza scénářů;
- b) functional testing;
- c) full testing, field testing, full interruption test.

Ad a) cvičení založené na diskuzi; walk-through test; desk check test; orientační seminář; analýza scénářů

Jedná se o nejjednodušší způsob testování s nízkými náklady na provedení. Pokud není implementace řízení kontinuity v organizaci dostatečně rozvinutá, je vhodné začít s těmito jednoduchými testy, jelikož tyto testy nenesou velké riziko narušení činnosti organizace z důvodu neúspěšného testu. Účastníci tohoto cvičení jsou členové krizového týmu (vedoucí oddělení, jejichž procesy jsou označeny jako kritické nebo jejichž oddělení bylo vybráno pro implementaci řízení kontinuity činností), dále pak osoba, která vytvořila plán (BC manažer), případně další zainteresované strany.

Cílem tohoto cvičení je bližší seznámení s doposud vydanou dokumentací a korekce případných chyb. Členové krizového týmu prochází dokumentaci řádek po řádku a diskutují o jednotlivých krocích, zvažují, zda jsou opatření stále aktuální, zda je zachována logická posloupnost aktivit a další.

Analýza scénářů – je speciální nástroj, který využívají především finanční instituce, které podléhají regulacím dle BASEL II (BASEL III) a přijaly nejpokročilejší metodu hodnocení operačních rizik (AMA – Advanced Measurement Approach). Analýza scénářů umožňuje hodnotit výši ztrát při výskytu rizika s nízkou frekvencí a vysokým dopadem (například výpadek IT systému, povodeň, zemětřesení, blackout aj.), tedy rizikem, pro něž je jako mitigant nastaven mimo jiné i systém řízení kontinuity činností. Scénář analyzuje různé možnosti průběhu události, od mírného zasažení až po nejhorší možné dopady (tzv. worst case scenario). Tento worst-case scénář pak dále slouží jako vstupní informace pro stresové testy³⁸ finanční instituce.

Ad b) functional testing

Do funkčního testování řadíme cvičení typu „Tabletop“. Tabletop je teoretické cvičení, na němž členové krizového týmu řeší konkrétní předložený scénář. Tento druh testu je realističtější, ale časově náročnější a klade vyšší požadavky jak na členy krizového týmu tak

³⁶ SNEDAKER, Susan, Business Continuity & Disaster Recovery: For IT professionals, Syngress Publishing Inc, 2007, ISBN 978-1-59749-172-3.

³⁷ KOSUTIC, Dejan, Becoming Resilient: The Definitive Guide to ISO 22301 Implementation, EPPS Services Ltd, Zagreb 2013, ISBN 978-953-57452-3-5.

³⁸ Guidelines on Operational Risk Management, Österreichische Nationalbank, Wien 2006.

http://www.fma.gv.at/typo3conf/ext/dam_download/secure.php?u=0&file=2142&t=1361498469&hash=7c291b0b9c9083fede76dd6a0f69b714

i na BC manažera, který obvykle plní funkci facilitátora. Tabletop cvičení může trvat i několik hodin a předpokládá hlubší znalosti BC dokumentace. Scénář cvičení může celý probíhat v reálném čase, ale může obsahovat i „časový skok“. I když je tento test považován pouze za teoretický, pro vyšší reálnost se nabízí možnost spojení např. s nácvičkou požární evakuace, který je v některých společnostech prováděn pravidelně každý rok.³⁹

Ad c) full testing, (field testing, full interruption test)

Tento typ testu je časově, finančně a organizačně velmi náročný. Je obvykle realizován ve společnostech, jejichž provoz je velmi rizikový (chemické továrny, jaderné elektrárny, mezinárodní letiště aj.) a v průběhu testu jsou hlavní činnosti společnosti zastaveny, případně přesunuty do náhradního pracoviště. Obvykle jsou do tohoto cvičení zapojeny nejen interní bezpečnostní složky (například podnikový hasiči) ale i složky integrovaného záchranného systému.

Pro většinu společností je tento test téměř nerealizovatelný, jelikož ztráty způsobené přerušením provozu jsou pro management společnosti nepřijatelně vysoké.

Udržování opatření BCM. Měl by být zaveden program udržování, který organizaci zajistí, že jakékoliv změny, které mohou mít vliv na podnik, budou včas identifikovány a posléze budou zavedena taková opatření v rámci BCM, která na tyto změny budou reflektovat. Některé změny mohou vyžadovat revizi analýzy dopadů a úpravu ostatních částí BCM tak, aby odpovídaly těmto změnám. Účelem procesu udržování BCM je zajištění způsobilosti managementu kontinuity činností organizace, resp. toho, že zůstává efektivní a aktuální.

Přezkoumávání opatření by mělo být vrcholovým vedením prováděno v opakujících se časových intervalech a zhodnotit tak způsobilost BCM, jeho stabilitu, adekvátnost a efektivitu. Přezkoumání by mělo ověřit, že politika BCM je v souladu s právními předpisy, strategiemi a směrnicemi správné praxe. Mělo by také odhalit možné požadavky na změnu politiky, strategií a cílů systému managementu kontinuity činností. V souvislosti s neustálým zlepšováním je třeba odhalovat příležitosti (nové technologie a přístupy), které je třeba zhodnotit z pohledu jejich přínosu pro organizaci a případně je implementovat.

Přezkoumání může být prováděné formou **interních nebo externích auditů⁴⁰, formou sebehodnocení, auditem prováděný oddělením kvality nebo posouzení výkonnosti (měření pomocí indikátorů KPI)**. Časové intervaly opakování přezkoumání mohou být ovlivněny zákony, velikostí a povahou organizace nebo požadavky zainteresovaných stran. Audit nebo program sebehodnocení by měly být zaměřeny především na:⁴¹

- klíčové produkty organizace a kritické činnosti a zdroje, které byly identifikovány a zahrnuty do strategie BCM organizace;

³⁹ Po evakuaci všech zaměstnanců z budovy se členové krizového týmu sejdou na jiném, předem definovaném místě, kde budou řešit předložený scénář „Požár v prostorech společnosti“, který je předem připravený BC manažerem.

⁴⁰ Externí audity se mohou dále dělit na certifikační, zákaznické nebo audity regulátora.

⁴¹ ČSN BS 25999-1 Management kontinuity činností organizace – Část 1: Soubor zásad, 2009, s. 47.

- politiky, strategie, pracovní rámec a plány BCM;
- oprávněnost a způsobilost BCM organizace, zda jsou efektivní a vhodné pro svůj účel;
- programy udržování a testování BCM organizace, zda byly efektivně implementovány;
- program školení nebo výcviku pro ověření, zda jimi organizace disponuje;
- postupy a role personálu, zda s nimi bylo efektivně komunikováno o BCM a zda tento personál pochopil své role a odpovědnosti;

V současné době je nastavení výkonnosti systému řízení kontinuity činností (KPI) velkou výzvou. Velkou pozornost tomuto tématu věnuje také nejnovější Good practice Guidelines 2013⁴², který zdůrazňuje, že měření výkonnosti by mělo sloužit ke kontrole, jak dobře byly vykonávány role a odpovědnosti za BCM, které jsou uvedeny v dokumentu Politika řízení kontinuity. KPI může obsahovat například následující činnosti:

- počet vykonaných naplánovaných cvičení;
- procento dokončení BIA;
- počet vypracovaných plánů;
- počet neshod, chyb nebo nálezů vyplývajících např. z incidentů, z průběhu cvičení nebo z auditů;
- procento nevyužitého rozpočtu.

Hodnocení splnění činností by mělo být provedeno nejméně jednou ročně⁴³.

Začlenění BCM do kultury organizace

V poslední fázi životního cyklu kontinuity činností organizace jde o zavedení výsledků všech předchozích fází do prostředí firmy tak, aby se stal BCM součástí organizace a její kultury. Aby byl management kontinuity činností organizace úspěšný, musí se stát součástí způsobu řízení organizace.

Vytvoření, podpora a implementace kultury BCM do organizace zajišťuje, že se stane součástí základních hodnot a efektivního managementu organizace. Organizace se zavedenou a kladnou kulturou BCM může efektivněji vytvářet program BCM a lépe zavádět veškerá opatření v rámci BCM. Taková organizace budí u zainteresovaných stran (u personálu, zákazníků, pojišťoven apod.) důvěru v její schopnost zvládat přerušení svých činností. Zároveň zvyšuje svou odolnost tím, že problematika kontinuity činností je známa a řešena na všech úrovních a také je minimalizována pravděpodobnost dopadu přerušení.

Pro zavedení kultury BCM do organizace je nezbytné, aby byla podporována vedením společnosti ze sféry top managementu. Také je nutné přidělovat odpovědnosti a zvyšovat připravenost školením nebo výcvikem dovedností a testováním plánů. Všechny personál musí pochopit význam BCM pro organizaci a také to, že právě oni mají klíčovou roli při udržování kontinuity činností. Pro budování připravenosti je nutné personál vzdělávat v oblasti BCM prostřednictvím informačních programů BCM. Může jít o konzultace s celým

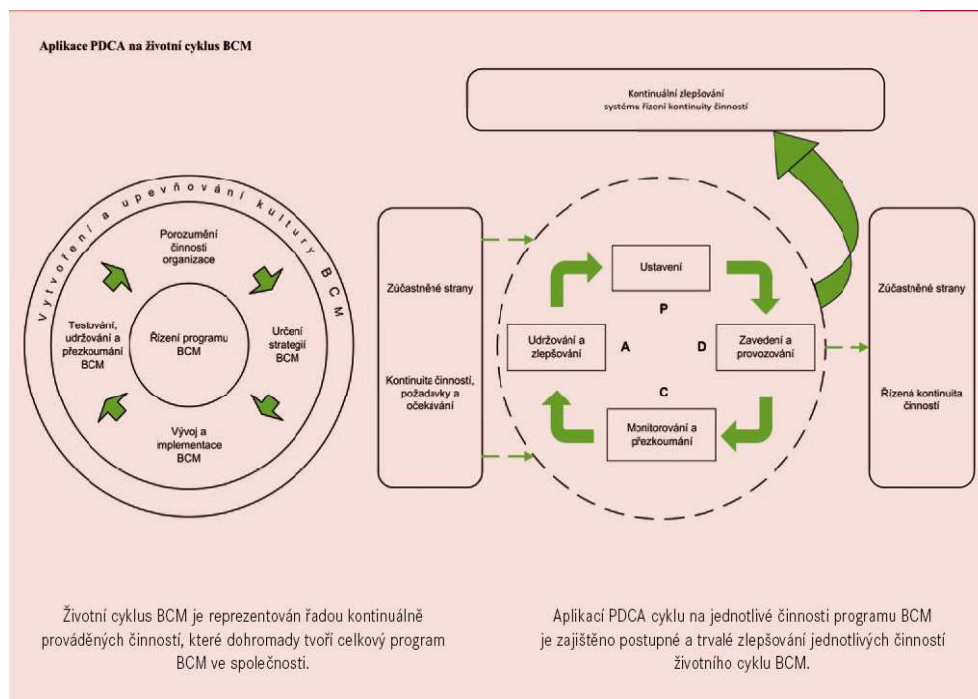
⁴² Srov. Good Practice Guidelines z roku 2010, kapitola Maintenance.

⁴³ Například při ročním hodnotícím pohovoru s nadřízeným.

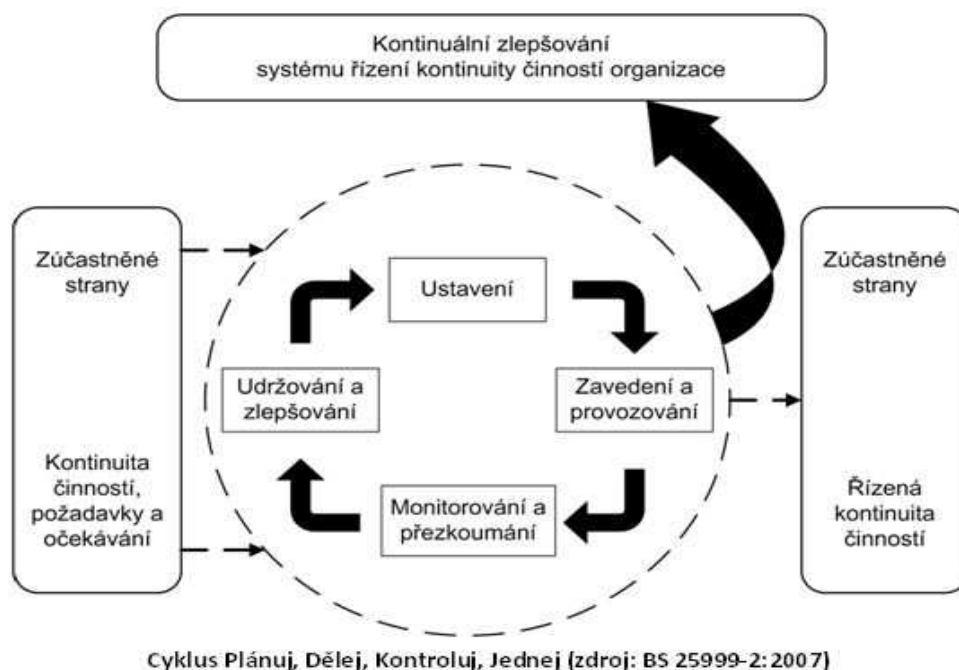
personálem organizace o zavádění BCM, diskuze v rámci porad, informační letáky a různé oběžníky, e-learningové kurzy, začlenění BCM na webových stránkách firmy, poučení se z interních a hlavně externích incidentů, procvičování plánů kontinuity v alternativních provozech a prostorech, apod. Organizace může svůj program připravenosti rozšířit na své dodavatele a další zainteresované strany.

Je třeba také provádět školení nebo výcvik dovedností zejména v oblastech managementu programu BCM, analýzy dopadů, vytváření a implementace plánů kontinuity činností organizace, programu testování plánů kontinuity činností organizace, posuzování rizik a hrozeb a také v komunikaci s médii. V neposlední řadě je nezbytné školení v dovednostech, které jsou nezbytné při odezvě na incident a obnovu činností organizace.

Ilustrace: Aplikace PDCA na životní cyklus BCM⁴⁴



Ilustrace: PDCA cyklus⁴⁵



⁴⁴ ŠIROKÝ, Libor. Od Golfu k certifikaci BCMS. Data Security Management. 2010, 3
 <<http://www.rac.cz/rac/homepage.nsf/CZ/Clanky>>.

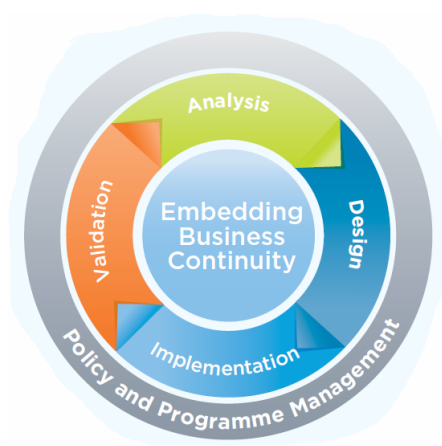
⁴⁵ BS 25999 – 1:2007. Business continuity management. Specification. London: British Standards Institution, 2007. 28 s.

Nové přístupy k nastavení životního cyklu BCM

Životní cyklus řízení kontinuity činností je založen na modelu PDCA, který je základním vyjádřením opakování procesů v moderním řízení. V průběhu let, kdy se teoretické poznatky ověřují v praxi, však na základě získaných zkušeností dochází postupně k určitým inovacím, které by měly vést k dosažení větší efektivity plánovaných i realizovaných opatření a především ke zvýšení odolnosti organizace proti možným dopadům nepředvídaných mimořádných událostí na jejich kritické činnosti.

Jedna ze změn, k nimž odborníky v oblasti řízení kontinuity činností dovedly praktické výsledky řízení, se týká i přehodnocení posloupnosti některých fází životního cyklu řízení kontinuity činností.

V současné době se tak prosazuje model, z něhož je zřetelněji patrné, že úvodním krokem životního cyklu musí být program a politika řízení kontinuity činností, které „obklopují“ čtyři „technické“ fáze životního cyklu: Analýzu, Návrh, Implementaci a Ověření. Jádrem, které musí být bráno během těchto čtyř fází bezpodmínečně v potaz je etablování řízení kontinuity řízení ve firemní kultuře a všeobecně akceptovaném modelu řízení organizace.⁴⁶



- **Analýza:** Tato část životního cyklu je věnována sledování a hodnocení organizace v podmínkách, ve kterých objektivně funguje, včetně vlivů a dopadů ve vztahu k okolí organizace.
- **Návrh:** Identifikuje a vybírá vhodné strategie a taktiky k určení, jak má být dosaženo kontinuity činností a pokrytí případných výpadků.
- **Implementace:** Uplatnění schválených strategií a taktik prostřednictvím zpracování či zdokonalení příslušných plánů řízení kontinuity činností (Business Continuity Plan).
- **Ověření:** Potvrzení, že program řízení kontinuity činností odpovídá cílům vytýčeným v politice řízení kontinuity a že příslušné plány jsou připraveny tak, aby plnily účely, pro které byly v organizaci zpracovány.⁴⁷

⁴⁶ BCI Good Practice Guidelines 2013 Global Edition

<http://www.thebci.org/index.php/resources/the-good-practice-guidelines>

⁴⁷ Good Practice Guidelines 2013 Global Edition: A Guide to Global Good Practice in Business Continuity, s. 13.