Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra informačních technologií

Student	: Jan Zdvořáček
Vedoucí bakalářské práce	: Ing. Tomáš Bruckner, Ph.D.
Oponent bakalářské práce	: Ing. Kateřina Martanová

TÉMA BAKALÁŘSKÉ PRÁCE

Business Continuity Management a IT

ROK: 2011

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze kterých jsem čerpal.

V Praze dne 30. 6. 2011 ....

podpis

Poděkování

Na tomto místě bych rád poděkoval panu Ing. Tomáši Brucknerovi, Ph.D. za vedení bakalářské práce, za jeho čas obětovaný konzultacím a za jeho cenné rady při zpracování práce. Dále bych rád poděkoval panu Ing. Markovi Štvanovi za konzultace a rady ohledně praktické části.

Abstrakt

Cílem této práce je provedení analýzy plánu pro zachování kontinuity služeb v reálné společnosti. K tomu je potřeba položit určité teoretické základy, nejprve v oblasti Business Continuity Managementu, a to k pochopení jeho významu pro organizaci, pochopení jeho implementace a jeho následného operativního řízení. Další část shrnuje teoretické poznatky o odvětví Business Continuity Managementu nazývaného IT Service Continuity Management. Ten je již konkrétněji zaměřen na kontinuitu poskytování služeb IT, které jsou v dnešní době pro zachování kontinuity businessu klíčové. Neboť drtivá většina všech business procesů je informačními a komunikačními technologiemi podporována. Porozumění základním pojmům tvoří pouze teoretickou základnu pro následující část a tou je analýza strategií na zachování kontinuity činnosti v konkrétní firmě.

Hlavním přínosem bude, na základě nabytých znalostí, provedení praktické analýzy IT Service Continuity plánu v reálné společnosti působící na českém trhu. Celý plán bude analyzován a vyhodnocen, tam kde bude prostor, budou navržena doporučení na možná zlepšení, která by umožnila zvýšit efektivitu tohoto plánu. Z této analýzy budou vyvozeny obecné závěry.

Klíčová slova

Business Continuity Management, IT Service Continuity Management, analýza.

Abstract

The aim of this thesis executes a service continuity analysis in a real company. To achieve this we must lay certain theoretical bases, first of all in Business Continuity Management area and that in comprehending its significance for the organisation, understanding its implementing and its consequent operative management. The following part sums up theoretical knowledge in Business Continuity Management branch called IT Service Continuity Management. IT Service Continuity Management is specifically focused on continuity in providing IT services, which play a key role in continuity preserving nowadays. It is even more so as the majority of business processes are supported by information and communication technologies today. Understanding the basic terms creates only a theoretical basis for the next part, which focuses on strategy analysis of preserving service continuity in a specific company.

The greatest benefit of this thesis will be, based on the knowledge achievement, executing a practical IT Service Continuity Plan analysis in a real company located on the Czech market. The whole plan will be analysed and evaluated and recommendations for potential improvement in the plan's efficiency increase will be suggested where applicable. General conclusion shall be drawn based on this analysis.

Keywords

Business Continuity Management, IT Service Continuity Management, analysis.

Obsah

Úvod

Každý si jistě uvědomuje, že žijeme v době, která je více či méně poznamenána fenoménem informací. Mají významný vliv na celou společnost. Informace hýbou světem, staly se tím nejdražším a nejcennějším a podle toho je s nimi nutné zacházet. Technický pokrok dospěl do stavu, kdy jsou informační technologie natolik rozšířené, že relativně zmenšují svět. Ale jak je jistě známo, jedná se jen o stroje, které mohou selhat. Přesněji řečeno, lze předpokládat, že jednou selžou, je jen otázkou kdy. A na takovouto situaci je dobré být připraven.

Tak jako je již téměř nemožné oddělit informační technologie z každodenního života nás všech, tak nelze oddělit informační technologie od činnosti jakékoliv organizace. I zde platí nepsané pravidlo, že „cokoliv se může pokazit, pokazí se“. A právě pro tyto situace jsou určeny procesy IT Service Continuity Managementu, ten je nedílnou součástí Business Continuity Managementu, který přináší komplexnější řešení problematiky.

Stanovené cíle této bakalářské práce je možné shrnout do následujících třech bodů:

- teoretické shrnutí poznatků o Business Continuity Managementu, které je nutné pro zpracování praktické části,
- teoretický základ IT Service Continuity Managementu, jehož poznatky jsou také potřeba k provedení analýzy,
- na základě získání teoretických znalostí provést analýzu plánu kontinuity společnosti z reálného tržního prostředí, vyhodnotit ji a případně navrhnout možná zlepšení.

Tomuto uspořádání bude odpovídat i budoucí struktura celé práce.

První kapitola plní jeden z hlavních cílů této práce, teoretické seznámí s problematikou Business Continuity Managementu, bude se snažit zasvětit čtenáře do používané terminologie, popsat proces implementace a následného řízení této disciplíny v již fungující organizaci. Zásadním přínosem je jistě i fakt, že lze zatím jen velmi těžko hledat zdroje informací o této manažerské disciplíně, v českém jazyce. Doufám, že tato práce by se mohla stát jedním z nich.

Další část se bude věnovat jednomu odvětví Business Continuity Managementu a tím je IT Service Continuity Management. Přínosem pro čtenáře jsou informace o IT

Service Continuity Managementu, jak ho lze implementovat, jak zapadá do celkového konceptu BCM a jak klíčovou roli pro organizaci hraje.

Business Continuity Management (ITSCM nevyjímaje) je již teoreticky zpracován na velice dobré úrovni, jak jsem se již zmiňoval, bohužel ne v českém jazyce. Avšak jeho praktická implementace do reálného provozu je na opravdovém začátku. Jako všude, i zde hrají roli finanční zdroje. Implementaci takto složitých procesů si zatím dovolují pouze větší, resp. dobře prosperující organizace. Proto bude obsahem poslední části názorná ukázka konkrétního procesu z reálné praxe, na kterém bude vysvětleno, jak lze jednotlivé procesy zanalyzovat, vyhodnotit rizika, dopady, jak připravit konkrétní plán na zachování kontinuity. Pomocí této praktické části se jistě mnohem lépe osvětlí i mnoho poznatků z teoretické části.

Věřím, že pro mnohé čtenáře jsou pojmy v názvu práce velká neznámá, opravdových odborníků na tuto problematiku je dosud velmi málo, do vědomí odborné veřejnosti se toto téma teprve postupně dostává. To je jeden z důvodů, proč jsem si toto téma vybral. Přínosy práce vidím jak v její teoretické části, kde by mohl hledat inspiraci manažer, který chce svou organizaci bránit proti nenadálým událostem. Tak je samozřejmě hlavním přínosem část praktická, protože jak lépe vysvětlit a obhájit teorii než na funkční praktické ukázce.

1 Business Continuity Management

Následující kapitola se bude zabývat manažerskou disciplínou označovanou anglickým termínem Business Continuity Management, odtud má původ i často používaná zkratka BCM. Tento termín bývá do českého jazyka nejčastěji překládán jako řízení kontinuity činnosti organizace.

1.1 Definice

V odborné literatuře lze narazit na dvě definice Business Continuity Managementu (dále jen BCM):

- Business Continuity Management je holistickým[1] procesem managementu, který identifikuje potenciální dopady ohrožující organizaci a poskytuje rámec pro vytvoření odolnosti se schopností efektivní reakce, která chrání zájmy jejích klíčových investorů, dobrou pověst, značku a činnosti vytvářející hodnoty. (BS 2599)
- Business Continuity Management je proces, který zabezpečuje činnosti organizace, ale neomezuje je.[2]

Tyto definice vypovídají mnohé o termínu BCM. Hned úvodem bych ale doplnil ještě jeden klíčový poznatek k pochopení BCM. Nejedná se o jednorázovou aktivitu organizace, nýbrž BCM je vždy součást firemní kultury.

1.2 Význam

Posláním každé organizace je, na základě vstupů, produkovat výstupy, to mohou být výrobky nebo služby. Tento proces je závislý na mnoha vnitřních i vnějších faktorech, jejichž spolehlivost je značně individuální. Posláním nebo významem BCM je eliminovat veškeré škody a následky selhání některého z těchto faktorů. Toho docílí analýzou možných rizik a přípravou plánů k jejich nápravě.

[1] Holismus je filosofický směr, který zdůrazňuje fakt, že celek je více než souhrn všech částí. Všechny vlastnosti nějakého systému nelze určit nebo vysvětlit pouze zkoumáním jeho částí.

[2] Převzato z prezentace BCM Jak obnovit procesy z pohledu IT? (Martanová, 2010)

Vnímání pojmu BCM stejně tak jako uvedení do praxe se obvykle liší v závislosti na konkrétním podniku. Jeho zavádění se odvíjí od specifik daných firem, od jejich aktivit, zaměstnanců, okolí, obchodních partnerů apod. (Cihlářová, 2010)

1.3 Terminologie

Pro začátek je třeba vymezit několik často používaných pojmů, aby nedošlo k jejich dezinterpretaci.

1.3.1 Obecné pojmy

V této kapitole budou uvedeny všeobecně známé pojmy a k nim definice jak jsou chápány v souvislostech BCM. (Szabados, 2008)

1.3.1.1 Organizace

Organizace, jak bude používána v této práci, je formální skupina lidí se společnými cíli. Spojují ji čtyři základní rysy (Winkler, 2011):

- dělba práce,
- spolupráce,
- hierarchie,
- společný cíl.

1.3.1.2 Havárie

Havárie je náhlá předvídatelná nebo nepředvídatelná událost, která má vážný dopad na činnost organizace. Vede k přerušení nebo úplnému zastavení činnosti organizace. Příkladem předvídatelné havárie jsou živelné katastrofy, které lze určitý čas dopředu identifikovat (povodně či silný vítr) dále stávky, atd. Nepředvídatelná havárie je například zemětřesení a podobné nepředvídatelné živelné katastrofy či neočekávaný výpadek elektrické energie.

1.3.1.3 Přerušení

Přerušení je částečné narušení činnosti organizace, je to jakákoliv očekávaná nebo neočekávaná událost, která je příčinou narušení normálního chodu organizace a tím i jejího poskytování služeb nebo výrobků.

1.3.1.4 Incident

Slovo označující nepříjemnou událost nebo příhodu. BCM ho vnímá jako situaci, která může způsobit přerušení, ztrátu nebo krizi.

1.3.1.5 Krize, krizová situace

Kritická událost, která pokud nebude správně řešená, může mít vážný dopad na činnost organizace, její pověst a správné fungování. Je to taková událost, která ohrožuje provoz, zaměstnance, zaměstnavatele, dobré jméno, pověst, důvěryhodnost anebo strategické cíle organizace.

1.3.1.6 Kontinuita

Kontinuita znamená nepřetržité fungování bez problémů způsobených přerušením.

1.3.1.7 Proces

Proces je soubor vzájemně souvisejících anebo vzájemně se ovlivňujících činností, které transformují vstupy na výstupy (ISO 9000).

1.3.1.8 Dopad

Ohodnocený výsledek (finančně i nefinančně) působení hrozby na analyzované aktivum (organizaci).

1.3.1.9 Riziko

V českém jazyce nabývá slovo riziko mnoho významů. Riziko je cokoliv, co se může stát a bude mít vliv na dosažení cílů organizace. Nebo lze riziko vysvětlovat, jako pravděpodobnost s jakou hrozba zvyšuje zranitelnost analyzovaného systému s negativním dopadem na něj. Výraz riziko je možné chápat také jako možnost, že se něco stane.

1.3.2 Pojmy zaměřené striktně na BCM

Nyní budou definovány odborné termíny, které jsou používány pouze v rámci BCM s jejich stručným vysvětlením. (Szabados, 2008)

1.3.2.1 Kontinuita činností

Schopnost organizace plánovat a vhodně reagovat na vznik incidentu anebo narušení činnosti s cílem zabezpečení kontinuity služeb na předem definované úrovni (schopnost organizace poskytovat služby a podporu pro své zákazníky a udržovat svojí životaschopnost před, během a po výskytu incidentu).

1.3.2.2 Řízení kontinuity činností

Holistický systém řízení, který analyzuje případné hrozby a jejich dopad na činnost organizace. Poskytuje rámec pro budování odolnosti a schopnosti efektivní reakce na vznik incidentu, která ochrání zájmy klíčových vlastníků a akcionářů organizace, dobrou pověst, značku a činnosti které generují zisk.

1.3.2.3 Plán kontinuity činností

Anglicky business continuity plan (odtud zkratka BCP) je soubor zdokumentovaných procesů, který zahrnuje všechny činnosti potřebné na zabezpečení nepřetržité dodávky služeb a produktů na požadované úrovni v případě, že potká organizaci incident nebo havárie.

1.3.2.4 Plán obnovy

Zkratka DRP, z anglického disaster recovery plan, v praxi je možné se setkat i s pojmem havarijní plán, obvykle se chápe jako podmnožina BCP. Dokument popisující zdroje, činnosti, procesy, úkoly a údaje. Je zaměřený na obnovu technické a technologické infrastruktury.

1.3.2.5 Program řízení kontinuity činností

Trvalý řídící proces podporovaný vrcholným managementem a zabezpečený potřebnými zdroji, kterým se zajistí, že budou vykonány všechny potřebné kroky na identifikování dopadů potencionálních ztrát, udržování strategií obnovy a plánů, zabezpečení nepřetržité dodávky služeb a produktů prostřednictvím tréninku, údržby a monitoringu.

1.3.2.6 Kritický proces

Kritický proces, resp. je zvykem používat plurál, kritické procesy jsou takové procesy, které podporují tvorbu klíčových produktů či služeb, které slouží organizaci k dosahování obchodních cílů.

1.3.2.7 Maximální tolerovatelná doba nedostupnosti

Maximální doba, po kterou mohou být nedostupné procesy, aniž by byl ohrožen chod celé organizace. V angličtině se lze setkat s názvem maximum tolerable period of disruption, ve zkratce MTPD.

1.3.2.8 Doba obnovy činnosti

Časový úsek, ve kterém musí být obnoven kritický proces. Tuto dobu označujeme zkratkou RTO, z anglického recovery time objective.

$$RTO \leq MTPD$$

RTO je doba, v rámci které musí být, po selhání, obnoveny klíčové procesy, systémy a funkce organizace. Jde o výstup z analýzy obchodních dopadů.

1.3.2.9 Maximální tolerovatelná ztráta údajů

Množství údajů, jejichž ztrátu lze tolerovat při mimořádné situaci, aniž by tato ztráta měla dopad na klíčové procesy organizace. Jinými slovy je to mezník v čase, po kterém jsou údaje už příliš staré na to, aby dokázaly reflektovat aktuální stav činnosti organizace dostatečným způsobem. Anglicky maximum tolerable data loss – MTDL.

1.3.2.10 Analýza dopadů

Business impact analysis (BIA) je proces analyzování obchodních funkcí organizace a dopadů na tyto funkce, které mohou být způsobeny přerušením obchodní činnosti. Pomocí této analýzy organizace vyhodnotí všechny kvantitativní (finanční dopady) i kvalitativní (nefinanční – dobré jméno, reputace) dopady, které mohou nastat v případě vážného incidentu.

1.3.2.11 Cíl obnovy činností

Čas, do kterého musí být obnoveno poskytování produktů, služeb nebo činností po incidentu či havárii. Zkratku RPO opět vysvětluje anglický název recovery point objective.

$$MTPD => RTO$$

$$MTDL => RPO$$

Jeho hodnota je odvozena z hodnot MTDL získaných od odborných pracovníků z analýzy dopadů BIA.

1.3.2.12 Minimální úroveň služeb

Z anglického minimal required service level vychází zkratka MRSL, můžeme se setkat i s označením úroveň kontinuity služeb organizace (LBC, Level of business continuity). Jedná se o ten nejmenší objem poskytovaných služeb nebo výroby, díky kterému je organizace schopna dosáhnout svých stanovených cílů.

1.3.2.13 Kritický prvek selhání

Unikátní zdroj služeb, aktivit nebo procesů, který nemá žádnou alternativu a jeho selhání povede k úplnému selhání klíčových činností organizace.

1.3.2.14 Přijatelná úroveň rizika

Celková úroveň rizika, kterou je organizace připravená akceptovat nebo je připravená se mu kdykoliv postavit.

1.4 Standardizační proces BCM

V této kapitole bude nastíněno jak BCM vznikal a jak se historicky vyvíjel. Stejně jako velká část důležitých objevů, se BCM začal objevovat během války, konkrétně studené války (v letech 1947 - 1991), kdy se sovětský blok systematicky připravoval na útok ze strany Severoatlantické aliance.

BCM v podobě jak ho známe dnes, vznikal v 80. letech 20. století ve Spojených státech. Jeho rozvoj podnítil fakt, že Spojené státy americké jsou často zužovány přírodními katastrofami (tornáda, hurikány, povodně) a jeho primárním cílem bylo minimalizovat hospodářský dopad těchto rozmarů počasí. Hlavní úlohou BCM bylo předpřipravit reakce jednotlivých organizací na živelné katastrofy, tak aby byly minimalizovány škody a jejich předchozí činnost byla co nejdříve obnovena. V roce 1988 byla založena instituce Disaster Recovery Institute International, která v roce 1993 vydala první standard pro BCM (Professional Practices for Business Continuity Planners). Roku 1994 vznikl ve Velké Británii Business Continuity Institute (BCI),

který převzal americký standard jako základ své činnosti a začal ho dále rozvíjet a přizpůsobovat evropským poměrům. Z této činnosti v roce 2002 vznikl dokument Business Continuity Management: Good Practice Guidelines, který je každoročně aktualizovaný a v roce 2006 britský standard pro BCM BS 25999, u kterého v současnosti probíhá mezinárodní standardizace do systému norem ISO.

ISO (International Organization for Standardization) rezervovala sérii ISO 27000 pro normy z oblasti bezpečnosti informací a konkrétně pod názvem ISO/IEC 27031 Information technology - Security techniques - Specification for ICT Readiness for Business Continuity bude publikována norma, která bude popisovat význam informačních a komunikačních technologií pro řízení kontinuity činností organizace. Datum publikace je však dosud nezveřejněný (Risk Analysis Consultants, Nová řada ISO/IEC 27000 , 2010).

BS 25999 se dělí na dvě části. BS25999-1:2006 A Code of Practice for Business Continuity, tato část definuje jednotlivé fáze, činnosti, vstupy a výstupy, které jsou součástí procesu zavádění BCM v rámci organizace. Poskytuje doporučení a postupy pro provedení analýzy dopadů, návrh vhodných strategií, přípravu a testování plánů kontinuity (BCP). Organizace si mohou vybrat, budou-li dodržovat celý soubor postupů nebo jen část. Standard lze použít pro vlastní hodnocení nebo hodnocení mezi organizacemi. Soubor postupů neobsahuje povinné požadavky pro řízení kontinuity činností (Risk Analysis Consultants, BS 25999-1 Code of practice for business continuity management , 2010). Další částí je BS 25999-2:2007 Specification for Business Continuity Management, definuje požadavky na ustanovení, zavedení, provozování, monitorování, přezkoumávání, udržování a zlepšování zdokumentovaného systému řízení kontinuity činností (BCMS, Business Continuity Management System). Standard mohou použít interní i externí strany, včetně certifikačních orgánů, aby zhodnotily schopnost organizace splňovat regulační požadavky, požadavky zákazníků i vlastní požadavky v rámci organizace. Případná certifikace BCMS se provádí podle BS 25999-2. Standard BS 25999-2 obsahuje pouze ty požadavky, které mohou být objektivně auditovány (kontrolovány). V současnosti se jedná o jedinou normu, podle které se provádějí certifikace systémů řízení kontinuity činností (Risk Analysis Consultants, BS 25999-2 Specification for business continuity management, 2010).

1.5 Cíle BCM

Cílem BCM číslo jedna je minimalizace rizika spojeného s přerušením kontinuity podnikání a s tím spojených ekonomických ztrát. Při realizaci BCM projektu se dbá zejména na zajištění (Cihlářová, 2010):

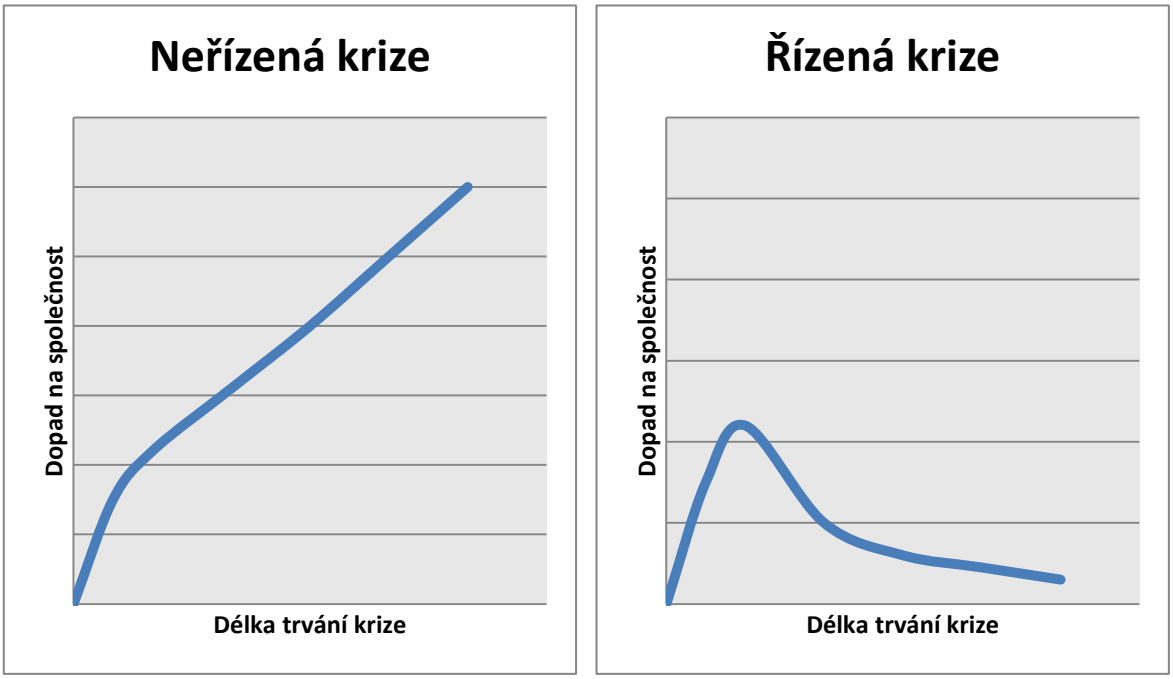
- bezpečnosti zdraví a životů personálu i obyvatelstva,
- souladu se smluvními závazky,
- interní komunikace,
- obnovy kritických procesů,
- řízení rizik,
- důvěry zákazníků a obchodních partnerů,
- dobrého jména podniku,
- pozice na trhu.

Jak bylo řečeno výše, díky BCM plánům a procesům dochází k minimalizaci ekonomických ztrát, avšak při výskytu nějaké opravdu závažné nepředvídatelné havárie nelze zapomenout na to, že ochrana zdraví všech zaměstnanců a veškerého personálu je bez jakýchkoliv výjimek vždy na prvním místě.

1.6 Mýty a fakta ohledně BCM

Zvláště v malých organizacích jsou rozšířeny chybné názory na BCM. Nejzásadnější z nich je ten, že pravděpodobnost nějaké hrozby, která naruší chod podniku je tak vzdálená a neaktuální, že odpovědní manažeři a vedoucí pracovníci ani nezvažují zavedení BCM. Což vychází z domněnky, že cena realizace BCM je příliš vysoká pro krytí rizik, které mohou nastat s tak malou pravděpodobností. Důsledkem toho dochází ke ztrátám, kterým by se podniky při realizaci BCM vyhnuly (Cihlářová, 2010). Oproti tomu stojí fakt, že pokud společnost nabízí BCM procesy, zvyšuje tím svoje uznání u zákazníků a zlepšuje si tak své jméno. Respektive mnoho zákazníků dnes služby BCM od svých dodavatelů přímo vyžaduje.

Jak bylo již řečeno, BCM je složitou součástí firemní kultury, obsahující stovky procesů a důkladnou analytickou činnost, což vyžaduje značné jak finanční tak personální zdroje. I přes to lze tvrdit, že jakékoliv jeho řešení byť jen pozměněním několika procesů, je lepší než řešení žádné. Tedy naprosté opomenutí krizového plánování. Dá se vycházet ze samotného faktu, že pokud máme na jakoukoliv činnost, alespoň nějakou, v lepším případě vhodnou strategii, vždy bude náš výsledek lepší než bez ní. Pro štěstí a náhodu není v tomto světě místo a už vůbec ne v managementu (viz Obrázek 1: Rozdíl mezi neřízenou a řízenou krizí (zdroj: Autor)).



Obrázek 1: Rozdíl mezi neřízenou a řízenou krizí (zdroj: Autor)

V posledních několika letech informační technologie značně změnily celý svět, včetně BCM. Vzhledem k tomuto fenoménu se staly všechny organizace silně závislé na ICT. Proto musí BCM této činnosti věnovat řádnou pozornost a BCM se téměř změnilo na ITCM (IT Continuity Management). Z tohoto vyplývá první chybné stanovisko, které je značně zavádějící, BCM je opravdu širší pojem a zaměřuje se na širší problematiku než pouze ICT. V praktickém pojetí však svět dosáhl situace, kdy je obnovení informačních technologií na prvním místě všech krizových plánů.

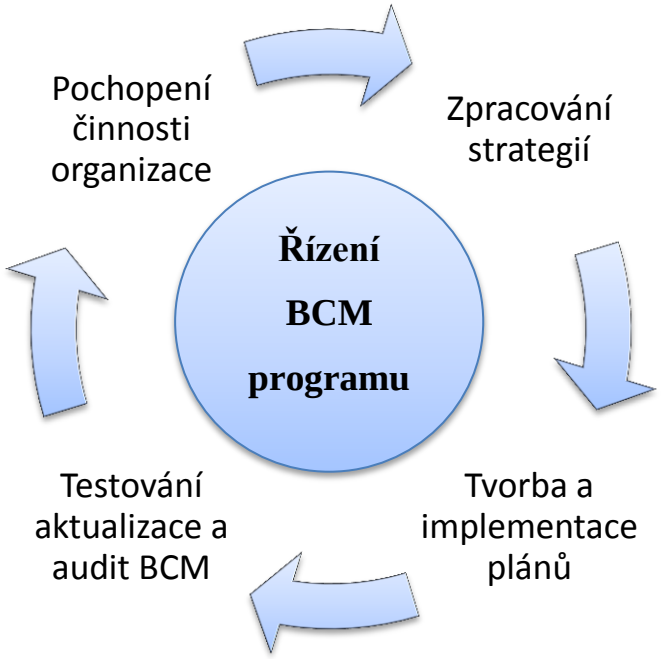
Pokud opravdu krize nastane, ať už z jakéhokoliv důvodu, je zde značný rozdíl mezi tím, pokud jsme na tuto situaci připraveni nebo pokud veškerá naše příprava spočívá pouze v naději, že pravděpodobnost krize je nízká.

Z grafu (Obrázek 1: Rozdíl mezi neřízenou a řízenou krizí (zdroj: Autor)) je patrný rozdíl mezi řízenou a neřízenou krizí. Pokud nedochází k jejímu řízení, tak

v důsledku různých konsekvencí a následných událostí dojde k nezastavitelnému růstu negativního dopadu na společnost. Pokud jsme schopni krizi řídit, dojde (samozřejmě s určitým zpožděním) k jejímu zvládnutí a tím i snížení nebo téměř anulování jejího dopadu na společnost a to v reálném čase. (Martanová, 2010)

1.7 Životní cyklus BCM

Rozhodující vliv na úspěšné zavedení BCM systému v organizaci má vytvoření firemní kultury BCM a jeho integrace do celkového systému řízení.



Obrázek 2: Životní cyklus BCM (Zdroj: Autor)

Jak říká samotná norma BS 25999-1, řízení kontinuity činnosti je kontinuální cyklický proces, který začíná stanovením BCM programu a navazujících vzájemně propojených fází (Obrázek 2: Životní cyklus BCM (Zdroj: Autor)):

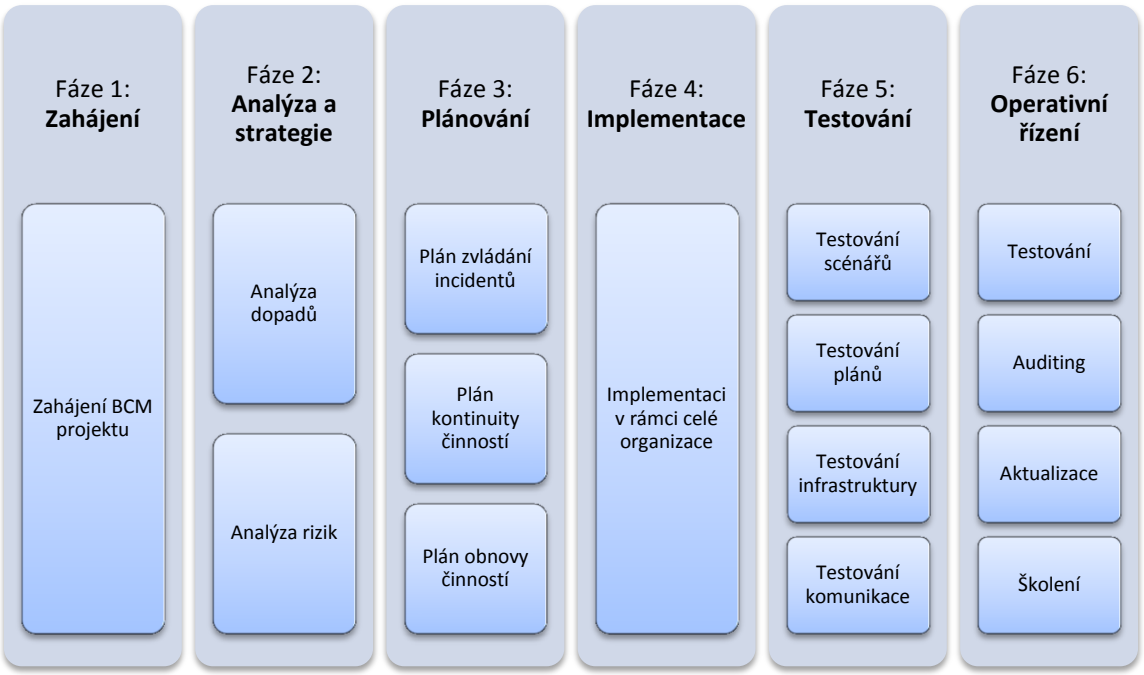
- analytické aktivity (pochopení organizace, zejména procesů činností),
- tvorba strategií,
- příprava a implementace plánů,
- testování, aktualizace a audity BCM.

1.8 Fáze BCM

Zavádění BCM je opravdu složitá množina procesů, proto je lze rozdělit do několika částí: (storyflex.cz, 2011)

- zahájení projektu,
- analýza a strategie,
- plánování,
- implementace,
- testování,
- operativní řízení.

Jednotlivé fáze obsahují několik dalších procesů, které dohromady zajišťují účinnou implementaci a funkci BCM. Jak je znázorněno na následujícím obrázku (Obrázek 3: Schéma jednotlivých fází BCM (zdroj: Autor)).



Obrázek 3: Schéma jednotlivých fází BCM (zdroj: Autor)

1.8.1 Zahájení projektu

Jak bylo již uvedeno výše, i když BCM je spíše firemní kulturou, je vhodné její zavedení odstartovat projektem. Toto rozhodnutí však musí mít plnou podporu celého managementu společnosti, protože je nezbytně nutné aby se do něho zapojil každý

pracovník organizace. Měla by být stanovena struktura, způsob vedení projektu, dále by měly být uvolněny všechny potřebné zdroje, tedy jak finanční tak personální, včetně s tím souvisejícího rozdělení zodpovědných osob za řízení BCM programu a zajištěny záruky manažerů, že se programu bude věnovat adekvátní pozornost a podpora. Mělo by dojít k vymezení základních poznatků, ze kterých bude vycházet business impact analysis (viz 1.3.2.10 Analýza dopadů). Jedná se především o stanovení klíčových aktivit společnosti, ze kterých vzejdou kritické procesy a nastavení hodnoty MTDL (maximum tolerable period of disruption, viz 1.3.2.7 Maximální tolerovatelná doba nedostupnosti). (Szabados, 2008)

1.8.2 Analýza a strategie

Nezbytným úvodem do fáze analýzy je pochopení podnikových procesů a jejich vzájemných vazeb. To je naprosto klíčové, protože pokud analýza vychází z chybných předpokladů, je velmi pravděpodobné, že i její závěry budou špatné. Cílem analytického týmu bude tedy hlavně:

- identifikace cílů, závazků a povinností organizace,
- identifikace zdrojů podporujících dosažení stanovených cílů,
- identifikace a vyhodnocení hrozeb, které mohou být příčinou narušení kritických procesů.

V této fázi projektu je důležité se zaměřit jak na závislosti a vazby mezi procesy, tak na vztahy ke třetím stranám. Průběh všech analytických aktivit, lze rozdělit do dvou kroků:

- analýza dopadů (BIA)
- analýza rizik.

1.8.2.1 Analýza dopadů

Business impact analysis je opravdu tím jádrem BCM, během ní dochází k identifikaci, ale i kvantifikaci dopadů přerušení nebo narušení klíčových procesů. V jejím rámci se stanový i minimální úroveň zdrojů potřebných na stanovení RTO (viz 1.3.2.8 Doba obnovy činnosti), RPO (viz 1.3.2.11 Cíl obnovy činností), LBC (viz 1.3.2.12 Minimální úroveň služeb). Cílem této analýzy je identifikace:

- klíčových (kritických) procesů organizace,

- dopadů na organizaci v případě vzniku incidentu, narušení nebo havárie v případě, že organizace nemůže vykonávat klíčové procesy. Součástí analýzy je i vyhodnocení finančních nákladů, tato suma se skládá z:
    - přímého finančního hodnocení,
    - nákladů na náhradu majetku,
    - nákladů spojených s obnovením kontinuity činnosti organizace,
    - ušlého zisku,
- hodnoty RTO.

Výstupy této analýzy vymezují oblast a rozsah strategie obnovy organizace, dalo by se tedy říci hlavní cíle BCM. Dalšími výstupy jsou hodnoty MTPD (viz 1.3.2.7 Maximální tolerovatelná doba nedostupnosti) i s požadavky na zdroje a RPO (viz 1.3.2.11 Cíl obnovy činností). Tyto výstupy analýzy dopadů slouží jako vstupy pro fázi zpracování strategií. Otázkou je, jak často tuto analýzu provádět. Doporučení zní jednou ročně, či dříve v případech, kdy dojde k výrazným změnám na trhu, kde organizace působí, významným technologickým změnám, změnám ve vnitřních procesech organizace nebo nějakým zásadním změnám vnějších vlivů[3] na organizaci. (Szabados, 2008)

1.8.2.2 Analýza rizik

Při hodnocení rizik je vhodné položit si pro hodnocení hrozeb, které mohou podnik potkat, tři jednoduché otázky (Cihlářová, 2010):

- S jakou pravděpodobností se hrozba realizuje?
- Jaké budou následky této hrozby?
- Které faktory by mohly snížit tuto pravděpodobnost nebo dokonce eliminovat riziko úplně?

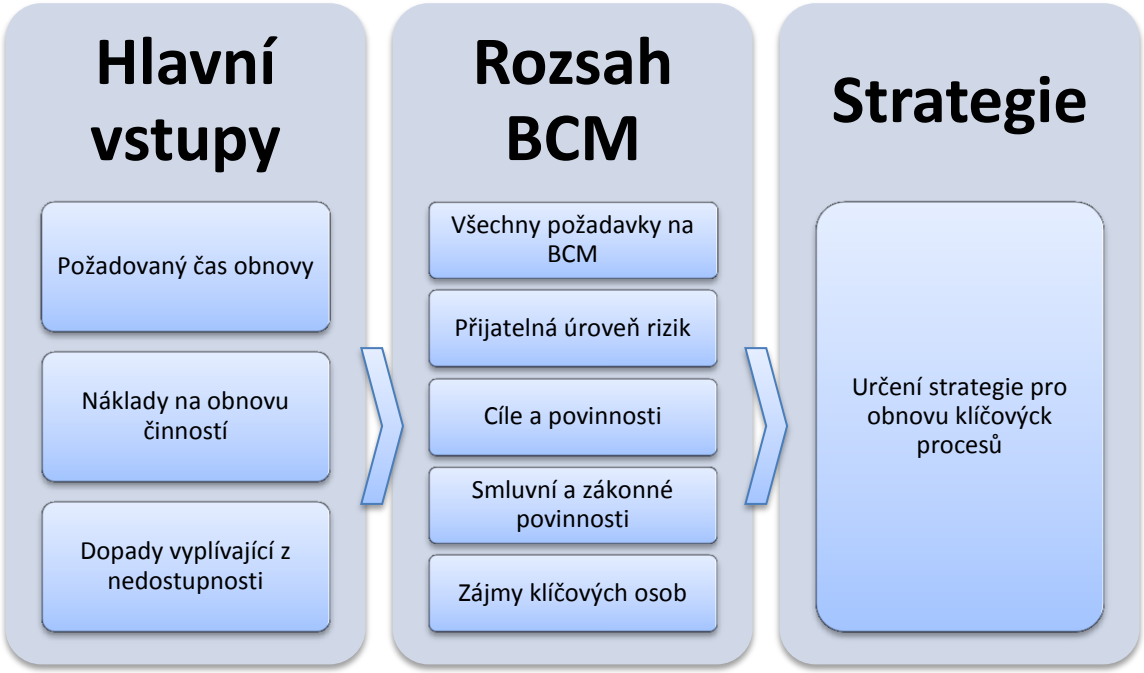
Analýza rizik posuzuje pravděpodobnost vzniku ale i pravděpodobnost rozsahu dopadu na kritické procesy a navrhuje příslušná řešení, která oba tyto faktory minimalizují. Obsahem zprávy, která je výstupem analýzy rizik, je vyhodnocení zranitelnosti organizace všemi specifickými druhy incidentů, dále jednoznačné určení a

[3] Vnější vlivy jsou takové vlivy, které nezávisí na činnosti organizace, ale souvisí s okolím, ve kterém organizace působí.

vyhodnocení rizik klíčových procesů s návrhy na jejich protiopatření. A poslední částí je seznam vytvořený z kritických prvků selhání a míst s koncentrovaným rizikem.

1.8.2.3 Výběr strategie obnovy

Na základě provedených analýz vybíráme vhodnou strategii obnovy (Obrázek 4: Výběr vhodné strategie obnovy (zdroj: Autor)):



Obrázek 4: Výběr vhodné strategie obnovy (zdroj: Autor)

Hlavními vstupy jsou: požadovaný čas obnovy (RTO), náklady na obnovu kontinuity činností a dopady vyplývající z nedostupnosti. Na základě těchto údajů se identifikuje požadovaný rozsah BCM a z toho vyplývající strategie. (Martanová, 2010)

1.8.2.4 Řízení kontinuity bez řízení rizik

Zavádění BCM v organizacích je trendem poslední doby, praxe ukazuje, že lze (oproti doporučením v normách a standardech) řídit kontinuitu činností i bez řízení rizik. Nedochází ke stanovení jednotlivých příčin (tedy hrozeb) ani jejich pravděpodobností a rozsahu dopadů. Jednoduše se vychází až z následků, které mohou nastat. Tyto poznatky z řad odborných pracovníků potom slouží jako základ pro DR (Disaster recovery) nebo BC (Business Continuity) plány.

1.8.3 Plánování

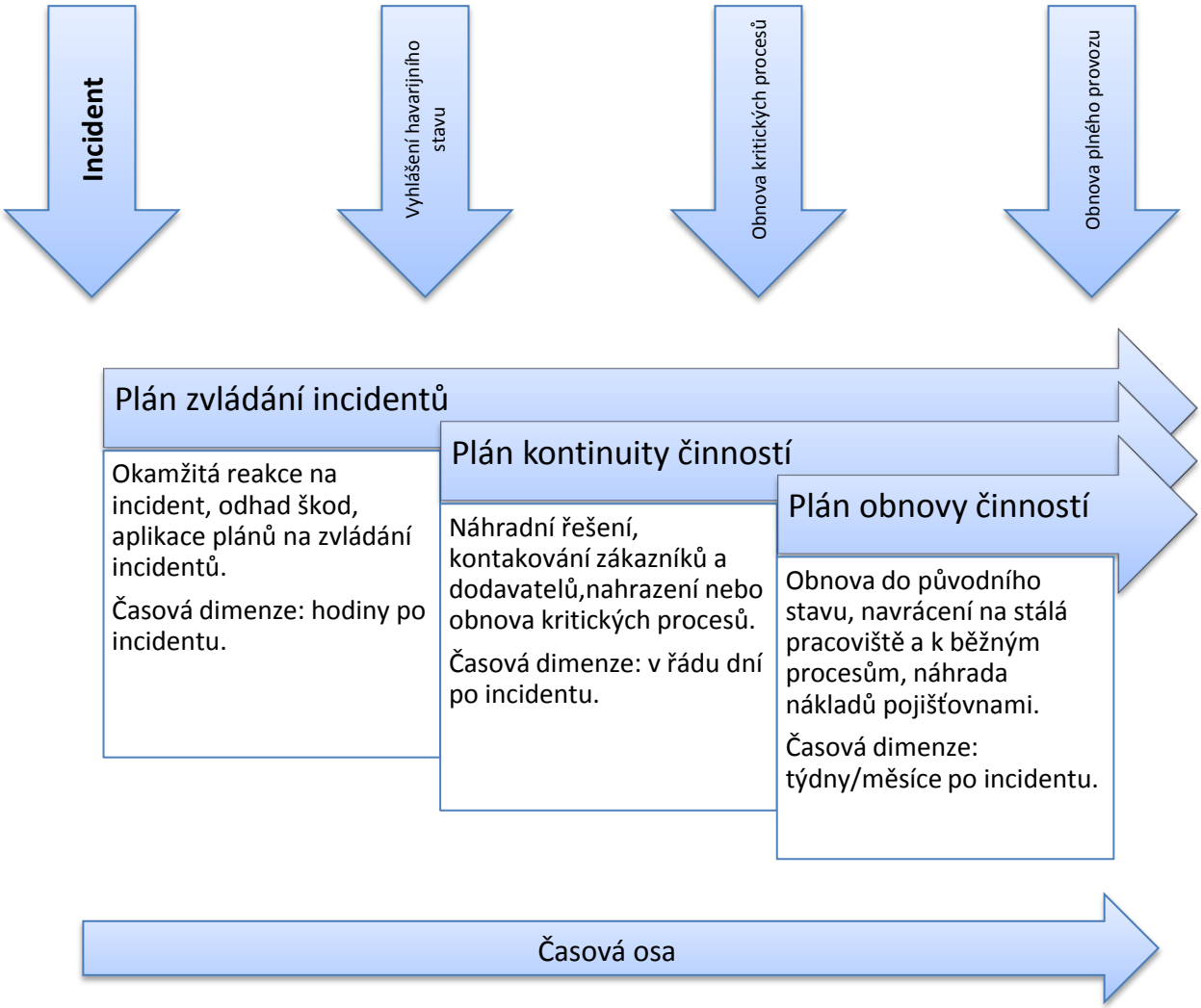
Hlavním cílem plánování je navrhnout vhodný a efektivní způsob reakce na jednotlivé druhy incidentů a zformulovat ho do podoby plánů obsahujících připravená řešení na zvládnutí nečekaných událostí. Ty jsou definovány na základě informací od zodpovědných pracovníků a detailního popisu veškerých činností organizace kritických pro kontinuitu klíčových procesů. Každý plán by měl mít (Martanová, 2010):

- definovaný účel a rozsah,
- zdroje (klíčový zaměstnanci, lokality, vybavení, HW, SW),
- být přístupný a srozumitelný pro veškeré uživatele,
- být svěřen konkrétní osobě nebo týmu za účelem kontroly, aktualizace a schvalování,
- obsahovat klíčové úkoly a referenční informace,
- definovat role a odpovědnosti,
- definovat rozhodovací mechanismy,
- počítat s lokalitami mimo hlavní budovu,
- obsahovat základní kontakty na klíčové osoby,
- obsahovat podrobnosti pro zvládnutí následků přerušení činnosti organizace,
- podmínky aktivace plánů.

K obnovení kontinuity činnosti v době incidentu jsou potřeba tři druhy plánů:

- plán zvládání incidentů,
- plán kontinuity činností,
- plán obnovy činností.

Z následujícího obrázku inspirovaného normou BS25999-1:2006 (Obrázek 5: Aktivace plánů na časové ose (zdroj: Autor)) vyplývá jaký je vztah mezi jednotlivými plány a jak na sebe navazují při průběhu reakce na incident. V případě vzniku incidentu je jako první aktivován plán zvládání incidentu. V řádu hodin od incidentu dojde k vyhlášení havarijního stavu a je aktivován plán kontinuity činností. Až bude situace taková, že lze začít s obnovováním všech procesů najde své uplatnění plán obnovy činností, za jeho pomoci by měla organizace dosáhnout stavu shodného se stavem před incidentem.



Obrázek 5: Aktivace plánů na časové ose (zdroj: Autor)

Všechny druhy plánů je vhodné vydat v tištěné formě a musí být umístěny tak aby byly dostupné všem zainteresovaným osobám za všech okolností.

1.8.3.1 Plán zvládání incidentů

Tento plán zahrnuje postupy a návody na okamžitou reakci na incident a všechna strategická rozhodnutí při zvládání incidentu. Na prvním místě je samozřejmě ochrana zdraví a životů personálu a pak následuje proces minimalizace dopadů na společnost. Plán zvládání incidentů definuje postupy jak komunikovat s obchodními partnery, veřejnou správou, bezpečnostními složkami, novináři a širokou veřejností. Také deklaruje všechny náležitosti pro soulad plánů s platnou legislativou příslušného státu. (Szabados, 2008)

1.8.3.2 Plán kontinuity činností

Na tento plán dojde řádově několik dní po incidentu a logicky navazuje na plán zvládání incidentu. Podává informace jak zvládnout obnovení kritických procesů ve stanovených lhůtách a na definované úrovni. Definuje role a z nich vyplývající zodpovědnosti a pravomoci jednotlivých zaměstnanců v době havarijního stavu. Dále zde z pravidla lze nalézt seznam základních zdrojů, popis dodavatelů a poskytovatelů služeb potřebných v tomto komplikovaném období a stejně jako plány pro zvládání incidentů obsahují i seznam kontaktů na důležité osoby.

1.8.3.3 Plán obnovy činností

Tento druh plánu dosáhne své účinnosti až několik týdnů po incidentu, kdy už jsou obnoveny všechny kritické procesy. Jeho úkolem je přivést organizaci k plné funkčnosti, tak jak tomu bylo před incidentem. Jedná se o technicko-technologický plán popisující obnovu provozu, ICT služeb (proto jsou jeho vlastníky nejčastěji ICT oddělení společnosti), všech lokalit náležících společnosti a veškerého zařízení, definuje obnovu všech zdrojů potřebných na zabezpečení obnovy činnosti a následného plného provozu. Konečně definuje i návrat všech procesů a činností do původního stavu plného provozu, jako před incidentem. (Szabados, 2008)

1.8.4 Implementace

Jak již název této fáze napovídá, proběhne implementace návrhů z předchozích fází na podnikové procesy, aby mohly probíhat další velice důležité činnosti jako testování, aktualizace plánů a auditing.

Právě v této fázi musí dojít ke konečnému začlenění BCM do firemní kultury a každému pověřenému pracovníkovi je určena jeho role v řízení BCM. Ověří se, zda jsou vyčleněny dostatečné zdroje a zda je všechen personál schopný akceptovat úlohu BCM v každodenních aktivitách. Z obchodního hlediska je dobré vyrozumět partnery o zavádění podobných podpůrných procesů, tím si získat jejich ještě větší důvěru než doposud a posílit tak svou konkurenční výhodu, případně je možné přenést na ně v budoucnosti část nákladů spojených s implementací BCM procesů.

1.8.5 Testování

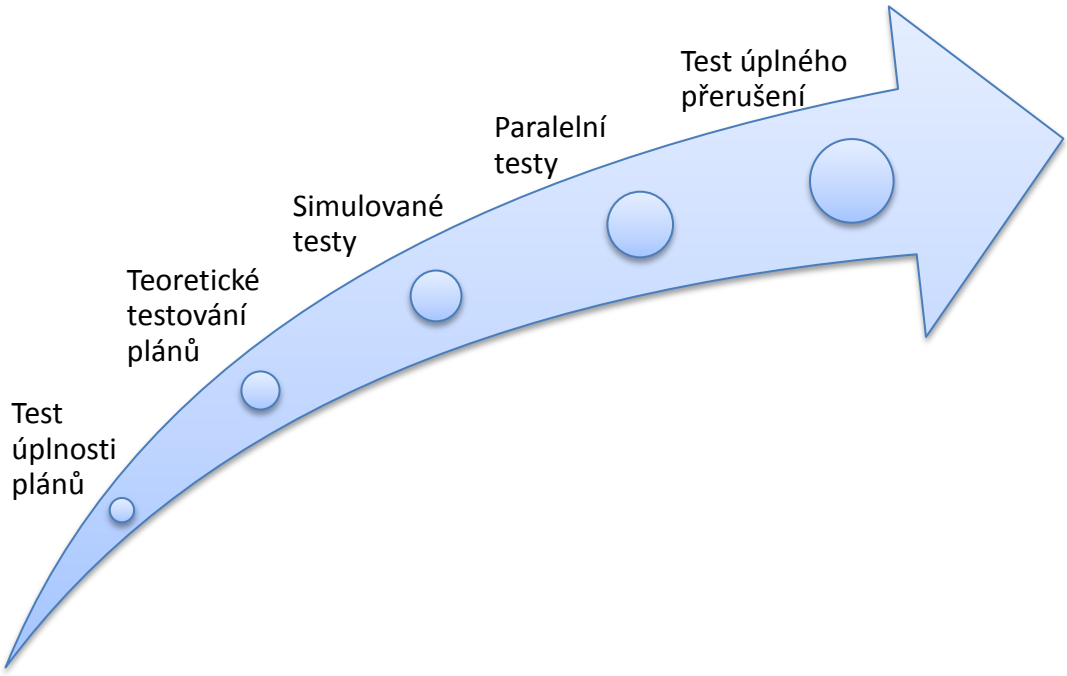
Testování nemá za úkol ukázat jak je BCM systém dobrý nebo ne, jeho úkolem je nalezení slabých míst systému za účelem jejich posílení a zlepšení. Aby byla zabezpečena kvalita testování, musíme volit systematický přístup. I samotné testování musí být pečlivě plánováno.

Před každým testováním je dobré vypracovat harmonogram a plán, ve kterém jsou navrženy testovací scénáře. Je nutné obstarat zdroje na testování, proto tedy musí dojít k definování a vyčlenění zdrojů na testovací procesy, pečlivě stanovit hloubku, rozsah a způsob jednotlivých testů a metriky, s jejichž pomocí budeme testy vyhodnocovat. Výstupem testování je zpráva hodnotící průběh a výsledky testu. Doporučuje se závěry testování pro jejich lepší vyhodnocení opakovaně přezkoumat a výstupem by mělo být vypracování konkrétních doporučení, kde se nacházejí slabá místa systému a jak je lze aktualizací plánů a strategií posílit. Poté je pochopitelně nutné tuto aktualizaci co nejdříve realizovat a zapracovat do jednotlivých plánů či jiné BCM dokumentace. Hlavní cíle testování by se daly shrnout do těchto bodů:

- ověření správnosti navrhnutých strategií,
- odhalení slabin a nedostatků plánů,
- ověření znalostí a schopností všech týmů, jejich členů a všech zainteresovaných osob,
- prověření zda jsou všechny navrhnuté postupy správné a aktuálně odpovídají současnému stavu organizace,
- zvyšování znalostí osob zainteresovaných v řešeních BCM (vlastně se jedná o takový trénink).

Je zde více možností jak testy provádět. Tyto testy se od sebe liší náročností na čas, zdroje, liší se komplikovaností a také je různý jejich zásah do reálného provozu organizace. Všechna tyto hlediska je nutné před zahájením testování zvážit a zvolit si takový druh testu, který zajistí potřebné výstupy a současně nebude nepřiměřeně náročný na zdroje. Doporučuje se postupovat od nejjednodušších testů ke složitějším. Se složitostí testů, souvisí i jejich časová náročnost. Mezi složitostí testů a jejich frekvencí se dá aplikovat nepřímá úměra. Tedy jednodušší testy budou prováděny častěji než testy složité. V následujících odstavcích budou stručně popsány druhy testů,

seřazené podle jejich náročnosti, od nejméně náročných až po ty nejsložitější. (Obrázek 6: Typy testů podle náročnosti (zdroj: Autor))



Obrázek 6: Typy testů podle náročnosti (zdroj: Autor)

Tím základním, jednoduchým, nejčastěji používaným testem je test úplnosti plánů, zde se jedná o nejjednodušší testovací metodu zahrnující teoretické přezkoumání kompletnosti a použitelnosti plánů. Kontroluje se jejich aktuálnost a úplnost. (Szabados, 2008)

Další pomyslnou úrovní testů je teoretické testování plánů. Rozsah tohoto testu je již podstatně větší, prověřují se konkrétní postupy obnovy, testuje se lidský faktor ověřováním znalostí zodpovědných osob, zjišťuje se, jak ovládají své role, jednotlivé postupy a vzájemnou komunikaci a koordinaci. Výstupem toho testu jsou zpravidla podněty pro zaškolení nových členů týmů či opakované školení současných členů.

Od teoretických testů lze přistoupit k testům praktickým, z nichž je nejjednodušší simulovaný test. Při něm dojde k praktickému vyzkoušení případně nacvičení jednotlivých plánů a postupů. Důraz je kladen na vzájemnou komunikaci a spolupráci mezi jednotlivými týmy či osobami podle připravených scénářů, tím se současně prověří všechny komunikační kanály. Do tohoto testu již patří i spolupráce s bezpečnostními a záchrannými složkami státu (např.: simulace požárů, evakuací, všeobecného ohrožení, atd.).

Opravdu komplexními testy jsou paralelní testy. Jak již název vypovídá, provádějí se paralelně s reálným provozem, přesunutím jednoho či více kritických

procesů do jiné lokality, kde dojde k jeho přerušení a komplexní obnově v požadovaných časech a na požadovanou úroveň. Tyto testy jsou již opravdu reálné a značně technicky náročné. Jako jejich hlavní cíl by se dalo označit ověření chování organizace v době vzniku mimořádné situace.

Nejvyšší úrovní testů jsou testy úplného přerušení. Jsou bezesporu nejnáročnější na zdroje, ale to vyvažují svojí komplexností. Simuluje se odstavení nějaké části organizace, nebo přerušení kritických procesů za plného provozu a samozřejmě jeho obnovení v náhradních prostorách za pomoci pouze aktuálně dostupných zdrojů. Jedná se o téměř stoprocentní prověření všech plánů i zainteresovaného personálu. Tyto testy jsou tak komplikované, že je důležité upozornit na rizika. Testy úplného selhání se opravdu velkým organizacím ani nedoporučují provádět, protože by jejich průběh mohl způsobit mimořádnou situaci.

Je možné tvrdit, že sekundární funkcí testování je pro celou organizaci (včetně veškerého personálu) získat návyky a zkušenosti pro případy, kdy bude nutné tyto plány opravdu aplikovat v reálné situaci.

1.8.6 Operativní řízení

I když se může zdát, že po sestavení plánů, implementaci a otestování je BCM projekt dokonale zaveden, byla by velká chyba se mu dále nevěnovat. Už ze své povahy musí být BCM udržovaný a pravidelně aktualizovaný. Tato fáze byla nazvána operativní řízení, je to neustále se opakující sled činností zahrnující testování plánů, jejich aktualizaci, testování zodpovědných osob, auditing systému, školení a udržování povědomí o BCM v celé organizaci. Všechny tyto činnosti mají jediný společný úkol, organizaci co nejlépe připravit na mimořádnou událost nebo incident. A pokud by v důsledku nějakého incidentu došlo k přerušení provozu, tak co nejrychleji navrátit organizaci k jejímu původnímu standardnímu stavu s co nejmenšími ekonomickými ztrátami.

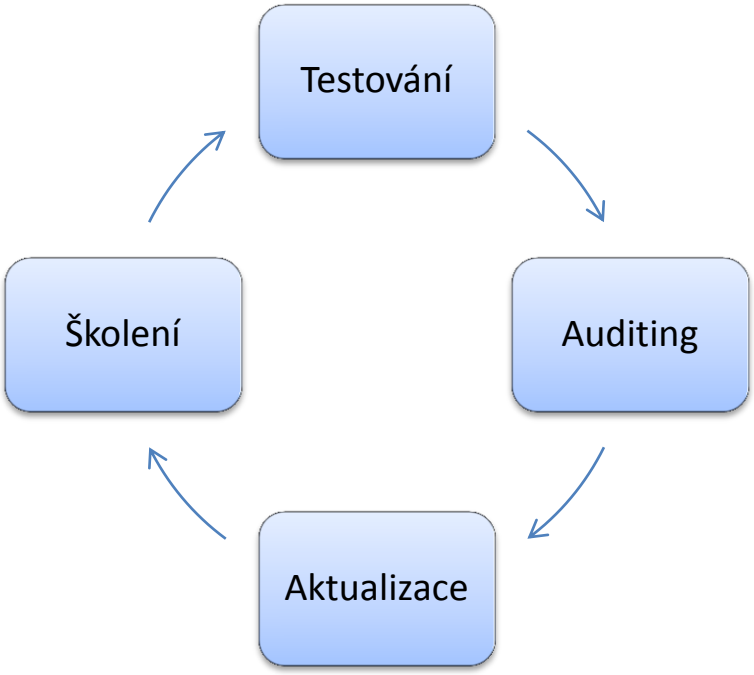
Aby byl BCM opravdu úspěšně zaveden musí vstoupit do podvědomí všech částí organizace, do každodenního strategického rozhodování a řízení organizace, musí vstoupit do tzv. firemní kultury[4]. Zavedení BCM do firemní kultury nám zajistí efektivní přípravu BCM programu, prohlubování důvěry v tyto praktiky, schopnost

[4] Firemní kultura reprezentuje soubor pravidel a principů, jimiž se řídí vnitřní chod společnosti. (Šilhánová , 2010)

vypořádat se s mimořádnou situací i upevňování pocitu bezpečí u tzv. třetích stran (nezainteresovaní pracovníci, dodavatelé, zákazníci). Součástí této BCM kultury by se mělo stát i vedení dostatečné dokumentace k projektu BCM (analýzy, BCM strategie, BIA, plány, testy a jejich výstupy, pravidla udržování, testování a auditu BCM, program vzdělávání a školení personálu, všechny příslušné smlouvy atd.). Stejně tak důležité je vést záznamy o průběhu obnovy při výskytu každé havárie. Zde by se měla zaznamenávat data zachycující čas vyhlášení havarijního stavu, jaké plány byly aktivovány, který personál byl s nimi spojený, všechny události ovlivňující proces obnovy kontinuity, komunikaci s krizovým managementem a čas návratu k normálnímu stavu. Takto zachycené informace jsou velice cenné pro analýzu a následnou optimalizaci plánů.

Pro zhodnocení stavu BCM je vhodný nezávislý pohled z vnějšku organizace, nejlepším řešením je tedy externí audit[5]. Přestože vlastní zaměstnanci se snaží o maximálně zodpovědný přístup k BCM, může být jejich pohled zkreslený rutinním přístupem k běžným provozním problémům nebo k aktuálně plněným úkolům. Proto je pohled z vnějšku organizace přínosný a cenný. Samozřejmě není nutné provádět audit při každé změně plánů, to by mohlo být finančně neúnosné. Úlohou externího auditu je prověření úrovně BCM systému, jeho efektivity a jeho zařazení do všech procesů organizace. Audit dále nezávisle ověří soulad BCM se strategiemi, politikou, praktikami a se standardy které si organizace osvojila. Prověří, zda dochází k pravidelným testům, v dostatečném rozsahu, vyvozování závěrů z nich a aktualizaci plánů podle výsledků testů. Nezávisle zhodnotí celé řešení programu řízení kontinuity činností a BCM plány. Je zřejmé, že výstupy v podobě konkrétních připomínek, by měly být v co nejkratším čase zapracovány do celého BCM systému.

[5] Audit (z lat. auditus, slyšení) znamená úřední přezkoumání a zhodnocení dokumentů, zejména účtů, nezávislou osobou. (Wikipedia, 2010)

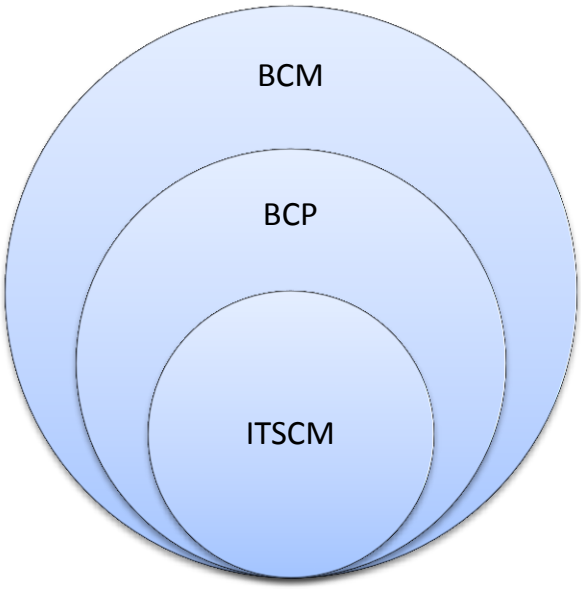


Obrázek 7: Schéma operativního řízení (zdroj: Autor)

Operativním řízením je tedy myšlený koloběh neustálého testování, auditingu, aktualizace BCM plánů a s tím spojeného proškolování zodpovědného personálu (viz. Obrázek 7: Schéma operativního řízení). Jde o nikdy nekončící proces, protože u BCM systému je ještě více než u ostatních operací důležitá aktuálnost plánů a procesů spolu se plnou kompatibilitou na podnikové procesy. Cílem aktualizace plánů je snaha, aby co nejlépe reflektovali změny, které mohou probíhat v organizaci. Mohou se měnit strategie a cíle organizace, mohou být optimalizovány některé kritické procesy. Organizace v reálném světě prochází mnoha změnami organizačními, technologickými, personálními, nebo změnami poskytovaných produktů, může být změněna legislativa upravující některé části procesů BCM. A protože vznik jakýchkoliv nových okolností si vyžaduje určitou změnu v krizových plánech, je nutné je pravidelně aktualizovat.

2 IT Service Continuity Management

IT Service Continuity Management obnovuje nezbytné IT služby pro business v dohodnutém rozsahu a čase. Dalo by se tvrdit, že IT Service Continuity Management (dále již pouze ITSCM) je podmnožinou BCM. Lépe řečeno ITSCM je nedílnou součástí BCM (viz. Obrázek 8: Zařazení ITSCM do struktur BCM (zdroj: Autor)). K BCM má podobný vztah jako celá organizace k IT. Nelze tvrdit, že funkce celé organizace závisí pouze na IT, ale bez něho by organizace s nejvyšší pravděpodobností vůbec nefungovala. Je to vlastně fenomén současnosti, IT se stalo nedílnou součástí každé organizace. Většina obchodních procesů, ve smyslu hlavních procesů v organizaci, je podporována IT infrastrukturou a jejími komponenty. Vysoká dostupnost IT služeb je podmínkou pro úspěšné fungování organizace, proto je nutné, aby všechny plány BCM zahrnovaly i části týkající se systémové a datové podpory obchodu. Zatímco zachováním funkčnosti procesní části organizace se zabývá Business Continuity Planning, obnovení technologické podpory řeší Disaster Recovery Planning, který má spíše reaktivní charakter. (Martanová, 2010)



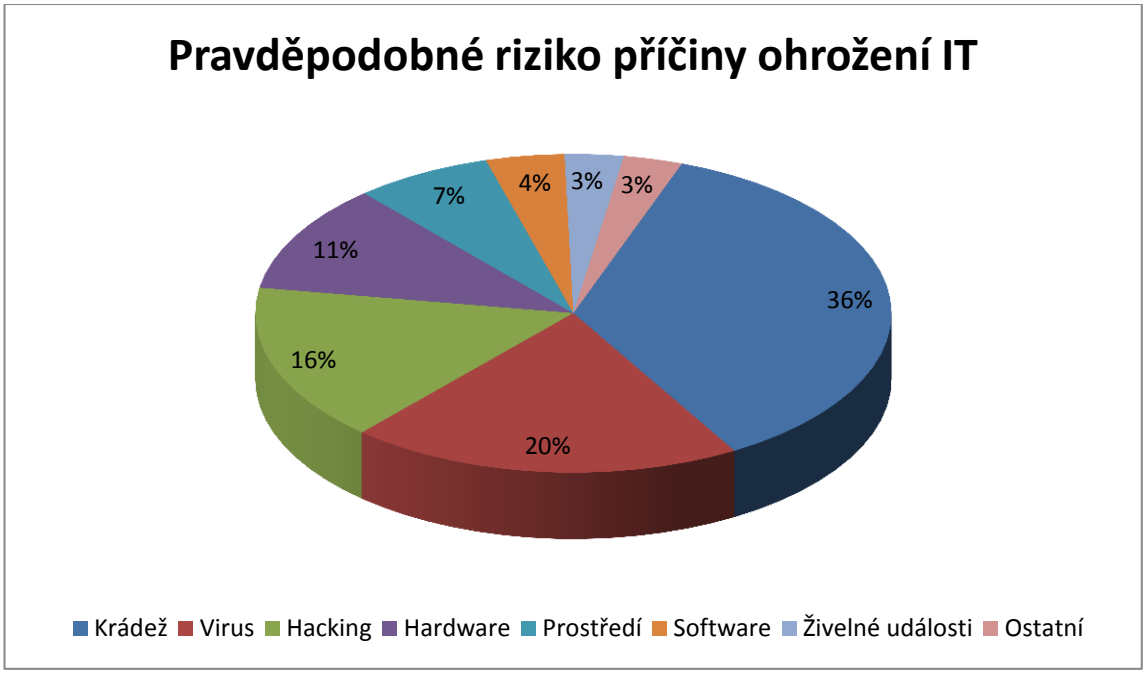
Obrázek 8: Zařazení ITSCM do struktur BCM (zdroj: Autor)

ITSC management ukazuje na rizika, která mohou mít tak náhlý a rozsáhlý dopad, který může aktuálně ohrozit kontinuitu činnosti. Naprosto typickými riziky jsou (BSI, 2006):

- ztráta hesla, poškození nebo odepření přístupu k službám infrastruktury (IS)

- selhání, nedostatečné nebo nedostatečně kvalitní dodávky od kritických poskytovatelů, dodavatelů nebo jiných třetích stran (např.: dodavatelé elektřiny, outsourcing vybraných služeb, atd.),
- ztráta nebo zneužití klíčových informací,
- sabotáž vydírání nebo komerční špionáž
- úmyslná infiltrace nebo útok na kritický bod informačního systému.

Podle průzkumu se příčiny rizika ohrožení IT rozdělují takto (Obrázek 9: Graf rozdělení pravděpodobných příčin rizika ohrožení IT (zdroj: Autor)):



Obrázek 9: Graf rozdělení pravděpodobných příčin rizika ohrožení IT (zdroj: Autor)[6]

2.1 Strategie IT Service Continuity

ITSC strategie by měla definovat směr a úroveň metod, které dosahují požadované cíle v úrovni IT služeb. Měl by zajistit, aby nebyl business nikdy oslabený nedostupností IT. Nedostupností rozumíme stav mimo akceptovatelnou, předdefinovanou a pravidelně přezkoumávanou hranici dostupnosti a výkonu. Stejně jako bylo zmiňováno u BCM strategií, tak i ITSC strategie by měla být odsouhlasena vedením a měla by mít i jeho podporu. Členové vedení (představenstva) by měly zodpovídat za strategii a uvědomovat si dopady změny řízení a dalších rozhodnutí která

[6] Data k tomuto grafu byla převzata z prezentace Jak obnovit procesy z pohledu IT? (Martanová, 2010)

mohou mít dopad na ITSC. Tvorbu ITSC strategie je vhodné rozdělit do 4 etap (BSI, 2006):

- počáteční reakce – aktivace příslušné strategie odpovídající vzniklému incidentu,
- obnovení služeb – zahrnuje obnovu služeb a to v pořadí podle předem stanovených priorit na předem stanovenou úroveň,
- poskytování služeb za mimořádných okolností – až do obnovení normálního provozu organizace, je nutné provozovat služby na předem stanovené minimální úrovni, dokud okolnosti nedovolí návrat k normálnímu provozu,
- obnovení normálního provozu – navrácení naprosto všech služeb do normálního provozu.

2.2 Porozumění rizikům a dopadům

Předně je důležité uvědomit si, že rizika se přirozeně vyskytují v každém systému, v každé společnosti, v každé organizaci. Před zahájením jakéhokoliv ITSCM programu musí být potenciální rizika a jejich dopady identifikovány a musí jím být porozuměno. Ať již je každá společnost vybavena IS jinak, prakticky o všech lze prohlásit, že pokud dojde ke ztrátě jakékoliv součásti IT, výsledkem je omezení nebo ztráta schopnosti používat a řídit svou infrastrukturu s následným úpadkem nebo ztrátou kritických aplikací nebo dat. Pochopitelně velikost tohoto dopadu na společnost záleží na velikosti její závislosti na IT.

2.2.1 Hodnocení zranitelnosti

Paralelně s analyzováním dopadů by měla být stanovena zranitelná místa v dodávkách IT služeb. Tato informace může být získána prostřednictvím hodnocení rizik IT infrastruktury ve vztahu k (BSI, 2006):

- pružnosti a dostupnosti systému,
- klíčovým dodavatelům a smlouvám,
- dokumentaci,
- hardwarovým a softwarovým prostředkům,
- uchování dat,

- režimům zálohování,
- personálu,
- zaškolení personálu,
- umístění budov a jejich příslušenství,
- bezpečnosti IT,
- monitorování systému,
- zdrojů energie,
- datovým přenosům,
- archivaci atd.

Úroveň rizika v každé organizaci se liší, proto je nutné, aby výsledky a následné hodnocení takovýchto průzkumů byly interpretovány racionálně a s ohledem na konkrétní organizaci.

2.3 ITSC plán

ITSC plán je snadno pochopitelný, jasný, jednoznačný a všezahrnující soubor dokumentů, který definuje činnosti potřebné pro obnovu IT služeb po incidentu. Aby zůstal aktuální za každé situace, je neustále testován, aktualizován, modifikován a vylepšován. Záleží na požadavcích organizace, ITSC plán může být jeden dokument nebo série navazujících dokumentů. ITSC plán by měl poskytovat detailní popis procedury pro zvládání každé fáze incident managementu. Může být vytištěn na papíře nebo uchováván jako elektronický dokument. Pokud nastane incident, ITSC plán by měl být přístupný:

- na správném místě,
- ve správný čas,
- pro správné osoby.

Je zde totiž možnost, že při závažném incidentu nebude možné vyhotovit kopii plánu nebo číst plány z obrazovky, proto je nutné s tím počítat, vyhotovit dostatek aktuálních kopií plánů a vhodně je rozmístit. Dobrou variantou také je, aby členové Incident Management teamu měly každý aktuální kopii u sebe, například ve svém notebooku. (BSI, 2006)

Obsah plánů by mohl obsahovat citlivé a důvěrné informace týkající se společnosti, proto je nutné s těmito dokumenty náležitě zacházet. Plány by měly být vždy uchovávány tak bezpečně a s takovými opatřeními, aby bylo zajištěno, že obsah nebude přístupný pro nezainteresovanou osobu.

2.3.1 Volba IT architektury

Před zahájením tvorby ITSC plánu musí být provedena kontrola IT infrastruktury a musí se prověřit, zda obsahuje všechny komponenty a technologie potřebné k obnovení IT služeb po incidentu. Pokud ne, potom je nutné, aby byl systém zdokonalen o potřebné komponenty jako například vysoce dostupný zálohovací mechanismus. Toho lze jednoduše docílit definováním IT architektury, která již tyto komponenty obsahuje. Podobně jako architektura bloku kanceláří bude zahrnovat únikové cesty a nouzové východy, tak by měla IT architektura obsahovat komponenty, jejichž jediným úkolem je zajistit kontinuitu služeb. Zde je nutné konstatovat, že většina obecně přijímaných druhů IT infrastruktury může být použita pro účely ITSCM.

2.3.1.1 Tři klíčové faktory

Při rozhodování o IT infrastruktuře je nutné vyvážit vliv těchto tří faktorů na rozhodování:

- RTO (Recovery Time Objective) – jak rychle po incidentu je potřeba obnovit IT služby,
- RPO (Recovery Point Objective) – bod v procesním cyklu, odkud mohou IT služby pokračovat (např. čas poslední zálohy),
- náklady – je vcelku pochopitelné, že zde platí nepřímá úměra, čím nižší hodnoty RPO a RTO tím vyšší jsou náklady na výsledné řešení.

2.3.2 Reakce na incident

Reakcí na incident, po jeho vyhodnocení, je vyvolání ITSC procesů. Pokud má organizace svoji technickou podporu, ta má za úkol neprodleně kontaktovat IMT[7], jakmile je informována o jakémkoliv incidentu. Je-li některý člen z IMT nedostupný,

[7] Incident Management Team, v plánech je popsáno jeho složení, tvoří jej specialisté ze všech oblastí potřebných k zotavení z havarijních situací, dále všechny role a s nimi spojené odpovědnosti. (BSI, 2006)

plní jeho zodpovědnost předem určený zástupce v rámci týmu. Platí zde nezbytná podmínka, že musí být některý člen přímo kontaktován. Zanechání hlasové zprávy nebo poznámky není dostatečná reakce na incident. (BSI, 2006)

IMT rozhodne o závažnosti incidentu a v závislosti na tom se rozhodne pro zmobilizování jednoho nebo obou z BCMT (Business Continuity Management Team) a CMT (Crisis Management Team) týmů. Pokud po prvotním posouzení situace, dojde IMT k závěru, že může zvládnout incident přímo, pak mohou zůstat ostatní týmy v nečinnosti. Takováto rozhodnutí se řídí pravidly, která musí být definována jako součást ITSC plánů.

2.3.3 Vyhodnocení problému

Incident Management Team má dále odpovědnost za posouzení velikosti dopadu incidentu. Tento tým by měl být tvořen členy s nejlepším možným přehledem v oboru IT služeb a velice dobrým přehledem o fungování systému organizace a všech procesů. Důvodem je, že kritická doba může být ztracena nerozhodností a pochybnostmi nekvalifikovaných členů o tom, zda může systém opravdu selhat. IMT by měl vyvinout soubor detailních kritérií založených na zkušenostech z minulosti a sledovat, zda se současný vývoj nepodobá nějakému dřívějšímu selhání. V případě že IMT identifikuje potencionální dopad na organizaci i mimo IT služby, je jeho zodpovědností postarat se o aktivaci BCMT[8], který využije organizací definované Business Continuity procesy.

[8] Business Continuity Management Team je část organizace, která se stará o zachování kontinuity činnosti organizace. (zdroj: http://web.mit.edu/bcmt/).

3 Analýza

Na následujících stránkách budou aplikovány doposud získané teoretické poznatky do praktického života. V úvodu byla, jako jeden hlavní cíl práce, uvedena analýza ITSC plánu. Pro tuto analýzu bude použitý jeden, na první pohled jednoduchý, proces v konkrétní organizaci a tím je přijetí objednávky pomocí elektronické výměny dokumentů (EDI). Jde o zásadní způsob komunikace s velkou většinou klientů. Analýza bude na konci této kapitoly vyhodnocena a okomentována.

3.1 Seznámení s prostředím[9]

Objektem analýzy je každodenní proces české pobočky společnosti FM Logistic. Tato společnost byla založena roku 1967 jako rodinná společnost Faure & Machet se specializací na dopravu a v roce 1996 expandovala na český trh. V současné době působí téměř v celé Evropě a v Číně, její aktivity by se daly shrnout do těchto pěti bodů:

- SCM, tedy řízení dodavatelského řetězce,
- doprava,
- skladování,
- co-packing,
- co-manufacturing.

Sledovaná pobočka sídlí v Tuchoměřicích, což je obec na okraji Prahy, skladový areál čítá 65000 paletových míst na rozloze 33000 m^2. Umístění skvěle vyhovuje základnímu požadavku logistického a distribučního centra, tím je dobrá dostupnost. Nachází se u rychlostní silnice R7, která je přímým spojením se západní Evropou a zároveň jen několik minut od mezinárodního letiště Ruzyně. Konkurenční výhodu jistě tvoří i připojení k železniční síti prostřednictvím železniční vlečky. Předmětem činnosti tohoto areálu je skladování, doprava a co–packing. Mezi největší zákazníky patří např. firmy Nestlé a Ferrero. Protože poskytuje služby potravinářskému průmyslu, musí dodržovat ty nejnáročnější bezpečnostní normy prostřednictvím HACCP[10].

[9] Veškeré informace ohledně společnosti FM Logistic byly převzaty z oficiálních webových stránek.

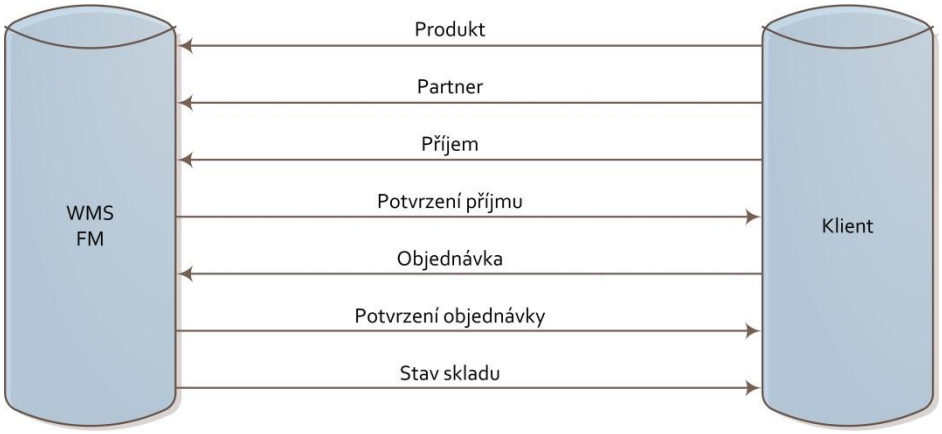
[10] HACCP (Hazard Analysis and Critical Control Points) je systém řízení kvality a zdravotní nezávadnosti potravin založený na prevenci. (zdroj: http://www.itczlin.cz/haccp.php)

3.2 EDI

Aby bylo možné přikročit k analýze, je zapotřebí uvést základní teoretický podklad k technologii elektronického sdílení dokumentů. EDI, z anglického Electronic Data Interchange, je výměna dle standardů strukturovaných dat mezi počítačovými aplikacemi, bez ohledu na použité technologie, z toho tedy vyplývá nutnost dokonalé kompatibility.

Elektronické dokumenty ušetří mnoho času. Rychlejší je jak jejich tvorba, tak jejich přenos i zpracování. Odpadá administrativní práce s přepisováním dokumentů do elektronické podoby a také prodlevy vyplývající z předávání dokumentů. Další nespornou výhodou je zvýšení kvality a spolehlivosti, protože odpadají možné chyby při přepisování dokumentů do elektronické podoby, překlepy a ostatní chyby lidského faktoru. Z toho logicky vyplývá, že EDI vede ke zvýšení kvality, spolehlivosti a rychlosti služeb, toto vše spojené i s úsporou nákladů. (Zdvořáček, 2011)

V FM Logistic probíhá EDI komunikace s klientem v této podobě (viz Obrázek 10: EDI komunikace s klientem (zdroj: Autor)).



Obrázek 10: EDI komunikace s klientem (zdroj: Autor)

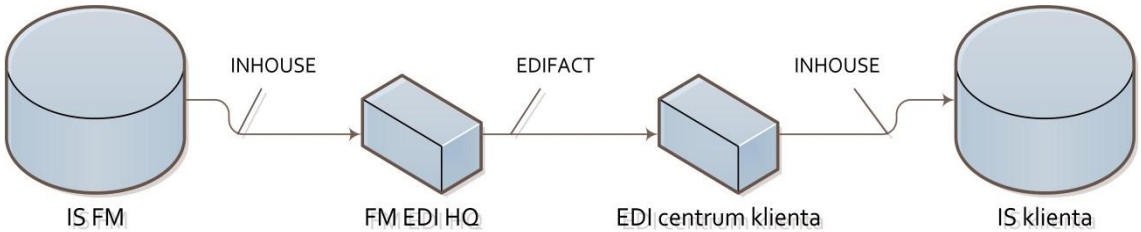
Z informačního systému klienta musí přijít nejdříve zprávy s informacemi o veškerém zboží, se kterým se bude pracovat a zařadí se do IS poskytovatele služeb. Pro WMS[11] jsou zásadní informace o fyzických rozměrech a hmotnosti palet, identifikační čísla a další specifické požadavky na skladování. Pokud má distribuční centrum distribuovat zboží obchodním partnerům klienta, je nutné, aby byly o těchto

[11] WMS neboli Warehouse Management System je aplikace pro podporu a řízení skladových operací, logistiky a výměny dat. (zdroj: http://www.systemonline.cz/erp/warehouse-management.htm)

společnostech dostupné veškeré kontaktní údaje. Po výměně těchto prvotních informací může začít komunikace už opravdu za účelem poskytování konkrétní ch služeb. Současně s fyzickým odesláním zboží je odeslán elektronický dokument se všemi kvantitativními údaji o zboží a po jeho faktickém přijetí je odesláno zpět klientovi potvrzení příjmu. Ten si od té doby může být jistý, že zboží dorazilo a je v pořádku uskladněno a může s ním nakládat pro své obchodní účely. Dalším elektronickým dokumentem je objednávka, tu opět iniciuje klient, obsahuje údaje o tom jaké zboží, v jakém množství, čase a kam se má distribuovat. Opět je objednávka potvrzena. A směrem ke klientovi odchází zprávy o stavu zásob ve skladu, které slouží klientovi jako informace o skladových zásobách, pokud to klient není schopen zjistit ze svého IS nebo se jedná o redundantní informaci, aby se obě smluvní strany ujistily o správnosti jejich evidence o stavu a pohybu zboží.

Hovoříme-li o výměně elektronických dat, je nutné upřesnit v jakém formátu. EDI je totiž pojem, který neurčuje, na jakém standardu bude komunikace probíhat. V Evropě je zřejmě nejrozšířenějším standardem EDIFACT, ale v poslední době mu směle sekunduje XML, oproti tomu v zámoří převažuje standard X12. Vzhledem k tomu, že analyzovaná firma sídlí v Evropě, jsou pro ni nejpoužívanějšími standardy EDIFACT a XML, to již záleží na dohodě s klientem, jaký standard bude používán v konkrétní komunikaci.

Dále je nutné připomenout, že překládání z tzv. Inhouse formátů, tedy formátů vycházejících z IS každé společnosti, do některého ze standardů EDI probíhá ve specializovaných EDI centrech. Zde záleží především na rozhodnutí každé individuální společnosti, zda její náklady na outsourcing služeb externího EDI centra nepřekročí náklady na provozování vlastního. Společnosti, které finanční kalkulací zjistí, že je pro ně výhodnější si překlad dokumentů kupovat jako službu, používají outsourcing. Každopádně model výměny elektronických dat je ve všech případech stejný a názorně ho vysvětluje následující obrázek (viz Obrázek 11: Model výměny elektronických dokumentů (zdroj: Autor)).

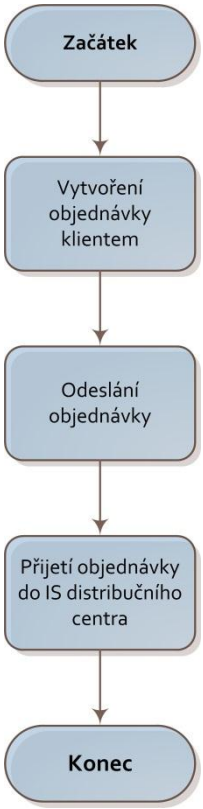


Obrázek 11: Model výměny elektronických dokumentů (zdroj: Autor)

Zde je jasně vidět jak se zpráva překládá, tentokrát ve směru od distribučního centra ke klientovi, může se jednat např. o nějakou konfirmační zprávu nebo informaci o stavu skladových zásob. Z IS distribučního centra FM Logistic proudí data v Inhouse formátu, který je vlastní jejímu IS do EDI HQ (EDI Headquarter), tedy do vlastního EDI centra společnosti FM Logistic. Tam proběhne překlad do předem stanoveného standardu například EDIFACT, kterému dokonale rozumí EDI centrum klienta a přeloží tuto zprávu do INHOUSE formátu, kterému rozumí IS klienta.

3.3 Popisovaný proces

Jak bylo již řečeno v úvodu této části, objektem analýzy je proces přijetí objednávky od klienta za pomoci elektronické výměny dat. Na první pohled je tento proces opravdu jednoduchý a to díky EDI, kdy velká většina nutných úkonů probíhá automaticky. Model tohoto procesu je na následujícím obrázku (Obrázek 12: Model analyzovaného procesu (zdroj: Autor)).



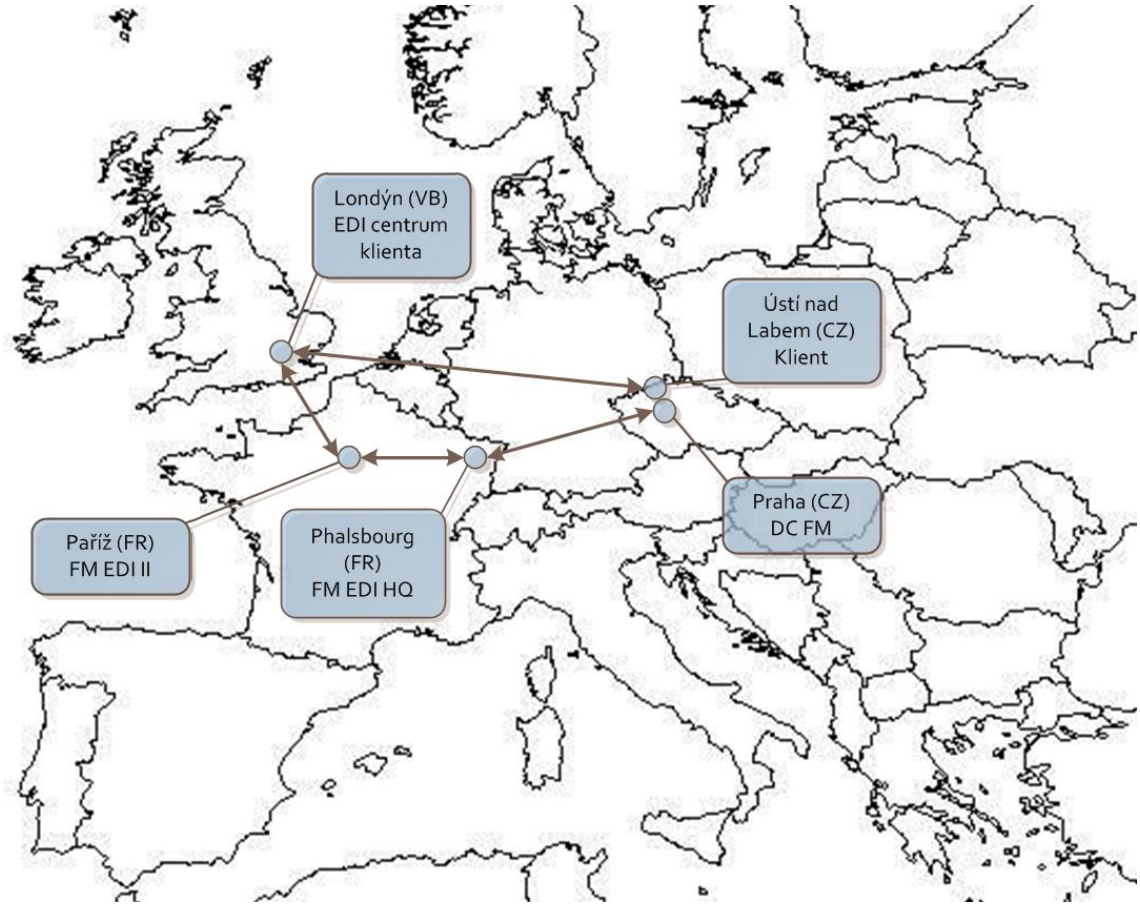
Obrázek 12: Model analyzovaného procesu (zdroj: Autor)

Tento proces spouští klient vždy, když chce vystavit objednávku. Tedy má zájem o čerpání služby ze strany distribučního centra. Fakticky se jedná o doručení zboží, které je uskladněno v distribučním centru, obchodnímu partnerovi klienta.

Prakticky každý den v podvečer přichází do WMS logistického centra soubor objednávek, které se zpravidla do následujícího dne expedují na místo jejich určení.

3.4 Analýza rizik

Aby bylo možné provést korektní analýzu jakéhokoliv procesu, je nezbytné ho dobře pochopit a brát v úvahu veškeré činnosti i ty, o kterých běžný uživatel třeba ani neví. Podíváme-li se tedy na zkoumaný proces opravdu detailně, zjistíme, že je mnohem více komplikovaný. V části věnované elektronické výměně dat je schéma, které popisuje, jak přenos probíhá (viz Obrázek 11: Model výměny elektronických dokumentů (zdroj: Autor)). Zohledníme-li další faktor, kterým je geografické uspořádání jak zákazníka, tak klienta a jejich EDI center, složitost výrazně vzroste. To můžeme vidět na následujícím obrázku (Obrázek 13: Geografické rozložení zákazníka, klienta a EDI center (zdroj: Autor)).

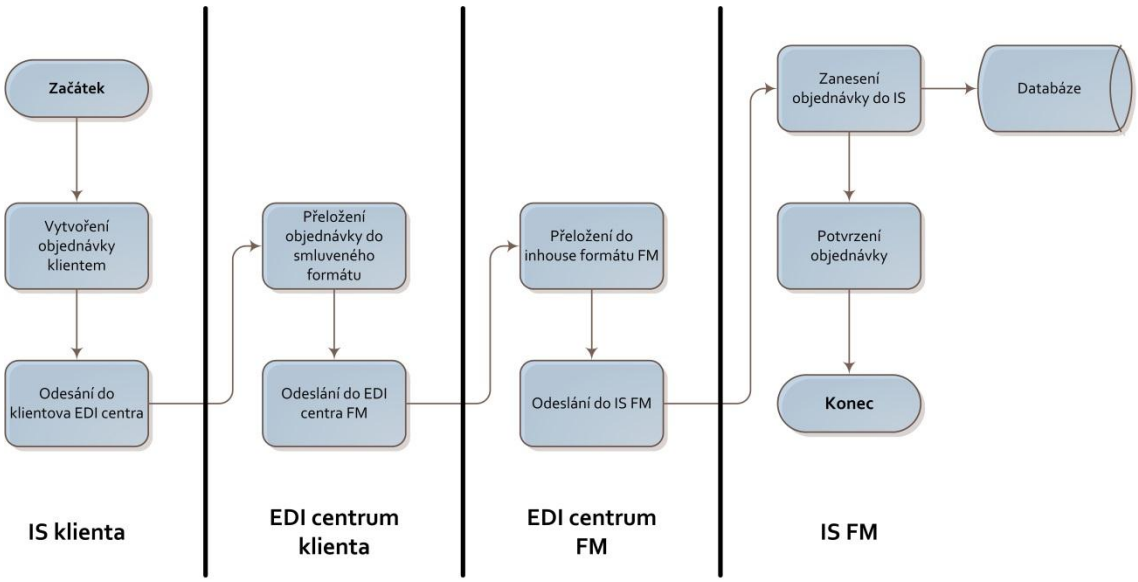


Obrázek 13: Geografické rozložení zákazníka, klienta a EDI center (zdroj: Autor)

Z tohoto plánku je zřejmé, že jedno z největších rizik, leží právě v přenosu dat. I když jsou od sebe klient a distribuční centrum vzdáleni jen několik desítek kilometrů,

data, která si spolu vyměňují, fyzicky obletí po datových spojích velkou část Evropy.

Dále je pro analýzu rizik nezbytné sledovat u analyzovaného procesu celý faktický průběh, tedy se všemi činnostmi, které jsou díky EDI automatizované a proto běžní uživatelé nevědí, že existují. Zde je nutné k analýze použít informace od kvalifikovaného zdroje, např. pracovníka IT oddělení. Faktický průběh procesu ukazuje následující diagram (Obrázek 14: Faktický průběh procesu (zdroj: Autor)).



Obrázek 14: Faktický průběh procesu (zdroj: Autor)

Z diagramu lze vyčíst další zásadní riziko tohoto procesu, po již identifikované závislosti na datových přenosech, je dále zřejmá závislost na správně fungujícím IS. Lze říci, že funkčnost IS závisí na čtyřech bodech. Kromě spolehlivých technologií pro přenos dat, je nutné mít správně fungující HW. A jak již bylo řečeno v úvodu, že i přes velký technický pokrok jsou informační technologie stále „jen“ stroje a ty jsou naprosto kriticky závislé na dostatečném přísunu energie. Posledním kritickým bodem, který se nejsložitěji řeší, je lidská chyba.

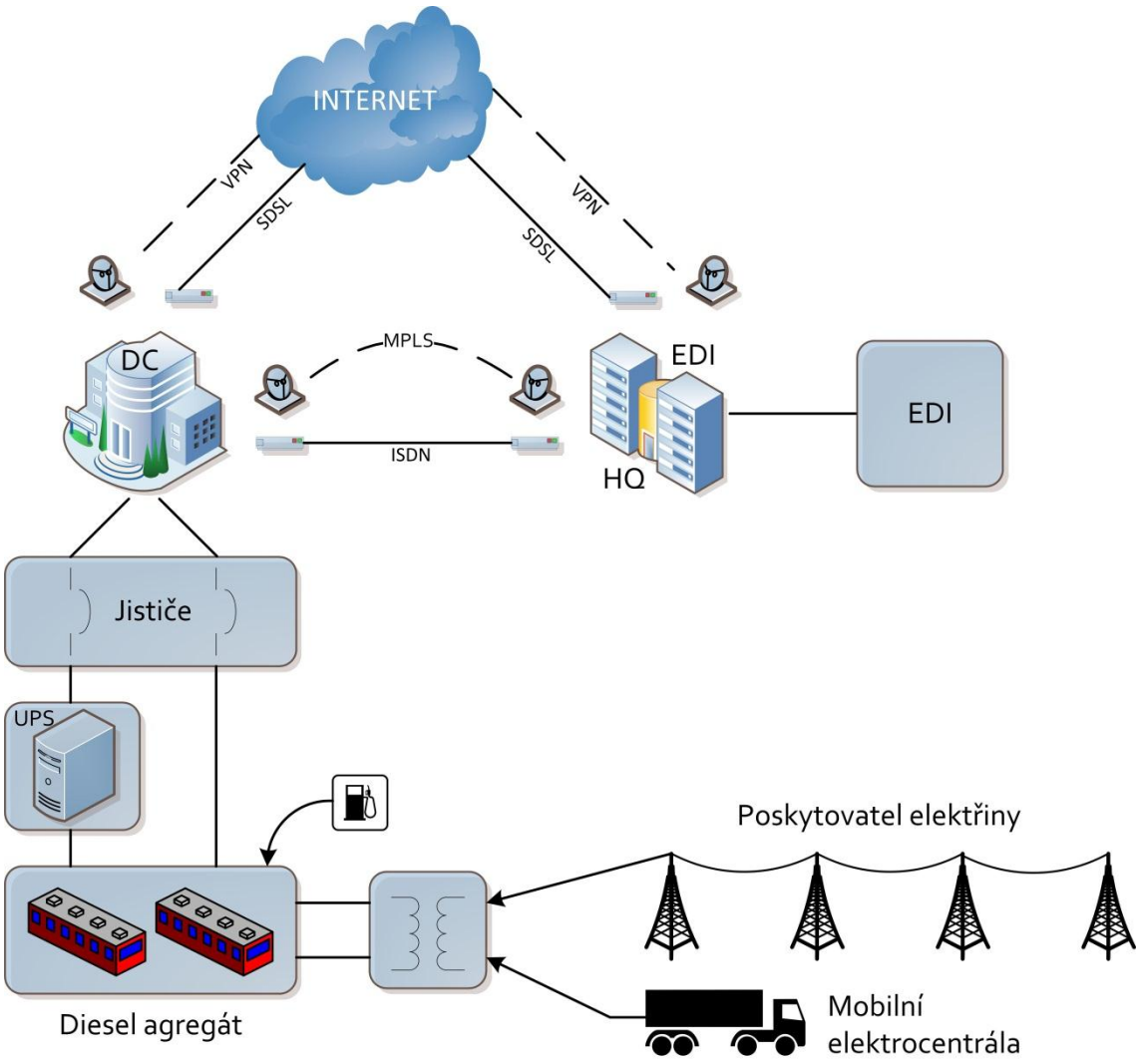
Pokud bychom měly posoudit dopad každého z těchto rizik na celou funkci procesu, tak je vždy fatální. Nedojde-li k doručení objednávek na další den, nemůže distribuční centrum odeslat zboží, klient nedostane požadovanou službu a ani třetí strana se svého zboží nedočká, pro všechny zúčastněné z toho plynou určité ztráty. Tyto ztráty lze jen velice těžko exaktně vyčíslit, neboť se jedná jak o finanční zprávy z nerealizovaného obchodu, ztrátou jsou možné náklady na penalizaci za nedodání zboží, vznikají i další obchodní ztráty např. zákazníci substituují nedodané zboží jiným, konkurenčním a to může vést ke změně jejich preferencí, odklonu od tohoto nedodaného zboží, případně až k poškození pověsti značky.

Pro zopakování, kritická rizika byla identifikována v:

- zásobování elektrickou energií,
- funkčním hardwaru,
- datových přenosech,
- lidském faktoru.

3.5 ITSCM plán

Nyní bude pozornost zaměřena na problematiku sestavení plánů, které řeší jak se s výše zmíněnými riziky vyrovnat, jak jim čelit a jak zachovat kontinuitu poskytovaných služeb pokud rizika nastanou. Úvodem je vhodné použít diagram, který bude sloužit k pozdějšímu vysvětlení několika postupů pro zachování kontinuity služeb (Obrázek 15: Plánek zásobování energií a datových spojů (zdroj: Autor)).



Obrázek 15: Plánek zásobování energií a datových spojů (zdroj: Autor)

Na tomto plánku je vyobrazena část řetězce EDI komunikace, za kterou zodpovídá poskytovatel logistických služeb.

Ještě je potřeba zmínit fakt, že s každým zákazníkem dojde ke vzájemné shodě o zodpovědnosti za přenos, ta musí být vždy jasná, každý si zodpovídá za svoji část přenosu sám.

3.5.1 Zásobování elektrickou energií

Budeme-li postupovat podle logické návaznosti, nejdůležitější je zachování dodávky energie pro IS, minimálně pro servery, disková pole a obecně řečeno pro veškeré vybavení serverové místnosti. Za normálního provozu odebírá distribuční areál FM Logistic elektrickou energii ze sítě, ta přes jističe zásobuje celou pobočku. Veškeré vedení elektrické energie je, podle doporučení, realizováno s redundancí, vedení je tedy dvojité. Pokud opravdu dojde k výpadku, není důležité, zda je to výpadek plánovaný či neplánovaný, zařízení UPS[12] začne kontinuálně (tedy bez přerušení) zásobovat energií serverovou místnost se vším vybavením, to zahrnuje obsah všech rackových skříní obsahujících všechny servery, disková pole a zabezpečení této místnosti. Zařízení zde konkrétně použité, je schopné zajistit tuto činnosti po dobu 40 minut, což je však potřeba opravdu velice výjimečně. Protože i toto zařízení UPS se může porouchat, je přemostěno metalickým vedením a s několikavteřinovým zpožděním po výpadku, začne startovat dieselová elektrocentrála, pokud by došlo k jejímu výpadku, je zde ještě záložní. Oba agregáty podstupují pravidelnou údržbu a mají nádrže naplněné naftou, kterou je možné dále doplňovat z cca 2 kilometry vzdálené čerpací stanice. Jejich výkon již zastoupí práci UPS a navíc stačí i na provoz zabezpečovacích systémů celého areálu a nouzových světel. Dále má společnost FM smluvního partnera, který je schopný do třech hodin od zadání požadavku přistavit mobilní elektrocentrálu v podobě nákladního automobilu s agregátem dostatečného výkonu pro provoz celého areálu. (Štvan, 2011)

Ideální by bylo mít kromě standardního poskytovatele elektrické energie dalšího redundantního poskytovatele, to bohužel není, při současných podmínkách na českém trhu možné, proto je náhradním řešením přistavení velké elektrocentrály na nákladním vozidle.

[12] UPS je zkratka z anglického Uninterruptible Power Source vyplívá, že se jedná o zařízení zajištující kontinuální zásobování elektřinou při přerušení jejího přísunu z jiného zdroje.

Problematika zásobování energií je tedy vyřešena naprosto dostatečným způsobem. Muselo by dojít opravdu k nějaké velice výjimečné události zcela zásadních rozměrů, které by překračovali hranice této společnosti, aby tento systém zásobování energií selhal.

3.5.2 Funkční HW

Zásobování energie je vyřešeno na velmi slušné úrovni, proto další logickou návazností je mít spolehlivě fungující HW. Zde nastal prostor pro zálohování a vytvoření takové IT architektury, která by byla dostatečně spolehlivá za všech okolností.

Bojovat proti spolehlivosti resp. nespolehlivost hardwaru se dá opět velice efektivně jeho redundancí a proti ztrátě dat jejich efektivním zálohováním. V analyzované společnosti je o data řádně pečováno, jsou zaznamenávána na disková pole RAID 5. Tato technologie ze svého principu potřebuje tři pevné disky, ve zdejších diskových polích se jich však používá pět, což zlepšuje celkovou rychlost diskového pole. Navíc se zde používá jeden disk jako Hot Spare, to znamená, že je připojen k fungujícímu zařízení, ale za normálního stavu není používán. Role Hot Spare disku je taková, že zastoupí kterýkoliv disk z diskového pole při jeho poruše. Redundance se dále uplatňuje i u dalších komponent jako jsou řadiče disků, zdroje (včetně přívodních kabelů energie), systémy chlazení, síťové karty (včetně síťového vedení), celé servery jsou řešeny redundantně a i dokonce EDI Centrum v Paříži je záložní. Většina výše jmenovaných komponent je typu Hot Swap, lze je tedy měnit za chodu celého systému. (Štvan, 2011)

Zálohování je realizováno na pásky technologií LTO, servery jsou replikovány na další Off Site server, to znamená, že je uložený v úplně jiné budově. Tato technologie by našla uplatnění při Disaster Recovery, tedy v případě, že by byla primární serverová místnost úplně zničena. I tento záložní systém je zálohován na LTO pásky, které jsou uskladněny v serverových místnostech, ale navzájem zaměněné, tedy pásky se zálohami hlavních serverů jsou u Off Site serveru a obráceně. Proto by i při úplné ztrátě jedné ze dvou místností měla zůstat záloha v té druhé. Dále jsou data chráněna, před útokem zvenčí, dostatečnou antivirovou ochranou, ochranou před nepovoleným přístupem z cizí sítě, pečlivým řízením uživatelských účtů (vhodné

přiřazování uživatelských práv uživatelům) a dále i řízeným přístupem k nejdůležitějším hardwarovým částem IT infrastruktury.

Zde by se dalo doporučit rozšíření o každodenní ukládání zálohovaných pásek do úplně jiného komplexu budov, např. do bankovního trezoru. I když je serverová místnost i Off Site záloha v oddělených budovách, jsou od sebe vzdáleny jen několik desítek metrů. Nedá se říct, že by toto řešení bylo nedostatečné, ale při ukládání pásek do bankovního trezoru by faktor bezpečnosti ještě vzrostl.

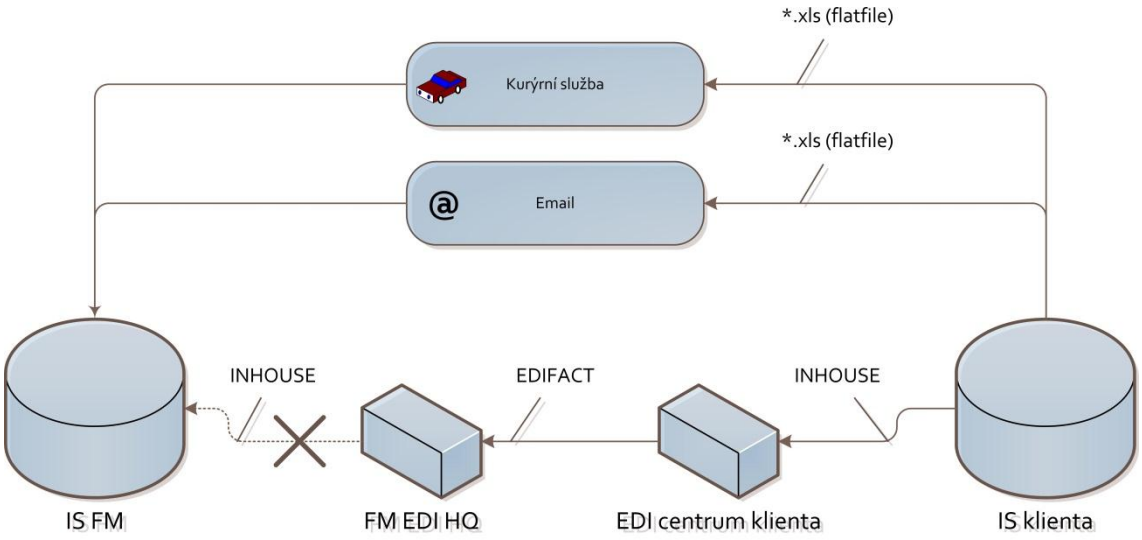
3.5.3 Datové přenosy

Další riziko bylo identifikováno v přenosu dat. Již bylo výše upozorněno, je smluvně dohodnuto, že si každý účastník výměny elektronických dat zodpovídá za svoji část přenosu, tedy za dění v jeho IS a jeho EDI centru, případně dění u jeho smluvního partnera provozujícího služby EDI centra.

Jak je patrné z plánku datových spojů (viz. Obrázek 15: Plánek zásobování energií a datových spojů (zdroj: Autor)), v FM Logistic je datové spojení s EDI centrem realizováno 4 druhy datových linek. Standardním postupem je využívání MPLS linky pro spojení distribučního centra a EDI centra, i když např. České radiokomunikace označují tuto službu jako spolehlivou a vhodnou do podmínek, kde jsou kladeny vysoké požadavky na dostupnost, existují zde četná náhradní řešení. Prvním náhradním řešením je přenos po ISDN lince, další možnost je přenos prostřednictvím VPN, kdy je internetové připojení realizováno pomocí SDLS nebo bezdrátově, každý od jiného ISP[13].

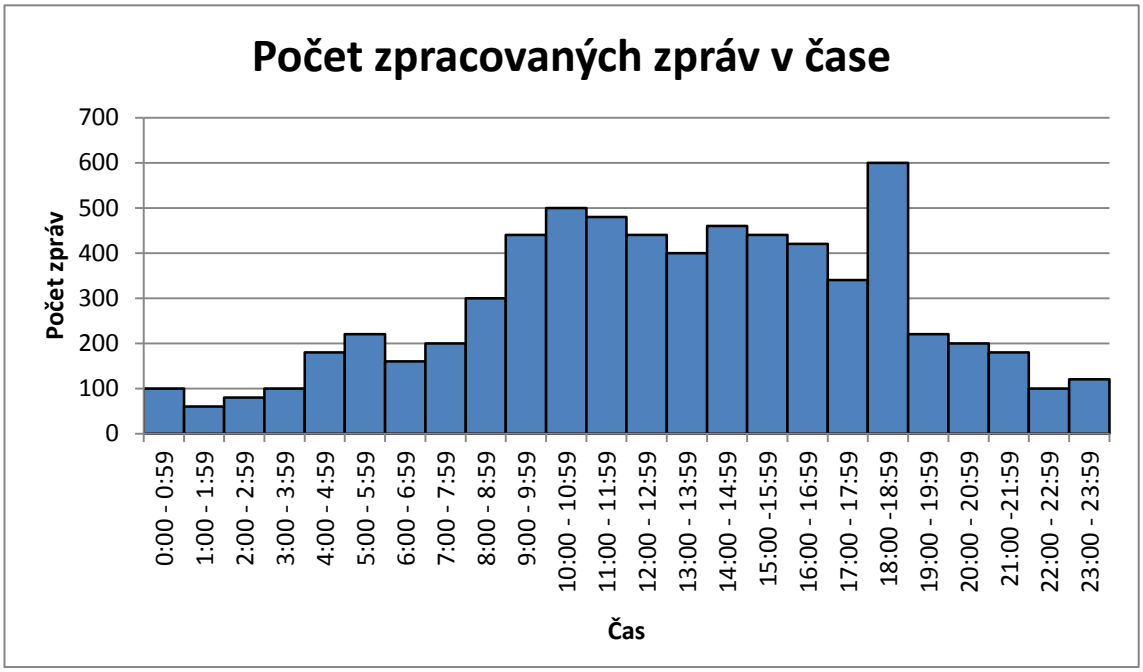
Pokud všechny pokusy přenést elektronický dokument selžou, je náhradním řešením vytvoření objednávek v excelovském souboru *.xls (viz příloha). Z tohoto souboru je možné vyexportovat data jako Flatfile, což je prostý textový soubor a ten odeslat buď emailem, nebo v nejhorším případě, kdy je DC elektronicky odříznuto od světa, lze tento soubor uložit na flashdisk či vypálit na CD odeslat do DC kurýrní službou. Model výměny dat by potom vypadal takto (Obrázek 16: Upravený model výměny dat (zdroj: Autor)).

[13] Internet Service Provider, česky poskytovatel připojení k internetu.



Obrázek 16: Upravený model výměny dat (zdroj: Autor)

K zastavení přenosu zprávy může dojít i vlivem softwaru. Je možné, že bude EDI centrum zahlceno množstvím zpráv čekajících na přeložení, to je dáno např. denním cyklem výměn dokumentů, který můžeme pozorovat na grafu (viz Obrázek 17: Graf počtu zpracovaných zpráv v čase (zdroj: Autor)). Přenosy zpráv se za normálního provozu počítají na tisíce denně, nejfrekventovanější je EDI centrum mezi 18 a 19 hodinou.



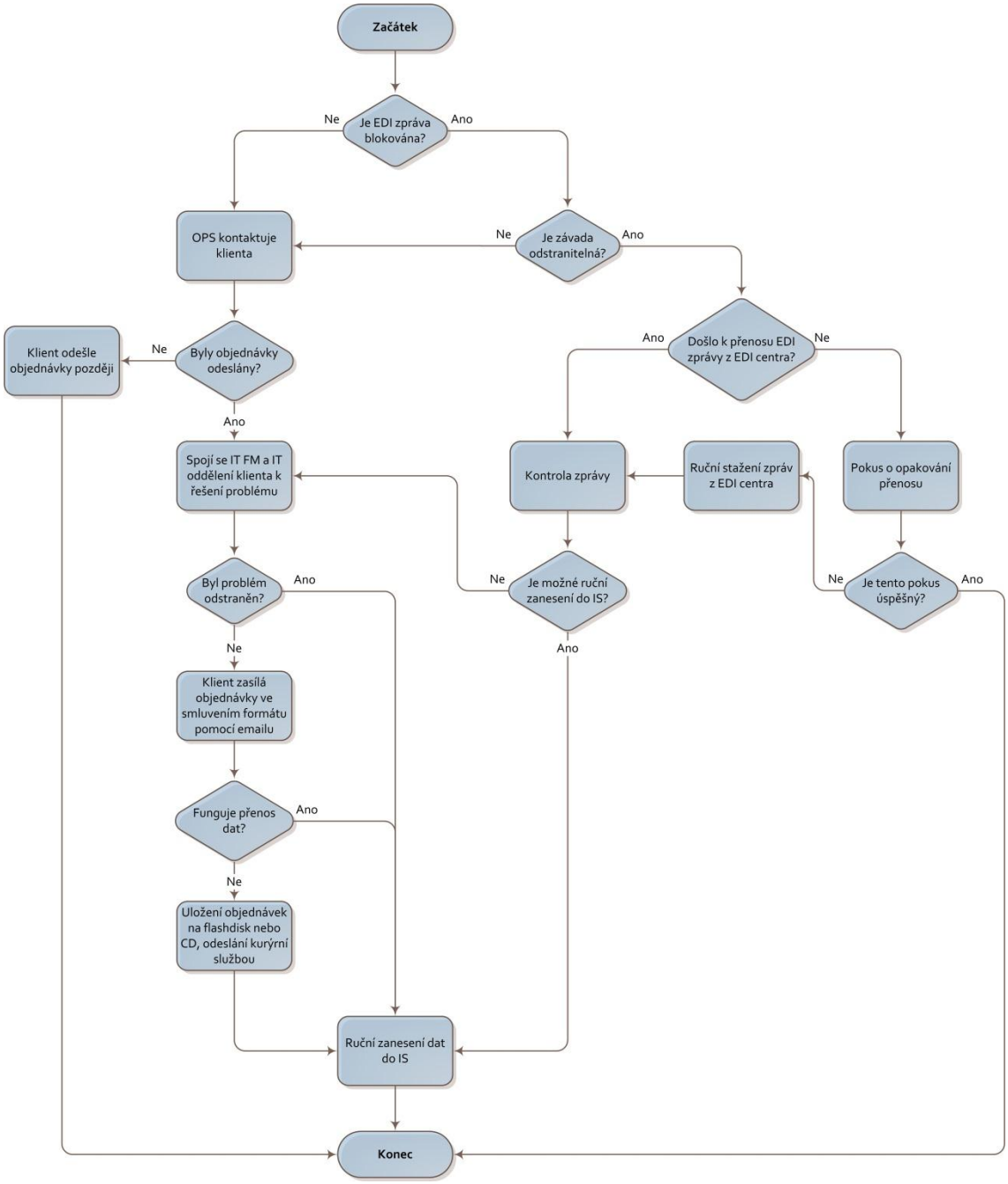
Obrázek 17: Graf počtu zpracovaných zpráv v čase (zdroj: Autor) [14]

[14] Hodnoty pro tento graf byly převzaty z prezentace EDI-FM.

Dalším rizikem je opět lidská chyba. Chybou plánování managementu nebo omylem personálu může dojít např. ke spuštění odesílání výsledků inventury (v tomto případě dorazí do EDI centra několik tisíc zpráv) ve všední den a tím je na mnoho dalších hodin zahlceno EDI centrum a zastaveno zpracování ostatních zpráv. Další možností je chybně strukturovaná zpráva, potom nedojde k jejímu přeložení.

Dále se může se stát, že zpráva obsahuje nějaká nekorektní data, tedy jde o případ, kdy jsou ve zprávě špatná data, která nemohou být automaticky zanesena do databáze IS. Tato data mohou být ve špatném formátu nebo neodpovídají předchozí komunikaci, proto je systém nemůže zanést do databáze, ale člověk s nimi pracovat může. Pokud zpráva z EDI centra dojde, ale nelze ji automaticky zanést do databáze, probíhá její kontrola pracovníkem IT oddělení. (Štvan, 2011)

Samozřejmě, že dříve než se přistoupí k náhradním řešením (email nebo kurýr), probíhají pokusy o obnovení spojení, použití alternativního přenosu nebo ruční zanesení objednávek, pokud se ve zprávě vyskytne chyba. Celý proces lze potom namodelovat takto (Obrázek 18: Proces náhradního zanesení objednávek na služby (zdroj: Autor)).



Obrázek 18: Proces náhradního zanesení objednávek na služby (zdroj: Autor)

Ke spuštění tohoto procesu dojde, pokud nejsou objednávky ve smluvený čas zaneseny v systému, to identifikuje OPS[15]. Na řešení problému v rámci vlastního IS má každá strana 30 minut a pak dojde na náhradní řešení.

Shrneme-li tento plán na zachování kontinuity, přenos je primárně řešen po samostatné lince, případně pomocí internetu a až když dojde na úplnou ztrátu

[15] Operativní pracovník skladu. (zdroj: Autor)

konektivity, je použit náhradní plán a tím je doprava dat kurýrní službou. Toto řešení je opět na vysoké úrovni a najít případ, kdy by selhalo, je velice těžké.

3.5.4 Lidský faktor

V měkkých systémech vždy hraje velkou roli lidský faktor. V tomto konkrétním procesu je většina činností automatizována, chyba způsobená lidským faktorem může nastat při zadávání objednávky a při práci s elektronickými dokumenty. Většinou se bude jednat o problém s datovým typem, který se objeví při vkládání objednávky do databáze v distribučním centru nebo o špatný formát celé EDI zprávy a to pak vede k problémům v EDI centru (to již bylo zmíněno v kapitole 3.5.3 o datových přenosech). Jak již bylo výše řečeno, tyto problémy se řeší kontrolou EDI zprávy a pokud se opravdu jedná jen o neshodu v datových typech, jinak jsou data srozumitelná, pracovníci IT mohou tato data zanést ručně.

Prevencí jistě je přijímání dostatečně kvalifikovaného personálu a jeho pravidelné průběžné školení. Nicméně lidskou chybu pramenící z nepozornosti, únavy nebo prostého omylu, nelze vyloučit nikdy.

3.6 Výsledek

Při hodnocení plánů kontinuity je nutné vzít v úvahu, že tato firma neimplementovala plány pro zachování kontinuity primárně podle žádných norem, ale dle citace jednoho manažera „tak aby to fungovalo“. Toto prohlášení přesně vystihuje situaci. Byl zde použit rozum a zkušenosti pracovníků ze všech zainteresovaných oborů, které se, jak je obecně známo, nedají ničím vyvážit.

Při hodnocení je potřeba mít na paměti určitá fakta, tato firma je z oblasti logistiky, kde je EDI jedním z hlavních způsobů komunikace s naprostou většinou zákazníků. Jde o typický proces a kontakt se zákazníky pomocí EDI probíhá téměř ve všech případech. Míra rozsahu řešení se může někomu zdát přehnaná, ovšem není tomu tak, protože se jedná o nejdůležitější proces v EDI, který má přímý vliv na business všech zúčastněných stran. Náklady na veškerou IT infrastrukturu, smluvní závazky atd. se dělí mezi všechny zákazníky, proto je tento stav vyhovující.

Dílčí zhodnocení jsou uvedena na konci každé kapitoly, souhrnné zhodnocení lze nalézt v následující tabulce (Obrázek 19: Tabulka s hodnocením plánů kontinuity v

FM Logistic). Každému identifikovanému riziku, byla ve výsledku přidělena stejná váha, protože mají všechna stejný dopad, tedy úplné přerušení sledovaného procesu. Dále je u každého rizika hodnocení rozděleno do tří hledisek, opět každé s jinou váhou (viz Obrázek 18: Proces náhradního zanesení objednávek na služby (zdroj: Autor)). Prvním hlediskem je vždy rozsah řešení, tím je myšlena celková propracovanost a úspěšnost řešení, pokud by bylo realizováno. Dalším hlediskem jsou náklady, tedy cena vybudování potřebné architektury, cena smluvních závazků za služby poskytované třetími stranami atd. Zde je ovšem nutné brát v úvahu, co vynaložení těchto nákladů přinese. Nejde jen o zachování kontinuity businessu, pokud dojde k nějakému přerušení, za těmito náklady je potřeba vidět i faktory jako vyšší důvěra zákazníků a dobré jméno společnosti. Jako poslední hledisko byla použita BCA. Tato hodnota je již více subjektivní (to je vyváženo nejnižší vahou, tedy nejmenším vlivem na výsledek) a skrývá se pod ní value for money nebo chcete-li benefit cost analýza, tedy jakýsi průnik předchozích dvou hledisek. Důraz je zde kladen na to, zda je zvolené řešení opravdu efektivní ve chvíli přerušení nebo havárie, ale také s přihlédnutím k nákladům a podmínkám na českém trhu. Detailní vysvětlení je uvedeno následně podle jednotlivých rizik.

Riziko	Hledisko	Váha	Hodnocení (0 - 10)	Celkem
Zásobování elektrickou energií (viz 3.5.1)	rozsah řešení	1,2	9	10,8
	náklady	0,8	7	5,6
	BCA	0,5	10	5
Funkční HW (viz 3.5.2)	rozsah řešení	1,2	9	10,8
	náklady	0,8	8	6,4
	BCA	0,5	9	4,5
Datové přenosy (viz 3.5.3)	rozsah řešení	1,2	10	12
	náklady	0,8	9	7,2
	BCA	0,5	9	4,5
Lidský faktor (viz 3.5.4)	rozsah řešení	1,2	8	9,6
	náklady	0,8	10	8
	BCA	0,5	7	3,5
SUMA (maximum 100)				**87,9**

Obrázek 19: Tabulka s hodnocením plánů kontinuity v FM Logistic (zdroj: Autor)

Nyní bude uvedeno několik komentářů k jednotlivým rizikům. U bodu zásobování elektrickou energií (viz 3.5.1) je rozsah řešení na takové úrovni jakou český trh poskytuje, chybějící náhradní poskytovatel je problém, na kterém ovšem společnost FM Logistic nic nezmění. Vzhledem k tomu, že provoz je na minimální úroveň obnoven v krátkém čase, maximálně v řádu minut a k výpadku energie pro servery a tu nejdůležitější IT infrastrukturu nedojde vůbec, nelze hodnotit jinak než velkým počtem bodů. Náklady na pořízení tohoto řešení jsou sice poměrně vysoké, to ovšem vyvažuje téměř nepřerušený provoz, proto známka 8. V reálném provozu je toto řešení tak spolehlivé, že benefit cost analýzu nelze hodnotit jinak než maximem.

Jako další riziko bylo identifikováno zachování funkčnosti hardwaru (viz 3.5.2) a uchování dat. Zejména systém zálohování a značně redundantně řešená IT infrastruktura s řízením jak fyzického, tak elektronického, přístupu k datům, je bez pochyb také velice spolehlivý. Při navrhování zlepšení byla zmiňována pouze větší péče o zálohy na páskách, proto lze hodnotit opět velmi vysokými body. Náklady na toto řešení musely být značné, zejména v oblasti pořízení hardwaru, tato společnost má ovšem své stálé dodavatele a při velikosti jejích odběrů, se jistě lze dohodnout na výhodné ceně. Navíc s přihlédnutím k tomu, že veškerou tuto technologii používá každý business proces a protože veškeré servery běží bez přerušení již přes jeden a půl roku, nebyly tyto náklady rozhodně vynaloženy zbytečně.

Datové přenosy (viz 3.5.3) poskytují externí firmy, proto nelze ovlivnit jejich spolehlivost. To je ovšem nahrazeno dostatkem náhradních řešení a procesů sdílení informací se zákazníkem při úplném výpadku datových komunikačních kanálů. Zde je rozsah řešení naprosto bez výhrad. Náklady na tato náhradní řešení se kalkulují se zákazníkem dodatečně, až když se identifikuje, na čí straně problém vznikl. Proto lze jejich hodnocení těžko generalizovat. Rozhodně nebudou nijak závratné proti nákladům na ztráty, které by mohly vzniknout. Vzhledem k tomuto faktu, je i výsledek benefit cost analýzy vysoký.

Řešení selhání, opomenutí a chyb lidského faktoru (viz 3.5.4) je v měkkých systémech vždy opravdu velkým problémem. V tomto procesu je řešen hlavně vytěsněním lidského faktoru v největší možné míře. Většina činností je automatizovaná, a to je zřejmě nejlepší řešení tohoto problému. Náklady na zavedení elektronických dokumentů jsou vyváženy úsporou času a administrativních nákladů, které elektronická výměna dat ušetří, proto zde připadlo nákladům největší bodové ohodnocení. Nicméně

ani to vliv lidského faktoru neodstraní úplně, proto je hodnocení benefit cost analýzy nižší.

Pokud by bylo vše hodnoceno 10 body (maximum), celkový výsledek by byl 100, což by byl výsledek limitně se blížící ideálnímu řešení. Toho lze dosáhnout pouze s extrémně rostoucími náklady. Společnost FM Logistic dosáhla hodnocení 87,9 bodu, což lze považovat za naprosto uspokojivý výsledek, vyjádřeno spravedlivým školním hodnocením výborný. A i když navrhovaná zlepšení posouvají hranice těchto plánů ještě dál, tak je to vždy za cenu značného zvýšení nákladů.

Na tomto konkrétním příkladu je patrné, že dobrý plán na udržení kontinuity činnosti lze vytvořit i bez přímého řešení podle norem a standardů. Je možné tvorbu založit na znalostech a zkušenostech odborných pracovníků a jejich kreativitě, ale tento způsob řešení je pak mimořádně náročný na lidský kapitál, kterým nedisponuje zdaleka každá společnost. Ty společnosti, které nemají takové štěstí na schopný personál, mohou využít příručky jako např. PAS77[16], to je publikace vydaná na základě best practices (nejlepších zkušeností) z oboru, doplňující normy BS 25999. I publikace tohoto typu vycházejí z praktických poznatků, které zobecňují pro potřeby různě zaměřených společností.

[16] Public Available Specification, česky veřejně dostupná specifikace.

4 Závěr

Pro vypracování analýzy plánů kontinuity aplikovaných na business proces bylo nutné se nejdříve seznámit s teoretickým základem jak Business Continuity Managementu (kapitola číslo 1) tak i se základy úžeji specifikovaného IT Service Continuity Managementu (kapitola číslo 2). Pro implementaci těchto procesů je nezbytné pochopit základní principy a naprosto nepostradatelné je akceptovat jejich důležitost. Protože pokud nebude business continuity manažer schopný obhájit náklady na plány pro zachování činnosti u nadřízených pracovníků, nebude možné plány rozvíjet na dostatečné úrovni.

Teorie byla zpracovávána tak, aby působila kompletně, uceleně a logicky odpovídala znalostem potřebným k vypracování teoretické části, ale i tak aby shrnula poznatky a znalosti týkající se této perspektivní manažerské disciplíny, protože v současně době česky psané publikace k této problematice téměř neexistují.

Hlavním přínosem práce bylo provedení analýzy konkrétního ITSC plánu ve společnosti FM Logistic (kapitola číslo 3). Jejím základem byl business proces, výrazně podporovaný informačními technologiemi. Po stručném uvedení do prostředí společnosti a vysvětlení používaných technologií byla provedena analýza rizik. Výstupem bylo určení konkrétních rizik a ta se stala základem pro analýzu jednotlivých plánů z hlediska každého ze zásadních rizik. Závěrečné hodnocení bylo vypracováno tak, aby co nejvěrněji a nejobjektivněji reflektovalo realitu nejen s racionálním přihlédnutím k nákladům, ale i k odvětví kde firma působí. Výsledek hodnocení ve společnosti FM Logistic byl shrnut jako výborný. Všechna navržená zlepšení či úpravy (které lze nalézt na konci každé kapitoly hodnotící řešení jednoho z rizik) by již vedly k neúměrnému zvýšení nákladů proti přínosům, které by přinášela. Tato analýza je přínosem jak pro tuto práci, tak by ji mohla využít analyzovaná firma, jako nezávislý pohled na sledovanou činnost.

Vzhledem k tomu, že v praxi současných českých firem není BCM dosud standardem, jsou možnosti budoucího rozšíření práce velmi rozsáhlé a různorodé. Lze navrhnout několik variant: prohloubení analýzy i na další procesy, přípravu projektu na změnu IT infrastruktury např. ve prospěch virtualizace nebo přípravu projektu, který optimalizuje náklady na hardware vzhledem k požadavkům na jeho spolehlivost.

Citovaná literatura

storyflex.cz. (2011). Získáno 20. květen 2011, z Business Continuity Management (BCM): http://www.storyflex.cz/229-business-continuity-management-bcm.html

BS 2599. (nedatováno). *Norma*.

BSI. (2006). *IT Service Continuity Management: Code of Practice.* London: BSI.

Cihlářová, A. (2010). Diplomová práce. *Aplikace metod BCM do havarijního*. Praha, Česká republika.

Haluzík, R. (11. 9 2007). *Business Continuity Management a aplikovaná metodika*. Získáno 20. 4 2011, z businessworld.cz: http://businessworld.cz/aktuality/business-continuity-management-a-aplikovana-metodika-2729

Historie FM Logistic. (nedatováno). Získáno 2011, z FM Logistic.

Martanová, K. (duben 2010). Jak obnovit procesy z pohledu IT? *1Business Continuity Management*. Praha.

Risk Analysis Consultants, s. r. (2010). *BS 25999-1 Code of practice for business continuity management* . Získáno 5. 5 2011, z iso27000.cz: http://www.iso27000.cz/rac/homepage.nsf/CZ/BS%2025999-1

Risk Analysis Consultants, s. r. (2010). *BS 25999-2 Specification for business continuity management*. Získáno 2011. 5 5, z iso27000.cz: http://www.iso27000.cz/rac/homepage.nsf/CZ/25999-2

Risk Analysis Consultants, s. r. (2010). *Nová řada ISO/IEC 27000* . Získáno 2011, z iso27000.cz: http://www.iso27000.cz/rac/homepage.nsf/CZ/27031

Šilhánová , E. (7. prosinec 2010). *Firemní kultura není jen soupis nudných pravidel*. Získáno 22. květen 2011, z Hospodářské noviny: http://hn.ihned.cz/c1-48485640-firemni-kultura-neni-jen-soupis-nudnych-pravidel

Szabados, L. (2008). *Business Continuity Management: Manager's Handbook.* TATE International Slovakia, s.r.o.

Winkler, J. (2011). Sociologie. Brno.

Zdvořáček, J. (2011). *EDI.* Semestrální práce z předmětu Podnikové informační systémy 4IT314, Kladno.

SHARP, J. Jak postupovat při řízení kontinuity činností: naplnění požadavků BS 25999 = The route map to business continuity management. Praha: Risk Analysis Consultants, 2009. ISBN 978-80-254-3992-0.

Za značnou část informací musím znovu poděkovat panu Ing. Markovi Štvanovi.

Seznam obrázků

Seznam zkratek

- IT informační technologie
- ICT informační a komunikační technologie
- HW hardware
- SW software
- IS infomační systém
- EDI elektronická výměna dokumentů
- HQ vedení
- DC distribuční centrum
- VPN virtuální privátní síť
- BCA benefit cost analýza

Přílohy

Struktura souboru náhradní objednávky ve formátu *.xls, je smluveno, že se používají verze 2000/2003, tedy opravdu *.xls, ne *.xlsx.

Název pole	Typ (maximální délka)	Popis
nbon	char (10)	číslo objednávky
refcde	char (10)	referenční číslo
dbon	char (10)	datum objednání
dliv	char (10)	datum doručení
POnumber	char (35)	doba na doručení
soldnb	char (10)	číslo zakázky (platícího)
shipnb	char (10)	číslo zakázky (příjemce)
soldname	char (35)	jméno plátce
shipname	char (35)	jméno příjemce
soldstr	char (60)	adresa platícího (ulice)
soldcity	char (40)	adresa platícího (město)
soldzip	char (10)	adresa platícího (zip kód)
shipstr	char (60)	adresa příjemce (ulice)
shipcity	char (40)	adresa příjemce (město)
shipzip	char (10)	adresa příjemce (zip kód)
ligcde	int	řádek v databázi IS zákazníka
ref	varchar (20)	identifikace zboží v databázi IS zákazníka
nstitem	varchar (35)	popis zboží
gty	int	množství
UOM	char (3)	jednotky
comment	varchar (120)	komentář

Datové typy:

- *char* – textový řetězec
- *int* – číselná hodnota
- *varchar* – textový řetězec