

Mgr. Lukáš Limberk; Mgr. Monika Johaníková

Vztah Business Continuity Managementu a managementu rizik

Anotace

Význam analytické fáze životního cyklu Business Continuity Managementu (BCM) spočívá v porozumění organizaci pomocí identifikace klíčových produktů, kritických činností a zdrojů pro zajištění kontinuity. Požadovaným výsledkem je, že program BCM je v souladu s cíli, závazky a povinnostmi organizace, které jsou jí uloženy smluvně nebo zákony. Analytické aktivity se realizují ve dvou krocích: analýza rizik (Risk Assessment) a analýza dopadů (Business Impact Analysis, BIA).

Klíčová slova

Řízení kontinuity činností, krizové řízení, řízení rizik, analýza dopadů, analýza rizik.

Summary

Importance of analytical phase of BCM life cycle consists in understanding the organization through identification of key products, critical services and resources for ensuring business continuity. Required status is harmonization of BCM program with goals, obligations and duties by contracts or legislative. Analytical activities are realized in two steps: Risk assessment and Business impact analysis.

Keywords

Business Continuity Management, Crisis Management, Risk Management, Business Impact Analysis, Risk Analysis/Risk Assessment.

Stručně k významu řízení rizik

Riziko je nedílnou součástí většiny manažerských aktivit. Na jedné straně se spojuje s očekáváním zvláště dobrých hospodářských výsledků, na straně druhé je toto očekávání doprovázeno nebezpečím podnikatelského neúspěchu vedoucího ke ztrátám, které mohou být tak velkého rozsahu, že to může vést až k destabilizaci organizace. V době globalizace ekonomiky spojené s častými změnami podnikatelského prostředí, je nezbytné, aby management rizika byl integrální součástí řízení podniku. Zavedením kvalitního managementu rizik v organizaci, se zvyšuje její odolnost vůči negativním dopadům vývoje podnikatelského okolí i flexibilita její reakce na možné změny a příležitosti. Ačkoliv je riziko spojeno spíše se soukromou podnikatelskou sférou, ani v neziskové veřejné sféře se manažeři nevyhnou situacím, kdy budou muset čelit nepředvídaným skutečnostem, které mohou mít závažný vliv na chod jimi řízených institucí.

Analýza rizik

Analýza rizik se zaměřuje na posouzení pravděpodobnosti, s jakou budou kritické procesy ovlivněny případným incidentem. Součástí analýzy rizik je i hodnocení úrovně rizik a navrhnutí takových opatření, která budou minimalizovat riziko vzniku závažných incidentů ovlivňující kritické funkce organizace. Základním účelem hodnocení rizik je identifikovat, určit a ohodnotit rizika, kterým organizace čelí ve vztahu ke svým kritickým procesům (nebo aktivitám) a stanovit přijatelnou úroveň rizika spolu s plánem opatření, která budou pomáhat kritickým procesům (nebo aktivitám) čelit identifikovaným hrozbám.

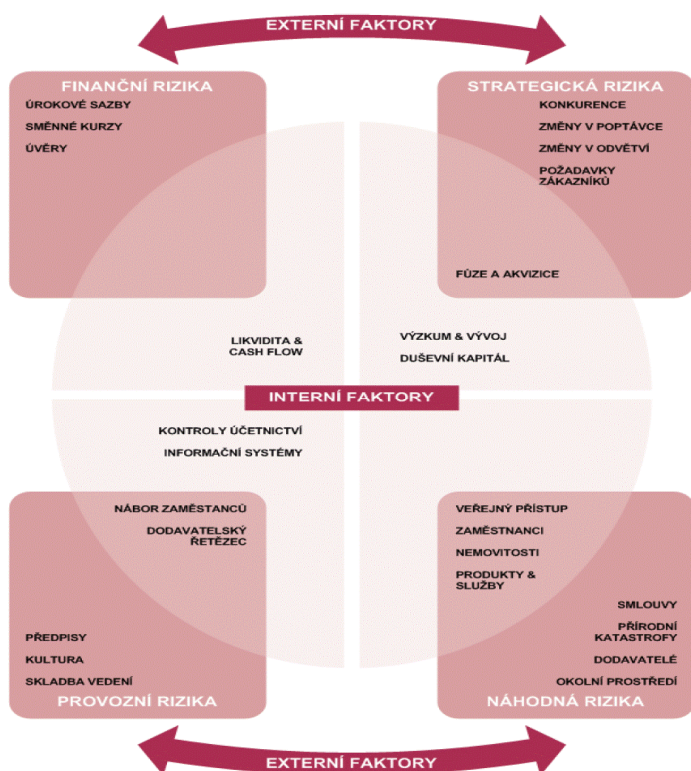
Je výhradním rozhodnutím organizace jaký přístup k posuzování rizik zvolí¹. Je však důležité, aby byl tento přístup vhodný a příslušný všem požadavkům organizace. Pravděpodobnost některých hrozeb může být relativně vysoká, přičemž dopady se můžou klasifikovat na minimální úrovni. Naopak, jiné hrozby můžou být méně pravděpodobné, zato jejich následky můžou být velmi vážné, nebo dokonce můžou ohrožovat samotnou existenci organizace. Konečné slovo by měl mít vrcholný management, který s přihlédnutím na svou vizi o směřování organizace rozhodne, která rizika považuje za „zanedbatelné“, „únosné“, „vážné“, nebo „velmi vážné až katastrofické“. Přesnost a správnost rozhodnutí závisí především na kvalitě informací, z kterých management vychází.

Vnější a vnitřní faktory rizik

Rizika, kterým je vystavena organizace a její činnosti, mohou vyplývat z vnějších nebo vnitřních faktorů. Na ilustraci jsou uvedeny příklady nejpodstatnějších rizik z různých oblastí a ukazuje, že příčiny některých konkrétních rizik leží vně i uvnitř organizace. Rizika mohou být rozdělena podle jejich druhu, jako například rizika strategická, finanční, provozní, náhodná atd.

¹ Pro účely hodnocení rizik v rámci BCM se obecně rozlišuje analýza rizik procesů a analýza rizik majetku/hodnot (assets).

Ilustrace: Příklady vlivů klíčových rizik²



Pojetí rizika v kontextu Business Continuity Management

Chápání rizika není jednotné. V odborné literatuře i v praxi se můžeme setkat s různými pojetím. V užším pojetí se na riziko nahlíží z negativní stránky rizika, jako na pravděpodobnost vzniku ztráty, možnost vzniku okolností, které ohrozí dosažení cílů organizace. Tato rizika jsou označována jako **rizika čistá**. V hospodářské praxi se však hovoří o **rizicích podnikatelských**, které kromě negativní stránky mají i svou pozitivní stránku. Takto pojaté riziko lze chápat jako možnou odchylku (pozitivní i negativní) od plánovaných či očekávaných výsledků resp. pravděpodobnost jejího vzniku. Jde tedy o odchylku skutečně dosažených výsledků od plánovaných, a to v důsledku odchylky žádoucí (vyšší zisk) nebo nežádoucí (ztráta). Na riziko lze nahlížet z mnoha hledisek. K základním způsobům třídění patří členění rizik na:³

- **Podnikatelská a čistá** – již bylo zmíněno výše.
- **Systematická a nesystematická**. Systematické riziko je riziko, které v různé míře zasahuje všechny hospodářské jednotky v oblasti podnikatelské činnosti. Jedná se o změny daňové legislativy, změny trhu (změny cen surovin, ekonomické cykly aj.). Rizika nesystematická jsou specifická ve smyslu jejich působení na jednotlivé

² A Risk Management Standard, The Institute of Risk Management (IRM), London 2002. 28 s.

³ VEBER, J. a kolektiv, Management: Základy, moderní manažerské přístupy, výkonnost a prosperita, Management Press, Praha 2009. 604 s. ISBN 978-80-7261-200-00.

organizace. Zdrojem tohoto rizika může být například odchod klíčových zaměstnanců, selhání významného subdodavatele, havárie výrobního zařízení a jiné.

- **Vnitřní a vnější:** Vnitřní rizika se vztahují k faktorům uvnitř firmy (rizika selhání pracovníků, rizika výpadků IT systémů apod.). U vnějších rizik se jedná o taková rizika, která se vztahují k podnikatelskému okolí, ve kterém firma podniká. Jedná se o externí zdroje, které se dále člení na makroekonomické (v podobě ekonomických, sociálních, technicko-technologických, ekologických vlivů) a mikroekonomické (konkurence, dodavatelé, odběratelé aj.).
- **Ovlivnitelná a neovlivnitelná:** Ovlivnitelné je takové riziko, které lze eliminovat, resp. oslabit s opatřením orientovaným na jeho příčiny, a to ve smyslu snížení pravděpodobnosti vzniku či rozsahu možných nepříznivých situací. U neovlivnitelných rizik nelze působit na jejich příčiny, ale lze přijmout opatření snižující nepříznivé následky těchto rizik.
- **Primární a sekundární:** Sekundární riziko je vyvoláno přijetím určitého opatření na snížení primárního rizika, tvořeného všemi výše uvedenými faktory. Příkladem může být vytvoření společného podniku se zahraničním partnerem, snížíme tak sice některá rizika diverzifikací trhu, ale zároveň vzniknou nová rizika (odlišná firemní kultura aj.).
- **Podle fází projektu:** Jedná se o fáze přípravy, realizace a provozu.

Významné je také členění rizik podle jejich věcné náplně. Z tohoto hlediska se obvykle rozlišují rizika:

- **Technicko-technologická:** Související s aplikací nových technologií a rizika ztrát z opotřebení zastaralých technologií.
- **Výrobní, provozní a operační rizika:** Nedostatek zdrojů různé povahy (surovin, materiálů, energie aj.), které mohou ohrozit výrobní proces. Rizika selhání dodávek zdrojů ze strany dodavatelů a podobně.
- **Ekonomická:** Například nákladová rizika, vyvolané růstem cen výrobních zdrojů.
- **Tržní:** Spojená s úspěšností produktů na trhu ve vztahu k objemu prodeje.
- **Finanční:** Jsou spojená se solventností organizace, resp. se schopností opatřovat zdroje pro financování svých záměrů a schopností dostávat svým závazkům.
- **Legislativní:** Hospodářská a legislativní politika vlády. (Daňové zákony, změna celní politiky aj.).
- **Politická:** Stávky, národnostní a rasové nepokoje, války, teroristické akce apod.
- **Environmentální:** Zpřísnění opatření na ochranu životního prostředí a s ní rostoucí náklady na tato opatření a podobně.
- **Spojená s lidským činitelem:** Podvodné či nezákonné jednání zaměstnanců a jiné.
- **Informační:** Týkající se firemních IT systémů a ochrany dat.
- **Zásahy vyšší moci:** Havárie a nebezpečí živelních pohrom (požáry, povodně, zemětřesení aj.). Také nelze opomenout hrozbu teroristických útoků.

Management rizika

Ve světě neustálých změn a rostoucích rizik, které mohou ovlivnit firemní procesy, roste i význam managementu rizik pro organizaci. J. Veber jej definuje takto:

„Management rizika lze chápat jako systematický a koordinovaný způsob práce s riziky, uplatňovaný v rámci celé organizace, tj. na všech úrovních řízení, zahrnující všechny procesy a všechny druhy rizik při respektování jejich vzájemných vazeb.“⁴

Základní cílem managementu rizika je zajištění přežití organizace, neboli udržení si jejího postavení a její další rozvoj. Management rizika je možné rozdělit do těchto fází.

Vymezení kontextu a cílů managementu rizika

Smyslem této fáze je určení prostředí firmy, a to jak vnějšího, tak vnitřního prostředí. Dále stanovení cílů managementu rizik v těsné návaznosti na strategické cíle podniku. V této fázi je třeba určit **rizikovou kapacitu**, což je maximální možná ztráta, se kterou se organizace je schopná vyrovnat. Její výše se odvíjí od solventnosti⁵ organizace. V rámci rizikové kapacity se určí takové riziko, jež odpovídá výši ztráty, kterou je organizace ochotna přijmout, pak mluvíme o **přijatelném riziku**. Určení velikosti přijatelného rizika, je strategickým rozhodnutím a jeho velikost také závisí na ochotě vedení organizace riskovat.

Stanovení významnosti rizika

Organizace jsou vystavovány velkému množství rizik, je tudíž třeba je rozdělit, jelikož není možné a ani účelné se zabývat všemi riziky⁶. Například některá rizika jsou sice významná, ale není možné je z hlediska enormní nákladovosti opatření nijak řešit. Na druhé straně jsou rizika sice méně významná, ale náklady na opatření jsou přijatelnější. Při zavádění opatření půjde tedy o podřízení se určitým kompromisům. Ke stanovení významu rizik se používá analýza citlivosti a matice hodnocení rizik.

Analýza citlivosti

Cílem analýzy citlivosti je zjistit změnu hospodářských výsledků a dalších ukazatelů v závislosti na změnách faktorů, které zapříčiňují tyto změny a jejichž budoucí hodnoty jsou nejisté. Jako ukazatel se určí například zisk a ten bude posuzován, resp. bude sledována jeho procentuální změna v závislosti na očekávaných dopadech určitého rizika. K jednotlivým rizikům pak bude přisouzena hodnota této změny (nejčastěji procentuální) jejíž pomocí bude možné vytvořit stupnici významnosti rizik.

⁴ VEBER, J. a kolektiv, Management: Základy, moderní manažerské přístupy, výkonnost a prosperita, Management Press, Praha 2009. 604 s. ISBN 978-80-7261-200-00.

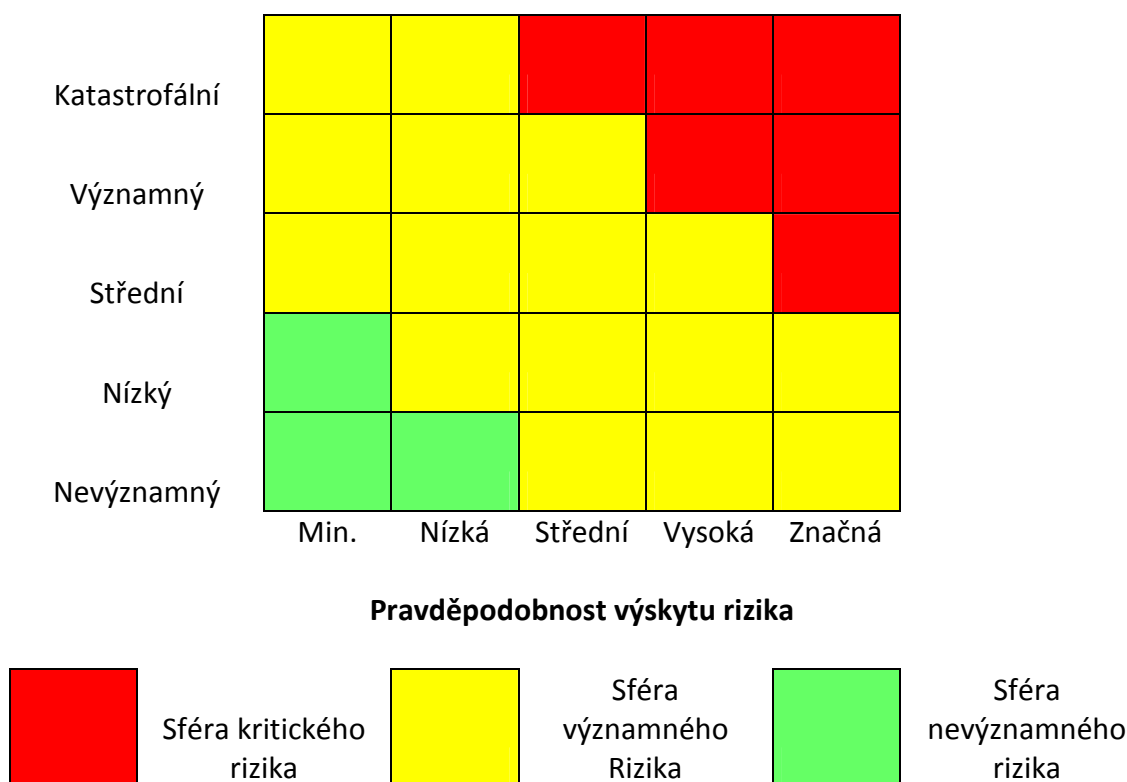
⁵ Solventnost = stálá, dlouhodobá schopnost podniku hradit své závazky v termínech splatnosti. Schopnost dostávat svým závazkům v krizových situacích, resp. hradit ztráty z činnosti.

⁶ Před samotným hodnocením by měla být, stejně jako u analýzy dopadů, vytvořena metodologie k procesu hodnocení rizik (viz kapitola analýza dopadů).

Matice hodnocení rizik

Zatímco analýza citlivosti je kvantitativní metodou, matice hodnocení rizik jsou nástrojem expertního hodnocení založeného na znalostech a zkušenostech těchto expertů. Podstata této metody je v posuzování rizika ze dvou hledisek, a to jednak z hlediska pravděpodobnosti výskytu činitele rizika a za druhé z hlediska intenzity působení rizika na podnikatelské činnosti firmy. Činitel rizika je pak tím významnější, čím je pravděpodobnější a jeho důsledky intenzivnější. Pro toto ohodnocení se používá obvykle stupnice, jejíž možnou podobu ukazuje ilustrace.

Ilustrace: Příklad matice hodnocení rizik.



Měření rizika

Jednotlivé rizikové faktory nepůsobí izolovaně, ale společně působí na dosahování cílů organizace. Cíle bývají vyjádřené výší zisku, likviditou a rentabilitou firmy, atd. Pro vyjádření rizika z hlediska dosahování hodnot těchto ukazatelů slouží:

- statistické charakteristiky variability (zisku, cash flow, rentability), jimiž jsou rozptyl, směrodatná odchylka a variační koeficient,
- nástroje a metodiky založené na konceptu Value at Risk.

U statistických charakteristik variability platí, že čím větší jsou tyto charakteristiky, tím větší je riziko vztahující se k zvolenému ukazateli. Nedostatkem těchto charakteristik

rizika je, že disponují dobrou vypovídací schopností, jen pokud je rozdělení pravděpodobnosti ukazatele, k němuž se riziko vyjadřuje, symetrické.

Tento nedostatek odstraňuje novější nástroj, a to je Value at Risk (riziková hodnota). Jde o beze sporu nejrozšířenější nástroj sloužící pro řízení tržních rizik ve světových bankách a finančních institucích. Ukazatel Value at Risk odhaduje maximální pravděpodobnou ztrátu portfolia finančních nástrojů v důsledku nepříznivých vlivů a pohybů tržních sazeb. Tuto metodu je možné používat mimo jiné i k výpočtu kapitálových požadavků k tržním rizikům pro účely kapitálové přiměřenosti.⁷

Hodnocení rizika a rozhodování o riziku

V této fázi se jedná o určení přijatelnosti rizika a rozhodnutí o způsobech zvládnutí rizik. Míra přijatelnosti rizika závisí na výši zmiňované tolerance firmy k riziku a stanovení maximální výše rizika, kterou je firma ochotna podstoupit. Na základě stanovení rizikové tolerance se pak uplatňují různé přístupy k riziku. V případě, kdy riziko nepřesahuje hodnotu rizikové tolerance a firma se rozhodne, že nebudou realizována žádná opatření, jde o **retenci rizika**, při které je firma připravena se s následky vypořádat z vlastních zdrojů. Pokud je riziko označeno za nepřijatelné, tak se mu organizace může vyhnout. **Vyhnutí se riziku** spočívá v upuštění od určitých aktivit nebo projektů, které by mohly být ohroženy rizikem, kterému se chce organizace vyhnout. Je však třeba si uvědomit, že tímto jednáním může docházet ke ztrátě příležitostí a oslabení konkurenceschopnosti. Další možností je **zmírnění rizika**, při kterém jsou realizována určitá opatření vedoucí ke snížení rizika. Zde je třeba zvolit vhodný způsob tohoto snížení, a to buď:

- odstranění či alespoň snížení příčin vzniku rizika;
- snižování negativních dopadů rizika;
- přesun rizika na jiné subjekty (pojišťovny, dodavatel, odběratele apod.).

Snížené riziko se pak označuje jako reziduální (zbytkové) riziko a nijak neupravené riziko jako riziko inherentní. Při rozhodování o způsobech zmírnění rizika je nutné si uvědomit, že:

- opatření se nemohou zaměřovat na jednotlivá rizika, ale je třeba je brát jako vazbami provázaný soubor rizik;
- s každým opatřením jsou spojeny určité náklady, které je třeba posuzovat;
- jde o jakési snížení rizika na ekonomicky účelnou míru, tj. jde o určitou optimalizaci rizika;
- opatření mohou sice snížit některá primární rizika, ale zároveň vyvolat sekundární rizika.

⁷ VEBER, J. a kolektiv, Management: Základy, moderní manažerské přístupy, výkonnost a prosperita, Management Press, Praha 2009. 604 s. ISBN 978-80-7261-200-00.

Přístupy ke snižování rizika

Opatření prováděná pro snížení rizika se dají rozdělit do dvou základních skupin:

- Opatření zaměřená na příčiny rizika, která jsou zaměřena na předcházení výskytu rizikových situací, oslabením příčin vzniku rizik.
- Opatření orientovaná na oslabení nepříznivých dopadů rizika, která se zavádějí, pokud je předcházení výskytu rizikových situací nemožné anebo příliš nákladné. Jedná se o opatření snižující negativní dopady v případě výskytu rizika.

V praxi se opatření směřující k zamezení nebo oslabení příčin rizika vyskytují méně často, nežli opatření zaměřená na snížení negativních dopadů výskytu rizika. Velikost těchto dopadů do značné míry závisí na schopnosti pohotové a účinné reakce organizace na vzniklou krizovou situaci. Pro zajištění schopnosti pohotové a kvalitní reakce na tyto situace, které lze ve většině případů předvídat, je nezbytné vypracovat určité kontingenční (havarijní, krizové, apod.) plány. Mezi tyto plány je možné zařadit i plány kontinuity činností organizace.

Management kontinuity činností je součástí managementu rizik⁸. BCM je jakýmsi článkem rámce managementu rizik, který napomáhá porozumět rizikům provozu nebo podnikání a dopadům těchto rizik. Management rizik se soustředí na řízení rizik komplexněji⁹, zatímco management kontinuity činností je zaměřen především na identifikaci klíčových produktů, které jsou nezbytné pro fungování a přežití organizace. A také stanovuje opatření pro zajištění minimální úrovně chodu klíčových činností, neboli těch činností, které jsou nezbytné pro zajištění klíčových produktů. Současně stanovuje postupy a opatření nutné proto, aby organizace mohla nadále plnit své závazky.

Analýza aktuálních hrozeb

V současné době není k dispozici v rámci Business Continuity managementu komplexní analýza hrozeb (rizik), kterými se soukromé organizace působící na území České republiky, nejvíce zabývají (neboli kterými riziky jsou nejvíce znepokojeni). Proto níže uvádím nejnovější studii¹⁰ BCI Institutu se zaměřením na kontinentální Evropu (bez Spojeného království) a tři vybrané oblasti působnosti organizace, v níž jsou obsaženy i názory respondentů z České republiky.

⁸ Například v bankách a jiných finančních institucích je obvykle tým Business Continuity Managementu zařazen pod Operační rizika, jelikož BCM je chápán jako jeden z nástrojů ke snižování rizika s velkým dopadem a nízkou pravděpodobností výskytu. Ve výrobních podnicích může být součástí oddělení Bezpečnosti apod.

⁹ Například řízení kreditního rizika, tržního, operačního rizik, rizika spojených s informační bezpečností, rizika spojená s dodavatelským řetězcem atd.

¹⁰ Studie byla prováděna v období listopad – prosinec 2012 a bylo do ní zapojeno 730 organizací z 62 zemí světa. Za kategorii „Kontinentální Evropa“ bylo obdrženo 110 odpovědí. Oslovení respondenti jsou členové BCI Institutu.

Vyhodnocení rizik podle sektoru působnosti organizace pro rok 2013¹¹ (vzorek)

Top 10 hrozeb pro výrobní sektor

39 respondentů

1.	Narušení dodávek
2.	Incident spojený s kvalitou produktu
3.	Incident spojený s bezpečností produktu
4.	Incident v oblasti bezpečnosti práce
5.	Útok na IT společnosti
6.	Prolomení dat
7.	Neplánované výpadky IT a telekomunikací
8.	Omezení dostupnosti přírodních zdrojů
9.	Incident spojený s neetickým chováním společnosti
10.	Přerušení dodávek technické infrastruktury

Top 10 hrozeb pro sektor IT a telekomunikace

110 respondentů

1.	Neplánované výpadky IT a telekomunikací
2.	Útok na IT společnosti
3.	Prolomení dat
4.	Bezpečnostní incident
5.	Přerušení dodávek technické infrastruktury
6.	Požár
7.	Insolvence klíčových zákazníků
8.	Nepříznivé počasí
9.	Náklady / dostupnost energií
10.	Incident v oblasti bezpečnosti práce

Top 10 hrozeb pro finanční sektor a pojišťovnictví

223 respondentů

1.	Neplánované výpadky IT a telekomunikací
2.	Prolomení dat
3.	Útok na IT společnosti
4.	Přerušení dodávek technické infrastruktury
5.	Bezpečnostní incident
6.	Nepříznivé počasí
7.	Nové právní předpisy a normy
8.	Teroristický útok
9.	Požár
10.	Dostupnost finančních prostředků / náklady na úvěr

Závěr

Výsledky analytické fáze v procesu BCM (analýza dopadů i analýza rizik) slouží jako vstupní podklady jak pro opatření ke zmírnění rizik, tak i pro následující fázi BCM procesu – **stanovení strategie BCM.**

¹¹ Horizon Scan 2013: Survey Report, The Business Continuity Institute, Caversham 2013 <http://www.thebci.org>