Od golfu k certifikaci BCMS

I certifikace může mít zajímavou historii. V případě BCMS[1] nebylo úplně snadné se jí dopátrat a poskládat celou mozaiku událostí dohromady. A jaký je současný stav?

Řízení kontinuity činností organizace (BCM, viz Box 1), jak je chápáno dnes, vyplynulo z požadavků na zajištění obnovy informačních systémů po haváriích sálových počítačů. Tradičně se havarijní plánování (disaster recovery planning, DRP) soustřeďovalo na obnovu technického vybavení po větším incidentu. Než se původní koncept DRP přerodil v dnešní „certifikovatelný" systém řízení kontinuity činností (BCMS, viz Box 1), uběhlo téměř 40 let.

Havarijní plán č. 1

Myšlenka na vytvoření formalizovaných pravidel a postupů řízené eskalace incidentů se zrodila jednoho nedělního odpoledne během hry golfu, psala se druhá polovina 70. let. Tím vášnivým hráčem golfu byl Norman Harris, viceprezident odpovědný za zpracování dat v Bank of Ohio.

V dobách hromadného zpracování dat prostřednictvím děrných štítků znamenala jakákoli drobná či větší závada sálového počítače obvykle narušení práce v celé bance. Bez ohledu na denní nebo noční dobu, bez jakéhokoli pokusu o předběžné posouzení závažnosti a rozsahu incidentu byl svými podřízenými ihned, a zpravidla i zbytečně, kontaktován Norman Harris. V dobách bez mobilních telefonů obnášelo vyřízení hovoru cestu do klubovny a zpět na odpaliště jamky č. 13, a to ještě v tom lepším případě.

Potřeba vytvořit a formalizovat postupy hlášení a zvládání ICT incidentů se tak zrodila z nutnosti eliminovat plané poplachy – byl vytvořen první plán obnovy po havárii (disaster recovery plan, DRP).

Potíže hned v prvním kole

Od počátku se první tvůrci DRP potýkali s tím, jak přesvědčit vedení svých společností, aby schválila nemalé investice do tvorby havarijních plánů a přípravy záložních lokalit. Zejména, když se jednalo o přípravu na závažné události a havárie, které s velkou pravděpodobností nikdy ani nenastanou. Investice do DRP bylo nutné zdůvodnit a před majiteli obhájit. To vedlo k vytvoření technik pro hodnocení potenciálních dopadů negativních událostí na celkové fungování společnosti. První metodiky analýz obchodních dopadů (business impact analysis, BIA) vznikaly ve Spojených státech v první polovině 80. let, a jsou tak o několik let starší než samotný koncept řízení kontinuity činností (viz Box 1).

Je důležité, že hned od začátku byla podchycena klíčová podstata implementace BCM. A to potřeba identifikovat důležité procesy, odhadnout následky jejich přerušení a na tomto základě navrhnout cenově efektivní strategie obnovy informačních technologií. Dnes je BIA neoddělitelnou, ale hlavně klíčovou součástí životního cyklu BCM.

BCM nebo BCMS — BOX 1

Organizace, které nemají potřebu deklarovat zavedení procesů řízení kontinuity (např. to jejich zákazníci nevyžadují), vystačí s BCM. Ty společnosti, od kterých stávající nebo potenciální partneři vyžadují vyšší garance spolehlivosti, budou usilovat o získání certifikace BCMS.

Řízení kontinuity činností (Business Continuity Management, BCM)
BCM je řídicí proces podporovaný vedením společnosti, který identifikuje potenciální dopady ztrát a jehož cílem je vytvořit takové postupy a prostředí, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností organizace v požadovaných časech a na předem stanovené minimální úrovni, v případě jejich narušení nebo ztráty. Jednotlivé činnosti spojené s implementací BCM jsou souhrnně označovány jako „životní cyklus BCM". [BS 25999-1]

Systém řízení kontinuity činností (Business Continuity Management System, BCMS)
Část celkového systému řízení, která prosazuje procesní přístup k implementaci, provozování, monitorování, přezkoumávání a zlepšování všech činností životního cyklu BCM. Přičemž systém řízení zahrnuje organizační strukturu, politiky a směrnice, odpovědnosti, postupy, procesy a zejména zdroje. [BS 25999-2] Vztah mezi první a druhou částí normy viz rovněž Box 3.

[1] Business Continuity Management System

Zrození BCM(S)

Počátky dnešního BCM(S) jsou datovány do poloviny 80. let. O rozšíření původního, čistě technicky zaměřeného konceptu se zasloužil jiný z pionýrů havarijního plánování. Vpravdě lidský rozměr dal původnímu DRP dnes již více než osmdesátiletý Ron Ginn (jeden z původních zakladatelů britského Business Continuity Institute). Jako první si totiž uvědomil, že obnova funkčnosti technologií ještě neznamená automatickou obnovou fungování celé společnosti.

Podle vytvořených a otestovaných DRP nebyl problém obnovit funkčnost sálových počítačů, včetně obnovy dat ze záloh, v záložní lokalitě. Nikdo však již neuvažoval nad tím, že bude nutné do záložní lokality přemístit zaměstnance, vytvořit jim vhodné podmínky pro práci. Nastavit postupy pro informování zaměstnanců o nastalé události a jejich pracovní náplni v následujících hodinách a dnech po havárii. Určit způsob a vymezit rozsah informací podávaných zákazníkům a médiím. Předem promyslet a zahrnout do plánů další aspekty související se zajištěním kontinuity a obnovy podnikání. To vše původní koncept plánování po havárii zcela opomíjel. A tak přichází na scénu BCM, na který je o několik let později aplikován systémový přístup k řízení kontinuity založený na cyklu PDCA (Plánuj – Dělej – Kontroluj – Jednej, Plan – Do – Check – Act).

Od obnovy ke kontinuitě

Byl to také Ron Ginn, kdo v roce 1985 takto rozšířený koncept původního DRP pojmenoval jako řízení kontinuity činností (BCM). Dodnes s nadsázkou rád říká, že si měl tehdy nechat spojení „business continuity“ patentovat [5].

V novém světle bylo ICT nutno chápat jako jeden ze zdrojů, které podporují fungování procesů a činností společnosti. Přičemž ale původní postupy a techniky DRP nebyly zatraceny, ale naopak nově aplikovány na mnohem širší okruh procesů a podpůrných činností. Dnes jsou DRP chápány jako podmnožina BCP (plány kontinuity činností) zaměřená na obnovu ICT zdrojů po incidentu nebo havárii. Přičemž BCP obsahují postupy a kroky pro zajištění kontinuity (přechodné období) a následné obnovy (návrt k normálu) procesů a činností.

Dalším logickým krokem ve vývoji BCM byl posun od pouhé obnovy, kdy se pouze vyčkává, až se něco stane, a teprve pak se začíná jednat, ke kontinuitě, kdy jsou dopředu promýšleny kroky obnovy. Nadto jsou zde připraveny alternativní způsoby fungování v době výpadku. Kde to jde, řeší se prevence a je snaha se hrozbám vyhnout či alespoň pravděpodobnost jejich úspěchu minimalizovat (zejména proto je součástí programu BCM také řízení rizik). Namísto pasivního vyčkávání organizace aktivně řídí kontinuitu svého podnikání.

Přesto trvalo ještě řadu let, než se tento rozšířený koncept ujal. Ještě dnes je BCM v řadě společností chápáno jako aktivita spadající čistě do působnosti IT oddělení.

Ve znamení tří devítek — BOX 2

Britský standard pro řízení kontinuity činností organizace je rozdělen do dvou částí. Z pohledu případné certifikace BCMS je důležitější část 2, ve které je u jednotlivých požadavků doporučující „should“ (měl by) nahrazeno povinným „shall“ (musí).

Důkazem toho, že Britové nenechali při práci na standardu nic náhodě, je i samotný název. Číslo 999 je na Britských ostrovech číslem integrovaného záchranného systému.

- **BS 25999-1:2006, Řízení kontinuity činností organizace – Část 1:** Soubor postupů. Tento standard ustavuje proces, principy a terminologii BCM. Je sestaven formou návodu a doporučení správné praxe a ukazuje, jaké praktiky by organizace měla nebo mohla převzít, aby zavedla účinné řízení kontinuity činností. Organizace si mohou vybrat, budou-li dodržovat celý soubor postupů, nebo jen část. Standard lze použít pro vlastní hodnocení či hodnocení úrovně vyspělosti BCM jiných organizací. Soubor postupů není specifikací (neobsahuje povinné požadavky) pro řízení kontinuity činností.
- **BS 25999-2:2007, Řízení kontinuity činností organizace – Část 2:** Specifikace. Na rozdíl od první části obsahuje pouze ty požadavky, které mohou být objektivně auditovány (kontrolovány). Organizace pak může využít doklad o úspěšném zavedení BCMS k ujištění všech zúčastněných stran (vlastníci, zaměstnanci, zákazníci apod.), že je systém ustaven, provozován a funkční. 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.

Počátky BCMS certifikace

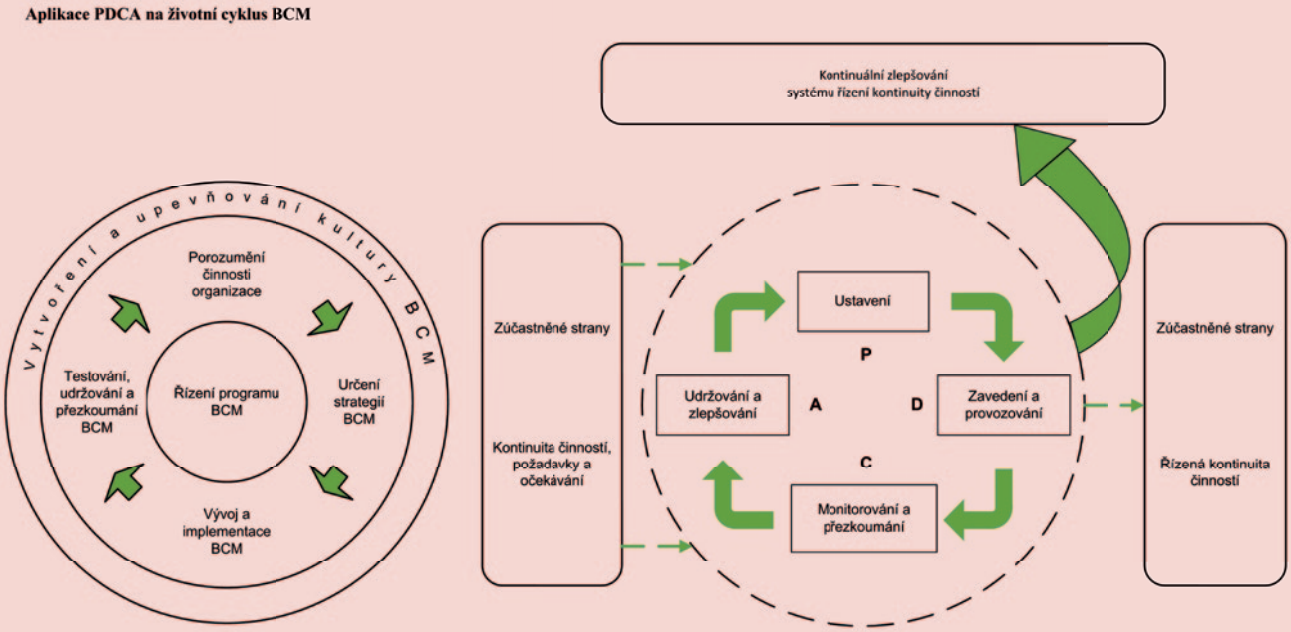
Prvním standardem, ve kterém se pojem business continuity management objevil, byl britský BS 7799 z roku 1995. Standard kromě jiných oblastí bezpečnosti vyzdvihl potřebu zavedení procesu řízení kontinuity činností pro minimalizaci následků a zotavení ze ztráty informačních aktiv.

Události na přelomu tisíciletí rozpoutaly novou vlnu zájmu o havarijní plánování a plánování kontinuity. V roce 2003 zveřejnil Britský normalizační institut (British Standard Institution, BSI) veřejně dostupnou specifikaci PAS 56, která sjednotila nejlepší praxi v oblasti řízení kontinuity činností a podle které v následujících letech postupovalo mnoho organizací na celém světě.

V roce 2006 byla Veřejně dostupná specifikace PAS 56 stažena a nahrazena novou britskou normou pro řízení kontinuity činností BS 25999-1 (viz Box 2). V roce 2007 vydal BSI druhou část tohoto nového standardu, která poskytuje specifikaci pro formální hodnocení schopnosti organizace řídit kontinuitu svých činností. Formální audity BCMS probíhají oproti požadavkům BS 25999-2 (viz Box 2).

Aplikace PDCA na životní cyklus BCM

BOX 3



Životní cyklus BCM je reprezentován řadou kontinuálně prováděných činností, které dohromady tvoří celkový program BCM ve společnosti.

Aplikací PDCA cyklu na jednotlivé činnosti programu BCM je zajištěno postupné a trvalé zlepšování jednotlivých činností životního cyklu BCM.

Propojení BCMS na ostatní systémy řízení

Systém řízení kontinuity činností patří mezi nejnovější přírůstky systémů řízení. Společně s moderními normami o systémech řízení využívá BS 25999-2 pro plánování, zavádění a zlepšování účinnosti systému řízení kontinuity činností cyklus PDCA. Standard je úzce propojen s normami ISO/IEC 9001:2005, ISO/IEC 14001:2004 a ISO/IEC 27001:2005 tak, aby bylo podpořeno jejich konzistentní a jednotné zavedení a provoz.

Jeden vhodně navržený systém řízení tak může naplnit společné požadavky všech těchto norem (závazek vedení, řízení zdrojů, požadavky na dokumentaci, interní audity, přezkoumání vedením apod.). Ve svém důsledku tento přístup činí implementaci integrovaného systému řízení (jednotný systém řízení, který splňuje požadavky alespoň dvou systémů řízení) vysoce efektivní.

Implementace a vlastní certifikační audit

Implementační kroky životního cyklu BCM zůstávají v zásadě shodné, jak bylo popsáno v článku [1]. Jedinou výraznější změnou je přesun kroku „vytvoření a upevňování kultury BCM v organizaci“ z paprsku na obvod kola životního cyklu BCM (viz Box 3). Lépe tak symbolizuje kontinuální potřebu přenášet potřebné znalosti a informace o významu zaváděného systému na všechny zúčastněné strany, zejména pak vlastní zaměstnance.

Srdcem celého programu nadále zůstávají analytické činnosti, BIA a hodnocení rizik. Ve schématu životního cyklu jsou skryty pod implementačním krokem „porozumění činnosti organizace“ (viz Box 3). Cílem BIA je identifikovat klíčové činnosti, které umožňují organizaci plnit její program, cíle a dopad jejich narušení na organizaci a všechny zainteresované strany.

Hodnocení rizik je pak zaměřeno na identifikaci hrozeb a určení pravděpodobnosti, že způsobí následek přerušení procesu. Návrhem a implementací vhodných opatření je snížena pravděpodobnost, že daná hrozba uspěje (způsobí následek). A pokud přece jen preventivní opatření selžou, je vždy po ruce otestovaný plán, který zmírní následky havárie. Zpravidla tím, že zkrátí dobu nedostupnosti, resp. pomůže obnovit procesy s ohledem na požadavky stanovené v BIA. Takový přístup platí zrovna tak pro komerční společnost, jako pro neziskovou organizaci nebo státní správu.

Postup vedoucí k úspěšnému zavedení BCMS lze zjednodušeně shrnout následovně:

1. Získat dostatečnou podporu vlastníků a vedení společnosti.
2. Zakoupit a nastudovat doporučení BS 25999-1 a doporučení BS 25999-2.
3. Vymezit rozsah a hranice implementace BCMS, tím může být celá společnost stejně jako vybraná divize výroby.
4. Identifikovat klíčové procesy, potenciální následky a možné příčiny jejich přerušení, jinými slovy provést analýzu dopadů a hodnocení rizik.
5. Navrhnout a nechat vedení schválit cenově efektivní strategie řízení kontinuity.
6. Nastavit postupy krizové komunikace a rozpracovat schválené strategie do postupů zajištění kontinuity a obnovy přerušených procesů.
7. Nastavit cyklus pravidelného testování a aktualizace plánů, kdy pravidelným revizím podléhají také ostatní výstupy BCMS.
8. Nastavit proces monitorování, přezkoumávání a neustálého zlepšování zavedeného BCMS.
9. Podstoupit certifikační audit.

Celková doba implementace, což obnáší alespoň jeden průchod cyklem PDCA, se bude odvíjet od velikosti organizace, nastaveného rozsahu BCMS, ale také od toho, co již má organizace před začátkem projektu zavedeno (např. funkční proces řízení rizik, existující havarijní plány klíčových informačních systémů nebo systém řízené dokumentace). Každopádně se nejedná o krátkodobý proces, je potřeba počítat minimálně se 6 až 12 měsíci.

Vlastní certifikační audit probíhá obdobně jako u ostatních systémů řízení. Auditor si dopředu vyžádá dokumentaci a nezjistí-li zásadní nedostatky, je přistoupeno k auditu na místě. V případě úspěšného získání certifikátu se auditoři jednou za rok vrací na místo činu, aby potvrdili oprávněnost získaného certifikátu. Jednou za tři roky provedou detailní kontrolu při velkém recertifikačním auditu. Audity BCMS lze efektivně spojit s audity ostatních zavedených systémů řízení, jedná se pak o audit integrovaného systému řízení.

Závěr

Přestože neexistuje žádná oficiální statistika, jako je tomu např. u certifikací ISMS, uvádějí různé neoficiální zdroje až 100 certifikací BCMS po celém světě [7]. Česká republika ale na svoji první certifikaci ještě stále čeká.

Prvotní impuls získat certifikát BCMS přichází zpravidla ze strany vlastníků, zejména pokud se jedná o společnosti se zahraniční majetkovou účastí. Stále častěji se také objevuje požadavek ze strany potenciálních zákazníků (opět zejména těch ze zahraničí), kteří vyžadují určité záruky, že společnost bude schopna dostát smluveným závazkům. Z dostupných případových studií pak vyplývá i celkem zajímavá a hlavně pozitivní informace: Největším přínosem není pro certifikované organizace ani tak samotný certifikát přibitý na stěně recepce, ale to, že se v rámci revize interních procesů podařilo identifikovat klíčové produkty a služby, jejichž přerušení nebo ztráta by pro ně mohla mít fatální následky. Vypracováním odpovídajících scénářů kontinuity a obnovy jsou nyní lépe připraveny negativním událostem čelit.

Libor Široký
siroky@rac.cz

Ing. Libor Široký, CISM

Od ukončení vysokoškolského studia na Fakultě jaderné a fyzikálně inženýrské v roce 2000 pracuje jako samostatný konzultant ve společnosti Risk Analysis Consultants, spol. s r. o., kde se zabývá především oblastí business continuity managementu.

POUŽITÉ ZDROJE

[1] ŠIROKÝ L. *PAS 56 má nakročeno k normě*. DSM 1/2006, s. 10–13.
[2] BS 25999-1:2006, *Business continuity management – Part 1: Code of practice*. British Standards Institution, 2006. http://shop.bsigroup.com/en/Browse-by-Subject/Business-Continuity/.
[3] BS 25999-2:2007, *Business continuity management – Part 2: Specification*. British Standards Institution, 2007. http://shop.bsigroup.com/en/Browse-by-Subject/Business-Continuity/.
[4] SHARP J. Jak postupovat při řízení kontinuity činností (z anglického originálu The Route Map to Business Continuity Management: Meeting the requirements of BS 25999). Risk Analysis Consultants, 2009. http://www.rac.cz.
[5] GINN R. *BCM from the beginning*. Continuity Magazine May/June 2010. http://www.thebci.org/continuity.htm.
[6] *Good Practice Guidelines 2010. A Management Guide to Implementing Global Good Practice in Business Conitniuty Management.* The Business Continuity Institute 2010. http://www.thebci.org/gpg.htm.
[7] ESTALL H. Getting your house in order. Continuity Magazine January/February 2010. http://www.thebci.org/continuity.htm.