

PAS 56 má nakročeno k normě

Věřně dostupná specifikace PAS 56:2003 – Guide to Business Continuity Management (BCM) poskytuje organizacím pevné základy, na kterých lze vystavět na míru šité plány kontinuity a obnovy všech kritických činností. Na rok 2006 je plánováno vydání oficiální britské normy. PAS 56 se tak stane první britskou a s největší pravděpodobností také mezinárodní normou pro oblast business continuity managementu.

Už se stalo nepsaným pravidlem, že to nejlepší v oblasti bezpečnosti informací pochází z britských ostrovů. Nikoho tedy asi nepřekvapí, že i nová norma pro oblast řízení kontinuity činností (Business Continuity Management, BCM) má své kořeny právě zde. Je jistě pravdou, že existuje celá řada doporučení a metodik zabývajících se oblastí řízení kontinuity. Doposud však chyběl všeobecně uznávaný standard, který by vytvářel ucelenou a kompletní sbírku těch nejlepších doporučení a postupů. V praxi je pak tento stav častou příčinou toho, že vytvořené plány obsahují řadu větších či menších nedostatků. Mezi časté chyby patří například to, že se plány zabývají pouze obnovou informačních technologií po havárii, neřeší však již ztrátu celé budovy.

Plány často nezohledňují ztrátu klíčových zaměstnanců, nezmiňují nebo podceňují komunikaci s médii a orgány státní ochrany. Plány také nebývají pravidelně

aktualizovány a obsahují tak například kontaktní údaje na osoby, které již dávno v organizaci nepracují, nereflektují změny v technologiích a klíčových procesech. Nyní se zdá, že by právě veřejně dostupná specifikace PAS 56 (viz box 1) mohla tuto mezeru zaplnit a v brzké době se stát hlavním standardem odvětví.

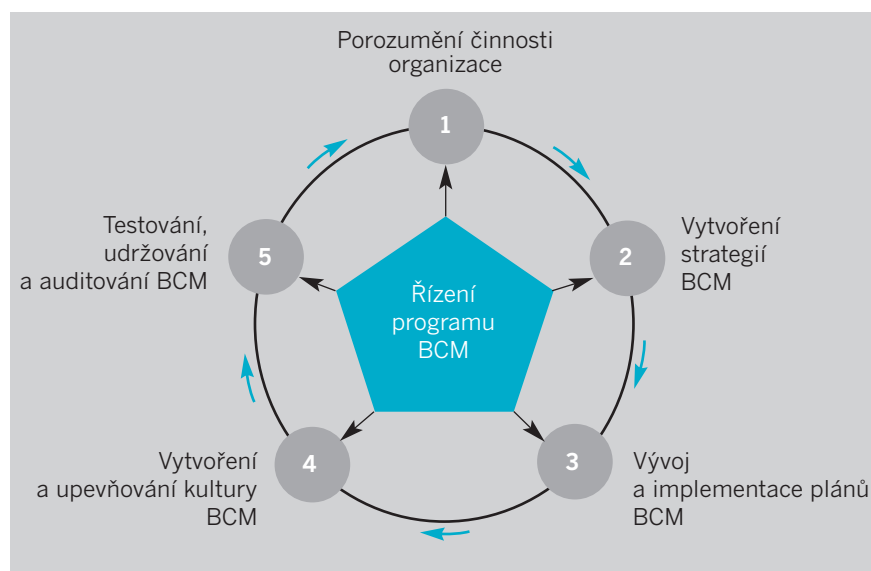
ŽIVOTNÍ CYKLUS BCM

Hlavním cílem PAS 56 je definovat proces principy a terminologii řízení kontinuity činností organizace, poskytnout

PAS 56 zdůrazňuje, že ačkoliv racionálně na sebe jednotlivé fáze navazují, v praxi nemusí být jejich pořadí a náplň striktně dodržovány. Například plány pro nejkritičtější procesy lze vytvořit nejdříve a teprve v dalším průchodu cyklem formovat plány pro méně kritické funkce. Každá z fází životního cyklu je rozdělena na samostatné etapy, které jsou podrobněji popsány dále v textu (viz také box 2).

ZAHÁJENÍ A ŘÍZENÍ PROCESU BCM

Úspěch celého procesu řízení kontinui-



OBR. 1: ŽIVOTNÍ CYKLUS BCM PODLE PAS 56.

základní rámec přípravy a reakce na incidenty a popsat techniky a kritéria pro vyhodnocení vyzrálosti a efektivity procesu řízení kontinuity činností v organizaci. PAS 56 popisuje řízení kontinuity činností organizace jako cyklický proces, který je zahájen ustavením programu řízení, na který plynule navazuje pět vzájemně propojených fází (viz obrázek 1).

ty je závislý na řadě faktorů, kde tím zdaleka nejpodstatnějším je podpora a aktivní prosazování ze strany vedení organizace. Viditelný závazek demonstrováný vydáním politiky BCM a další angažovanost vedoucích pracovníků jsou jasným signálem směřujícím k zaměstnancům, investorům a třetím stranám, zdůrazňujícím význam řízení kontinuity činností v organizaci. Podle PAS 56 by

PAS (PUBLICLY AVAILABLE SPECIFICATION) 56

V rámci britského systému normalizace je veřejně dostupná specifikace považována za předchůdce oficiální normy. Oproštěna od zdlouhavého procesu normalizace poskytuje PAS v relativně krátkém čase potřebné kvalitní informace a kvalifikovaná doporučení v daném oboru. Historie této veřejně dostupné specifikace se začala psát v březnu roku 2003. PAS 56 byla připravena a vydána britským normalizačním institutem, British Standards Institute (BSI), ve spolupráci s Business Continuity Institute (BCI) a za sponzorského přispění řady dalších britských organizací. Jejím základem se stala sada vybraných praktik a doporučení pro oblast řízení kontinuity činností organizace, Good Practice Guidelines, sestavená a vydaná BCI v roce 2002.

Box 1

ŘÍZENÍ PROGRAMU BCM

- Vytvoření politiky BCM
- Nastavení řídicího procesu
- Ověření stavu BCM

POROZUMĚNÍ ČINNOSTI ORGANIZACE

- Identifikace strategických cílů organizace
- Provedení analýzy dopadů (BIA)
- Hodnocení rizik

VYTVOŘENÍ STRATEGIÍ BCM

- Nastavení celkové strategie organizace
- Strategie obnovy procesů a činností
- Strategie obnovy zdrojů

VÝVOJ A IMPLEMENTACE PLÁNŮ BCM

- Plán krizového řízení

- Plán kontinuity činností
- Plán obnovy zdrojů

VYTVOŘENÍ A UPEVNĚNÍ KULTURY BCM

- Hodnocení stávajícího povědomí, identifikace slabých míst
- Školení a programy zvyšování povědomí
- Přezkoumání stavu

TESTOVÁNÍ, UDRŽOVÁNÍ A AUDITOVÁNÍ BCM

- Testování strategie, plánů a rolí
- Aktualizace programu a náprava slabých míst programu
- Audit programu

Box 2

zodpovědnost za kompletní proces řízení kontinuity činností měla být svěřena některému členu vedení organizace. Je potřeba, aby byli včas jmenováni zaměstnanci a to do přesně definovaných a popsáných rolí, stanoveny jejich odpovědnosti, povinnosti a kompetence v rámci celého procesu. Toho lze například dosáhnout zavedením a používáním matice odpovědností RACI¹ (delegovaná odpovědnost/hlavní odpovědnost/spolupracuje/informovaný) pro každou roli nebo funkci.

PAS 56 přináší koncept měření vytrvalosti (připravenosti organizace na krizovou událost) procesu řízení kontinuity činností, který je založený na rozsáhlém souboru hodnotících kritérií. Podle těchto kritérií je možné kontinuálně monitorovat, vyhodnocovat a ověřovat stav zavedení programu BCM a verifikovat výstupy z jednotlivých fází jeho životního cyklu. Kritéria mohou být použita buď jako součást sebehodnotícího procesu nebo auditorem v rámci oficiálního auditu.

POROZUMĚNÍ ČINNOSTI ORGANIZACE

Tento kritický krok celého procesu řízení kontinuity činností doporučuje PAS 56 rozdělit do tří úzce propojených etap:

- identifikace kritických činností organizace;

- analýzy dopadů;
- hodnocení rizik.

Nejprve je nutné porozumět tomu, jaké vlastně jsou klíčové cíle organizace, jak budou tyto cíle dosaženy, jaké produkty a služby jsou důležité z hlediska dosažení stanovených cílů, v jakém časovém horizontu je nutné těchto cílů dosáhnout a koho je potřeba do realizace těchto cílů zapojit. Kromě identifikace kritických činností organizace je také důležité identifikovat zdroje jejich možného selhání.

Analýza dopadů označuje a hodnotí dopady narušení, přerušení a nebo ztráty kritických činností organizace a minimální úroveň zdrojů potřebných pro určení vhodné strategie jejich obnovy. Vymezuje přijatelný časový úsek, ve kterém je nutné obnovit kritické a jiné související činnosti, včetně jejich obnovy na předem stanovenou úroveň funkčnosti. PAS 56 zdůrazňuje potřebu analyzovat poskytované služby a produkty jako celek a ne jako jednotlivé samostatné komponenty.

Cílem hodnocení rizik je nalézt a ohodnotit rizika, která ohrožují kritické činnosti organizace. Spolu se závěry z analýzy dopadů umožňuje stanovit akceptovatelnou úroveň rizika a sestavit plán opatření, kterými lze tato rizika ošetřit.

Strategie řízení kontinuity činností organizace

PAS 56 definuje vytváření strategie řízení kontinuity jako určování a výběr alternativních metod, jejichž použitím budou po incidentu obnoveny kritické činnosti a procesy organizace na minimální přijatelné úrovni. Při vývoji strategie rozlišuje tři úrovně strategického plánování:

- celkovou strategii organizace;
- strategii obnovy kritických činností;
- strategii zajištění zdrojů potřebných pro realizaci plánů kontinuity a obnovy.

Pro zajištění obnovy jednotlivých kritických činností v požadovaném čase uvažuje čtyři základní strategické modely (viz box 3). Při výběru té nevhodnější strategie jsou klíčové závěry z provedené analýzy dopadů, zejména tedy maximální přijatelná doba nedostupnosti jednotlivých procesů.

VÝVOJ A IMPLEMENTACE PLÁNŮ OBNOVY FUNKČNOSTI

PAS 56 doporučuje organizovat plány s ohledem na tři základní fáze každého incidentu:

- krizové řízení;
- zajištění kontinuity činností;
- zajištění obnovy činností.

Cílem jednotlivých plánů je identifikovat činnosti a zdroje potřebné pro hladké zvládnutí nastalých krizových situací. Zatímco malé organizace vystačí s jedním plánem, větší budou mít zpravidla více samostatných dokumentů. Informace, které jsou často aktualizovány, jako například kontaktní údaje, by měly být uvedeny v samostatných přílohách. Ze stejných důvodů se také doporučuje namísto

¹ RACI (responsible / accountable / consulted / informed).

AKTIVNÍ/ZÁLOŽNÍ MODEL

Mimo "aktivní" provozní lokality existuje odpovídající záložní lokalita pro provoz kritických činností organizace (model je založen na přesunutí personálu z aktivního na záložní místo, kde je zapotřebí, aby byly k dispozici udržované a aktuální systémy a zálohy dat).

AKTIVNÍ/AKTIVNÍ MODEL (ROZDĚLENÝ PROVOZ)

Model je založen na existenci dvou geograficky dostatečně vzdálených „aktivních“ provozních lokalitách ve kterých jsou umístěny kritické činnosti organizace. Tyto lokality jsou si vzájemně zálohou a je mezi ně rozdělena pracovní zátěž. Obě místa by měla mít takovou

kapacitu, aby zvládla celou pracovní zátěž, pokud to bude potřeba.

MODEL ALTERNATIVNÍ LOKALITY

Vedle "aktivní" provozní nebo produkční lokality existuje odpovídající záložní lokalita, která pravidelně funguje jako primární místo (jednou za čas je sem přesunuta provozní/produkční činnost).

MODEL NOUZOVÉHO ŘEŠENÍ

Model je založen na existenci alternativních způsobů výroby produktů nebo nabízených služeb při ztrátě běžných provozních procesů nebo komponent (např. ztráta systémového nebo produkčního vybavení může znamenat návrat se k manuálním metodám).

Box 3

TESTY ÚPLNÉHO PŘERUŠENÍ

Nejobtížnější test, při kterém se simuluje úplné zničení lokality organizace s následným obnovením funkčnosti systémů a procesů v záložních prostorech a s využitím pouze zde umístěných zdrojů. Tento typ testů se nedoporučuje u velkých organizací, mohly by být příčinou vzniku krizové situace.

PARALELNÍ TESTY

Přesunutí jednoho nebo více vybraných kritických procesů organizace do záložní lokality a jejich kompletní obnova v požadovaném čase. Tyto testy jsou technicky zaměřené a jejich hlavním cílem je ověření schopnosti organizace pokračovat v činnosti v případě vzniku krizové události.

SIMULAČNÍ TESTY

Praktické nácviky a prověřování jednotlivých postupů a týmové interakce podle předem připravených scénářů. Součástí testů je ověření funkčnosti komunikačních linek, otestování komunikace s dodavateli, zákazníky, médií a záchrannými složkami. Příkladem simulačních testů může být např. nácvik evakuace budovy nebo fiktivní požár serverovny.

TEORETICKÝ PRŮCHOD PLÁNEM

Kontrola úplnosti plánů rozšířená o teoretické prověření konkrétních postupů obnovy, ověření znalostí rolí jednotlivých členů týmu a jejich vzájemné komunikace (vysvětlují co by v dané situaci dělali, jak by postupovali, koho kontaktovali, atd.). Cílem testů je odhalit nedostatky v navržených postupech obnovy jednotlivých procesů. Může to být také dobrý způsob, jak zaškolit nové členy týmu.

KONTROLA ÚPLNOSTI PLÁNŮ

Nejjednodušší typ testů, zahrnuje teoretické přezkoumání kompletnosti informací obsažených v plánech, provádí se ověření správnosti, úplnosti a aktuálnosti uvedených údajů, jako jsou např. kontaktní informace na členy týmu, umístění záložních prostor a seznam technických prostředků.

Náročnost testů

Frekvence testů

PAS 56 popisuje plán kontinuity činností jako milník celého procesu řízení kontinuity. Plán pokrývá aktivity potřebné pro zajištění kontinuity kritických činností organizace v průběhu narušení či přerušení běžného provozu. Plán by měl poskytnout základní rámec a postupy reakce na nastalý incident, který ovlivňuje jednu nebo více kritických činností organizace. Měl by poskytnout postupy pro minimalizaci dopadů a obnovení činností na předem stanovenou úroveň a v požadovaném čase. V neposlední řadě kvalitní plán také zaručuje ochranu obchodní značky, dobré pověsti a důvěry všech vlastníků, akcionářů a ostatních zainteresovaných stran.

Plán kontinuity činností definuje role a odpovědnosti a identifikuje kritické aplikace, operační systémy, personál, vybavení, hardware a časové harmonogramy jejich obnovy tak, jak bylo určeno v rámci analýzy dopadů. Jeden plán kontinuity činností se zpravidla odkazuje na řadu samostatných plánů pro obnovu zdrojů.

Plány obnovy zdrojů jsou technicky zaměřené a cílené na navrácení či obnovení provozu, IT služeb, lokalit, zařízení a další potřebné infrastruktury po skončení krizové události. Plán by měl poskytnout efektivní a na míru šité řešení obnovy zdrojů potřebných pro požadovanou funkčnost kritických činností organizace.

VYTVOŘENÍ A UPEVŇOVÁNÍ „KULTURY ŘÍZENÍ KONTINUITY“ ČINNOSTÍ V ORGANIZACI

Důležitým prvkem řízení kontinuity činností je také vytvoření a neustálé posilování obecného povědomí o důležitosti a celkovém významu řízení kontinuity a ustanovení základní kultury organizace v této oblasti. PAS 56 zdůrazňuje, že budování, všteňování a upevňování kultury řízení kontinuity je zdlouhavým procesem, který se může setkat s určitým odmítnutím.

Na podporu změny firemní kultury by neměla být podceněna kvalitní příprava a samotná realizace programů školení

OBR. 2: TYPY A METODY TESTOVÁNÍ PLÁNŮ PODLE PAS 56.

jmen uvádět přednostně označení funkcí jednotlivých účastníků plánu. Každý plán by měl jasně specifikovat podmínky své aktivace, a stejně tak určit osoby s odpovědností za vykonávání každého bodu plánu.

Plán krizového řízení se zaměřuje na okamžitou reakci na vzniklý incident bez

ohledu na jeho příčinu. Efektivní řízení vyžaduje silné vedení a dobrou koordinaci mezi jednotlivými účastníky plánu. Účinné a včasné vyhodnocení nastalých krizových situací a jejich úspěšné zvládnutí jsou kritické faktory, které omezují dopad incidentu a zajišťují ochranu organizace před velkou finanční ztrátou.

a zvyšování znalostí všech zainteresovaných pracovníků. Vzdělávací aktivity a aktivity směřující ke zlepšení povědomí by pro zajištění svého efektivního průběhu měly být zaměřeny na pochopení procesů plánování kontinuity.

V tomto ohledu je v významná aktivní podpora ze strany vedoucích zaměstnanců a nepodcenění komunikace se všemi externími subjekty a to zejména tam, kde jsou služby poskytovány formou outsourcingu.

Testování, aktualizace, změny a audit Nejdůležitější, ale také zdaleka nejobtížnější částí celého programu řízení kontinuity, je testování navržených plánů a jejich pravidelná aktualizace.

Teprve samotné testování prokáže, zda jsou navržené postupy dostatečně, ale také srozumitelně popsány a v praxi proveditelné. Aby se prokázala vyspělost a vytrvalost celého procesu řízení kontinuity, mělo by testování zahrnovat strategii řízení kontinuity činností, plány obnovy funkčnosti, nácvik rolí členů týmu a ostatního personálu a testování IT systémů organizace.

V minulosti byl kladen přehnaný důraz na testování obnovy IT systémů a tento omezený přístup v řadě organizací dodnes přetrvává. PAS 56 však zdůrazňuje, že klíčovým prvkem každého plánu jsou právě lidé, účastníci plánu, jejichž zkušenosti, znalosti, dovednosti a schopnost se správně rozhodnout. Silné stránky jednotlivců by měly být oceňovány a zjištěné slabiny brány spíše jako prostor pro zlepšení než pro kritiku. Dokument rozlišuje několik typů testů (viz obr. 2), od prvotní kontroly obsahu plánů přes teoretické ověření navržených postupů až po funkční testy, kdy je simulována reálná krizová událost.

Aby plány neustále odrážely změny uvnitř i vně organizace, by měly být zavedeny postupy jejich aktualizace a při vzniku nových požadavků by měly být adekvátním způsobem doplněny. Revize postupů by měla být začleněna do programu řízení změn v organizaci, aby bylo garantováno, že problematika kontinuity činností je vždy náležitě zajištěna.

Tyto postupy by měly být schváleny a podporovány ze strany vedení organizace. Proces aktualizace by neměl být omezen pouze na samotné plány. PAS 56 zdůrazňuje potřebu pravidelného přezkoumávání závěrů z hodnocení rizik a analýzy dopadů.

Proces auditu má za úkol nezávisle ověřit soulad s politikou řízení kontinuity činností, strategiemi a osvědčenými zkušenostmi (best practices) nebo standardy, které si organizace osvojila. Audit by měl podrobně prozkoumat úroveň a vytrvalost celého procesu řízení kontinuity činností organizace. Měl by nezávisle ověřit klíčové dokumenty a postupy poukázat na nedostatky, které v nich identifikuje a následně zajistit jejich odstranění.

Budoucí vývoj PAS 56

Přes její nesporné přínosy lze ve stávající verzi této specifikace nalézt řadu oblastí, které vyžadují přepracování předtím, než se PAS 56 stane obecně přijímaným a uznávaným standardem. PAS 56 je sice určen pro všechny organizace bez ohledu na jejich velikost a obor podnikání, měl by však brát více v potaz rozdílné potřeby malých a velkých organizací.

Doporučení vhodná pro velkou korporaci nemusejí být vhodným řešením pro organizaci malou. Obdobně doporučení pro organizace finančního sektoru ne-

musejí být stejně relevantní pro společnost vyrábějící potraviny. Je jasné, že vytvoření jednotného rámce pro řízení kontinuity, který by byl vhodný pro všechny typy organizací, je velice těžký úkol. Budoucí standard by však měl být natolik flexibilním, aby umožňoval případnou certifikaci organizací všech velikostí a oborů podnikání.

V srpnu letošního roku byla ustavena technická komise, která by měla na základě PAS 56 v následujících několika měsících připravit finální návrh nové normy. Tento návrh bude podroben veřejné diskuzi a po zpracování všech relevantních připomínek bude, s největší pravděpodobností v průběhu roku 2006, vydán pod hlavičkou BSI jako plnohodnotná britská norma. Všeobecně se očekává její následné přijetí jako normy mezinárodní, podobně jako tomu bylo například v případě BS 7799.

LIBOR ŠIROKÝ
siroky@rac.cz



ING. LIBOR ŠIROKÝ

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.

MANAGEMENT SUMMARY

PAS 56:2003 – Guide to business continuity management sjednocuje proces, principy a terminologii business continuity managementu, popisuje obsah a výstupy jednotlivých etap zavádění BCM a související aktivity. PAS 56 poskytuje doporučení pro dobré manažerské praktiky a nastiňuje kritéria pro vyhodnocování zavedených procesů. Cílem článku je seznámit čtenáře s touto britskou specifikací, která se již v příštím roce stane britskou normou a následně s největší pravděpodobností také normou mezinárodní.

LITERATURA:

- [1] PAS 56:2003 Guide to Business Continuity Management, British Standards Institution, 2003
- [2] SMITH, D. J., ed. Business continuity management: Good practice guidelines. Worcester: The Business Continuity Institute, 2002
- [3] BS ISO/IEC 17799:2005 Information Technology – Security techniques – Code of practice for information security management, British Standards Institution, 2005