

# Role ICT při zvyšování konkurenceschopnosti firem a státu

na pražském Žofíně

## 7 nejčastějších chyb a jejich řešení při vazbě mezi BCM a ITSCM

Vladimír Kufner

ITSM & PPM senior consultant, HP SW Professional Service Organization

6.6.2011

# Agenda

- Definice klíčových termínů – Wikipedia, ITIL
- Národní a mezinárodní normy a regulativy
- Trendy v oblasti BC/DR
- Nejčastější chyby v oblasti BC/DR
- Osobní doporučení
- Otázky a odpovědi



# Definice klíčových termínů



# Definice Wikipedia



WIKIPEDIA  
The Free Encyclopedia

## – Disaster Recovery/DR

- proces, politiky a procedury, které se vztahují k přípravě obnovy nebo zajištění kontinuity technické infrastruktury kritické pro organizaci po přírodních či lidmi zapříčiněných katastrofách. DR je podmnožinou business continuity/BC

## – Business Continuity/BC

- aktivita, pomocí které organizace zajišťuje, že kritické podnikové funkce (funkce businessu) budou dostupné zákazníkům, dodavatelům, regulátorům a dalším stranám, které mají mít k těmto funkcím přístup

## – Enterprise Risk Management/ERM

- Obecná (nikoliv pouze IT) disciplína, při které organizace v různých sektorech průmyslu provádějí počáteční odhad (assessment) rizik;
- tato rizika pocházející z různých zdrojů (resp. opatření na jejich eliminaci a nebo omezení) dále organizace řídí, využívá, financuje a monitoruje za účelem zvyšování krátkodobé a dlouhodobé hodnoty podniku vůči svým akcionářům, veřejnosti a dalším zúčastněným stranám

# Definice ITIL



## – IT Service Continuity Management/ITSCM

- Proces odpovídající za správu rizik, která by mohla vážně ohrozit služby IT. ITSCM zajišťuje, aby poskytovatel služeb IT mohl vždy poskytnout minimální dohodnutou úroveň služeb, přičemž omezuje rizika na akceptovatelnou úroveň a plánuje obnovu služeb IT. ITSCM by měl být navržena tak, aby podporoval Správu kontinuity businessu.

## – Business Continuity Management/BCM

- Podnikový proces zodpovědný za správu rizik, která mohou mít závažný dopad na business. BCM ochraňuje zájmy klíčových zainteresovaných stran, reputaci, značku a aktivity vytvářející hodnoty. Proces BCM zahrnuje redukci rizik na akceptovatelnou úroveň a plánování obnovy podnikových procesů, objeví-li se narušení businessu. BCM stanoví cíle, rozsah a požadavky pro Správu kontinuity služeb IT.

## – Vysoká dostupnost (High Availability/HA)

- Přístup nebo návrh, který minimalizuje nebo potlačuje důsledky poruchy komponenty infrastruktury (konfigurační položky) na uživatele služby IT

## – Availability Management/AvM

- proces, odpovědný za definování, analýzu, plánování, měření a zlepšování všech aspektů dostupnosti služeb IT

## – Capacity Management/CaM

- Proces, odpovědný za to, že kapacita služeb IT a infrastruktura IT jsou schopny dodat služby na dohodnuté úrovni, za přiměřených nákladů a včas

## – Business Impact Analysis/BIA

- činnost či metoda používaná v rámci BCM, která identifikuje vitální (nezbytné) funkce businessu a jejich závislosti. Tyto závislosti mohou zahrnovat dodavatele, personál, další podnikové procesy, služby IT atd

## – CCTA Risk Analysis and Management Method (CRAMM)

- metoda (a také SW), který umožňuje identifikaci aktiv (Assets), registraci možných ohrožení (Threats), definici zranitelností (Vulnerabilities) a vyčíslení reálných rizik (Risks)

# CRAMM (CCTA Risk Assessment Management Methodology)

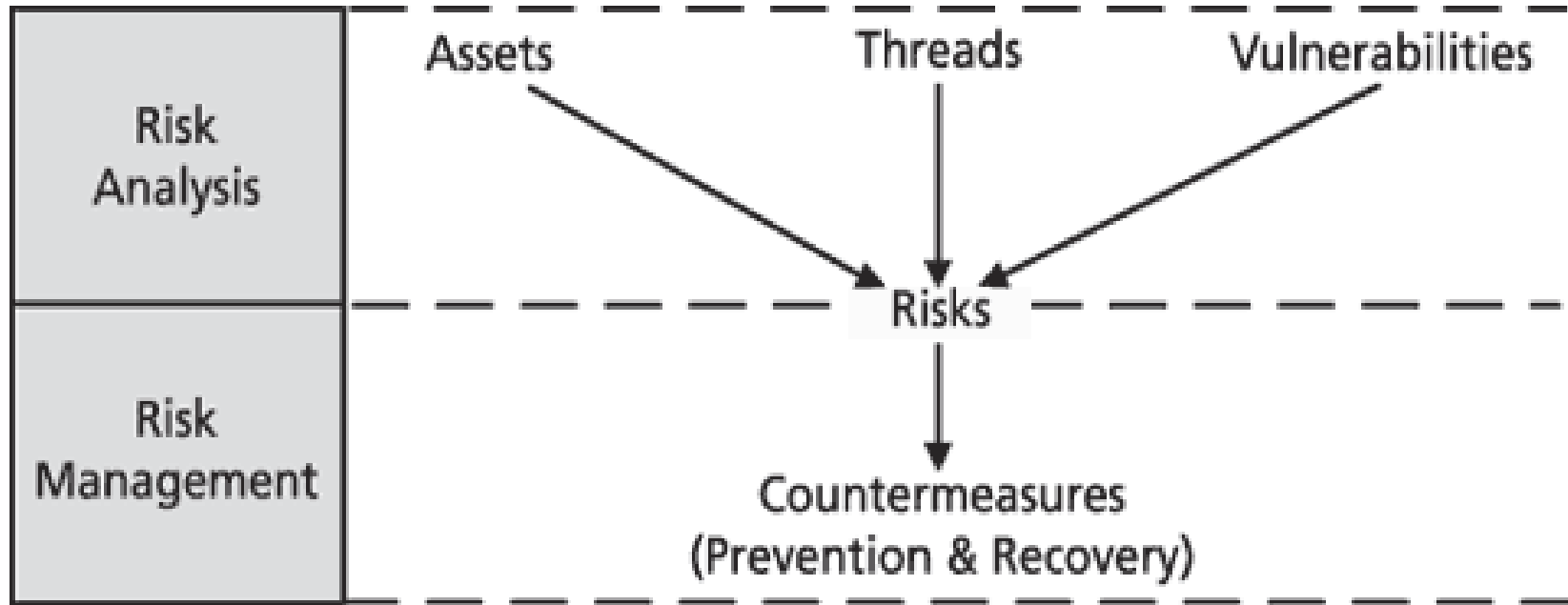


Figure 13.2 The CCTA Risk Assessment Model (source: OGC)

# Jaký je rozdíl mezi BIA, DR/ITSM a ERM?

- BIA se koncentruje na zjištění dopadu , identifikace vitálních podnikových funkcí a definuje požadavky na obnovu služeb; část procesu BC
- DR/ITSCM je procesní přístup umožňující řešení havárií služeb v oblasti ICT v případě katastrof a živelných událostí
- ERM je obecná podniková disciplína zaměřená na identifikaci, klasifikaci a plánování opatření za účelem buďto úplné eliminace těchto rizik nebo jejich snížení; z tohoto pohledu je DR sub-elementem ERM

# Mezinárodní normy a další legislativa



# Mezinárodní normy, legislativa a další rámce

## – Regulativy

- FSA (UK)
- HB221 a APS 232 (AU)
- NFPA 1600 (USA, Kanada)

## – Pravidla u finančních institucí

- Např. Basel II a připravovaný Basel III
- NYSE Rule 4370

## – Národní normy

- BS 25777 (PAS 57) IT Service Continuity Management
- BS 25999 (PAS 56) Business Continuity Management. Code of Practice & Specification
- AS/NZS 5050:2010 Business continuity - Managing disruption-related risk

## – Normy ISO

- ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management
- ISO/IEC 24762:2008 . Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services
- ISO 31000:2009 (AS/NZS 4360 Standard in Risk Management)



# Trendy v oblasti DR/BC

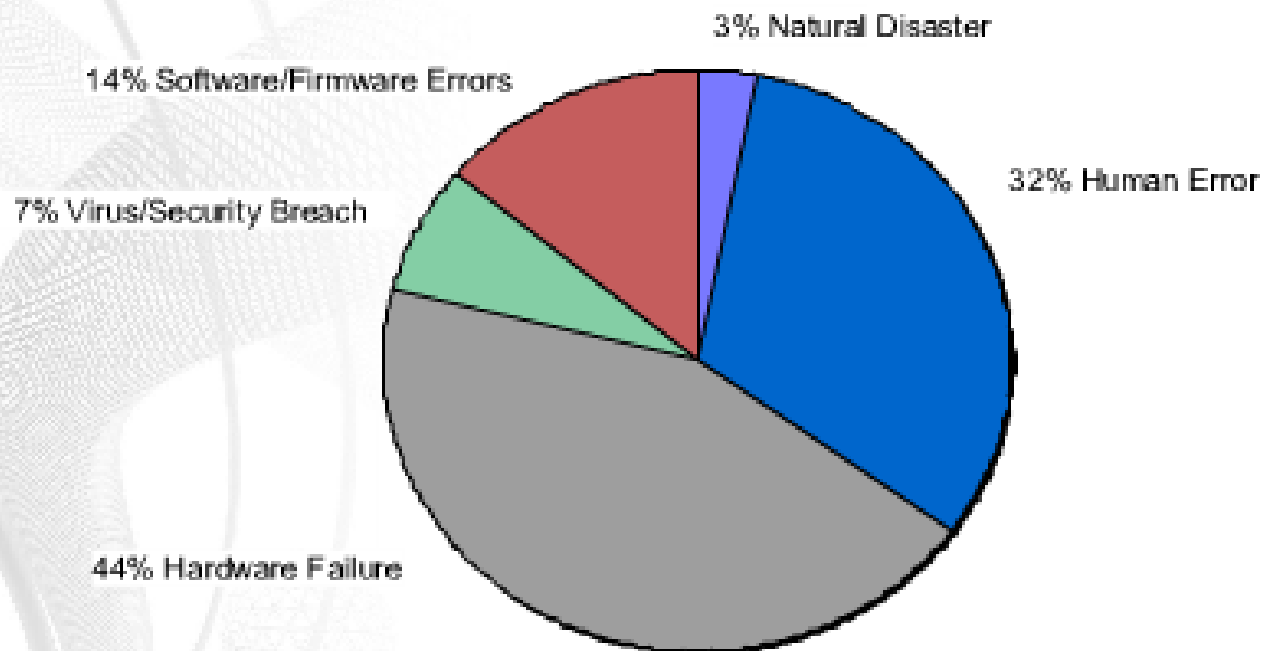


# Trendy v oblasti DR/BC

- Enormně se zvyšuje se počet regulativních standardů
- IT Governance
- Outsourcing – nový model poskytování služeb, bezpečnostní rizika
- Nové technologie
  - Přejechod na mirroring a replikace dat
  - Portabilní komunikace v různých podobách
  - Virtualizace
  - Cloud computing (SaaS, PaaS, IaaS atd.)
  - Automatické testování DR
  - Specializované programy (SW) na BC/DR

# Procentuelní příčiny událostí

## Leading causes of BCDR disruptions, by percentage



Zdroj: IDC report 2007

# Nejčastější chyby v oblasti DR/BC

# Nejčastější chyby v oblasti DR/BC

- Seriozní business case a financování
- Chybějící podpora businessu
- DR není záležitost jen IT
- Nejasná priorita služeb a pořadí jejich obnovy
- Neseříózní testování DR
- Nejasné nebo neurčené pravomoci
- Podcenění informování zaměstnanců
- Pořizování levného, nekvalitního HW

# Osobní doporučení v oblasti DR/BC



# Osobní doporučení v oblasti BC/DR

- Ujasněte si reálné potřeby businessu v případě mimořádné události
- Proveďte nejen BIA ale také regulérní analýzu rizik
- Spočítejte si business case a na jeho základě si vyčleňte si na BC/DR rozumné finance
- Ujasněte si procentuální příčiny havárií
- I když vaše firma neprovádí BC, buďte v IT připraveni provádět DR
- Udržujte plány pro BC/DR aktuální
- Určete odpovědnosti až na úroveň jednotlivých osob a zajistěte krizovou komunikaci
- Předpokládejte spíše to nejhorší, nikoliv to nejlepší
- Testování

**Budte připraveni na to, že implementace opatření v oblasti BC/DR je drahá**

# Závěr

- "Nemůžeme **řešit** problémy stejným způsobem **myšlení** který jsme použili, když jsme tyto problémy **vytvořili.**"

• Albert Einstein

- "Při přípravě na válku jsem si vždy ověřil, že **plány** jsou **zbytečné**, ale plánování je **nezbytností.**"

• Dwight D Eisenhower

- Pokud plánujete na rok, pěstujte obilí. Pokud plánujete pro dekádu, pěstujte stromy. Pokud plánujete pro celý život, školte a vychovávejte **lidi.**

• Čínské přísloví

# Otázky a odpovědi

Vladimir.kufner@hp.com

