Standardy/praktiky pro řízení služeb informační bezpečnosti

Doc. Ing. Vlasta Svatá, CSc.
Vysoká škola ekonomická
Praha

Služby informační bezpečnosti

- Nemožnost oddělit informační bezpečnost od IT služeb – součást všech IT služeb
- Specifický druh IT služeb – úrovně:
  - Operativní –security services (zálohování, archivace)
  - Taktická – security management (např. BCP)
  - Strategická (Security Governance, plán, zavedení ISMS - metriky)
- Možnost insourcing-outsourcing
- Outsourcing – nutnost integrovat dva ISMS, SLA

PROBLÉMY

ŘEŠENÍ

- Standardy/praktiky pro ISM:
  - ITIL V3—OGC, nejlepší praktika pro ITSM — JAK?
  - Cobit 4.1—ITGI, základní rámec pro IT Governance,
  - ISO/IEC 27002:2005—zavádění ISMS

CO?

ITIL V3

- **Knihy**:
  - Strategie služeb (Service Strategy)
  - Návrh služeb (Service Design)
  - Implementace služeb (Service Transition)
  - Provoz služeb (Service Operation)
  - Průběžné zlepšování služeb (Continual Service Improvement)
- **Informační bezpečnost**:
  - každý proces (např. v procesu Supplier Management (Service Design) popis náležitostí kontraktu na dodávku služeb: definování bezpečnostních požadavků a požadavků na kontinuitu služeb),
  - Kniha Service Design - proces Information Security Management (ISM)

Kniha Návrh služeb: proces ISM (1)

- Propojení dalších procesů návrhu služeb:
  - Řízení katalogu služeb (Service Catalog Management)
  - Řízení úrovní služeb (Service Level Management)
  - Řízení dostupnosti (Availability Management)
  - Řízení kapacity (Capacity Management)
  - Řízení kontinuity služeb IT (IT Service Continuity Management)
  - Řízení dodavatelů (Supplier Management)

Kniha Návrh služeb: proces ISM (2)

- **Subprocesy:**
  - **Návrh bezpečnostních kontrol:** návrh vhodných technických a organizačních kontrol důvěrnosti, integrity a dostupnosti aktiv, informací, dat a služeb organizací
  - **Testování bezpečnosti:** pravidelné testování zavedených kontrol a jeho reporting
  - **Řízení bezpečnostních incidentů**
    - **preventivní kontroly:** (např. kontrola přístupových práv)
    - **reduktivní kontroly:** proaktivní minimalizace škod (např. pravidelné denní zálohy, testování plánů obnovy)
    - **detekční kontroly**: identifikace incidentů (např. monitorování sítě)
    - **represivní kontroly:** zabraňují opakování nebo pokračování incidentů (např. zablokování systému při nesprávném heslu nebo PIN),
    - **korektivní kontroly:** náprava škod způsobených bezpečnostním incidentem (např. obnova systému ze zálohy),
  - **Hodnocení bezpečnosti**: zhodnocení stavu informační bezpečnosti vzhledem k měnícím se podnikatelským rizikům

COBIT 4.1

- Control Objectives for IT and Related Technologies- definuje množinu cílů řízení (Control Objectives) pro oblast IT
- **Sada dokumentů**
  - Framework, Control Objectives, Management Guidelines a Maturity Models
  - 34 procesů, 4 domény: Plánování a organizace, Pořízení a implementace, Dodávka a podpora a Monitorování a hodnocení, 214 control objectives
- **Informační bezpečnost**:
  - součástí téměř každého definovaného procesu (např. v procesu PO4 Definice IT procesů, jejich organizace a vazeb ve formě kontrolního cíle PO4.8: Odpovědnost za rizika, bezpečnost a soulad se standardy,
  - samostatný proces domény Dodávka a podpora DS5: Zajištění bezpečnosti systémů
  - příručka Cobit Security Baseline
  - Mimo Cobit:
    - Information Security Governance: Guidance for Information Security Managers
    - Enterprise Risk: Identify, Govern and Manage IT Risk

DS5 – Zajištění bezpečnosti systémů

- obecný popis procesu včetně zdůraznění vazby na cíle IT Governance - Řízení rizika,
- přehled cílů řízení tohoto procesu:
  - DS5.1 – Řízení informační bezpečnosti
  - DS5.2 – Plánování informační bezpečnosti
  - DS5.3 – Řízení autentizace a autorizace
  - DS5.4 – Řízení uživatelských účtů
  - DS5.5 – Testování, dohled a monitorování bezpečnosti
  - DS5.6 – Definování bezpečnostních incidentů
  - DS5.7 – Ochrana bezpečnostních technologií
  - DS5.8 – Správa kryptografických klíčů
  - DS5.9 – Prevence, detekce a korekce škodlivých programů
  - DS5.10 – Bezpečnost sítí
  - DS5.11 – Výměna citlivých dat
- přehled potřebných vstupních dat z jiných procesů
- přehled výstupů, které tento proces poskytuje jiným procesům
- přehled aktivit procesu a odpovědností za ně podle liniových rolí ve firmě
  - např. za činnost: pravidelná kontrola a hodnocení uživatelských práv by měl být odpovědný vlastník business procesu, který může tuto odpovědnost delegovat na roli odpovědnou za audit nebo řízení rizika a bezpečnosti, CIO by měl být o této aktivitě informován a vedoucí provozu konzultován
- přehled cílů a metrik; tři úrovně cílů (IT, procesní a aktivit) a dva druhy metrik (outcome measures – metriky výstupu a performance indicators – metriky realizace)
- modely zralosti procesu - CMM

IT CÍLE např. Zajistit integritu informací a infrastruktury	CÍLE PROCESŮ např. Umožnit přístup ke kritickým a citlivým údajům pouze autorizovaným uživatelům	CÍLE AKTIVIT např. Definovat bezpečnostní incidenty
• Počet incidentů s dopadem na podnikové procesy • Počet systémů, u kterých se nedodržují požadavky bezpečnosti • Čas potřebný pro udělení, změnu a odebrání uživatelských práv	• Počet a druh očekávaných a skutečných narušení přístupu • Počet porušení zásady oddělení odpovědností • Procento uživatelů, kteří nedodržují standardy hesel • Počet a druh odstraněných škodlivých kódů	• Frekvence a počet monitorovaných bezpečnostních událostí • Počet a druh zastaralých účtů • Počet neautorizovaných IP adres, portů a výpadků provozu • Procento prozrazených kryptografických klíčů • Počet přidělených, změněných nebo zrušených přístupových práv

CobiT Security Baseline

Sada pro přežití - Information Security Survival Kit

- **Rozdíl proti Cobit 4.1**
  - Cobit: bezpečnost jako jedno z mnoha rizik spojených s používáním IT
  - Cobit Security Baseline: rizika specifická pro informační bezpečnost,různí uživatelé
- **Obsah**:
  - 20 bezpečnostních procesů, které jsou provázány na domény Cobit 4.1
    - 44 kontrolních kroků, vazby na obsah ISO/IEC 27002 a procesy Cobit 4.1
  - „sady pro přežití": domácí uživatelé, profesionální uživatelé, manažeři, výkonní ředitelé, vyšší výkonní ředitelé a členové představenstva
  - Pro každou tuto skupinu uživatelů příručka nabízí
    - Přehled rizik spojených s danou skupinou uživatelů
    - Dotazník, který má pomoci dané skupině uživatelů zhodnotit, zda dodržují pravidla ISG
    - Seznam akcí, které by měli realizovat
  - Závěr: bezpečnostní rizika - tři kategorie:
    - Rizika záměrného zneužití počítače (trojský kůň, DOS, Email spoofing, spamming atd.)
    - Rizika plynoucí z porušení pravidel, norem (porušení autorského práva, nepřiměřené využívání internetu, průmyslová špionáž, nesoulad s pravidly a regulacemi)
    - Havárie (porucha disku, porucha dodávky elektřiny, problémy softwaru).

ISO/IEC 27002:2005

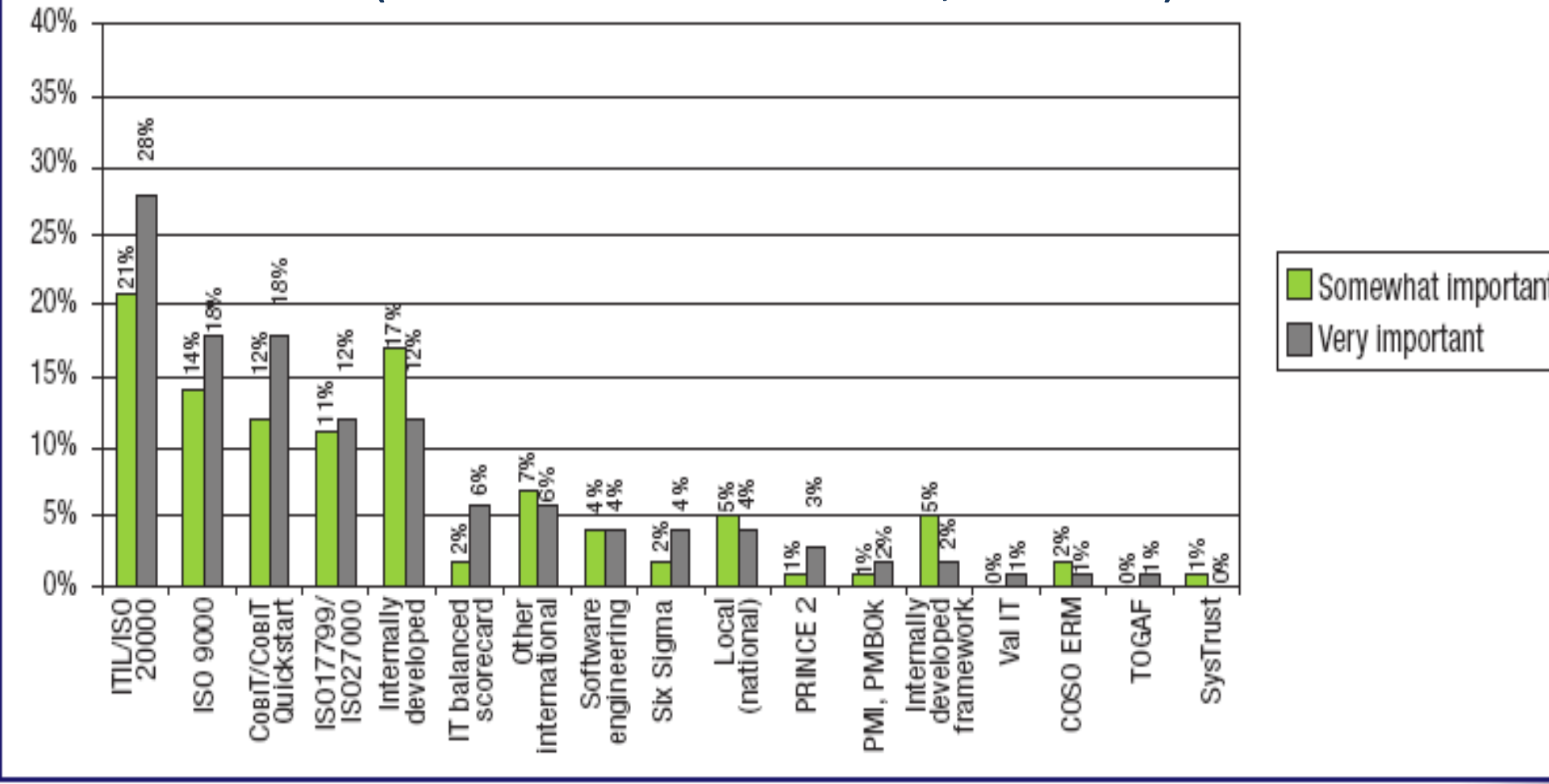
Soubor postupů pro management bezpečnosti informací

- ucelená vyvážená soustava opatření pro ochranu informačních aktiv
- 11 oblastí, každá oblast dále obsahuje tzv. cíle opatření (celkem 39) a opatření (133)
- **Oblasti ISMS** :
  - Bezpečnostní politika
  - Organizace bezpečnosti
  - Klasifikace a řízení aktiv
  - Bezpečnost lidských zdrojů
  - Fyzická bezpečnost a bezpečnost prostředí
  - Řízení komunikací a provozu
  - Řízení přístupu
  - Akvizice, vývoj a údržba IS
  - Zvládání bezpečnostních incidentů
  - Řízení kontinuity činností organizace
  - Soulad s požadavky

	Forma	Způsob vnímání inf. bezpečnosti	Velikost organizace	Primárně určena pro	Možnost certifika-ce procesů	Možnosti zavádění
ITIL	Nejlepší praxe	Jako součást řízení IT služeb	Velká, střední	IT specialisty	ANO ISO/IEC 20000	Interně Externě
COBIT	Rámec/ nejlepší praxe	Jako součást regulatorních požadavků na Corporate nebo IT Governance	Všechny velikosti	Pro všechny uživatele	NE	Interně
ISO/IEC 27002	Norma	Jako součást regulatorních požadavků v oblasti ochrany soukromí dat, řízení rizika	Velká	Specialisty řízení informační bezpečnosti	ANO	Externě

Jaká řešení ve vazbě na řízení IT rizik užíváte nebo plánujete použít?

(Vzorek: 749 CIO a CEO, 23 zemí)



Děkuji za pozornost!