Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Prehľad štandardov informačnej bezpečnosti

Daniel Olejár

Jún 2013

KPMG
cutting through complexity™

Štandardizácia v informačnej bezpečnosti

- Význam
  - Nemusíme objavovať to, čo je známe a overené
  - Kompatibilita metód a úrovne ochrany systémov
- Zdroje použiteľných noriem
  - ISO
  - Národné štandardizačné orgány
    - NIST (USA)
    - BSI (Nemecko)
  - Príležitostne medzinárodné organizácie (OECD)
  - Aktivizuje sa ENISA
  - Národné a medzinárodné organizácie (IETF, SANS Institute, ISACA, RSA laboratories a i.)
  - STN – preberáme medzinárodné normy (ISO)

ISO normy pre informačnú bezpečnosť

- Sústredíme sa na najdôležitejšie ISO normy, potom spomenieme užitočné normy NIST a BSI
- ISO normy pre oblasť IB cca 80, z nich niektoré vo vývoji
- Stručné delenie:
  1. Manažment IB
  2. Kryptológia
  3. Evaluácia a certifikácia systémov
  4. Bezpečnostné riešenia (Security controls)
  5. Identifikácia a autentizácia
- Z praktického hľadiska najzaujímavejšia je prvá skupina
- Prebieha systematizácia noriem, zosúlaďovanie IB s manažmentom, a manažmentom kvality
- Prečíslovanie noriem, rad 27000 vyhradený pre manažment IB

ISO/IEC normy radu 27000 (1)

základné

- 4 základné:
- **ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary**
  - Úvod do ISMS (information security management systems, systémov manažmentu informačnej bezpečnosti)
  - Základné pojmy a definície pre oblasť ISMS
  - Prehľad rodiny noriem 27000
- **ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements**
  - Relatívne stručný štandard
  - Definuje požiadavky na zriadenie, implementáciu, prevádzku, monitorova-nie, revíziu, údržbu a zlepšovanie systému riadenia informačnej bezpečnosti
  - Zohľadňuje činnosť, ktorú organizácia vykonáva a hrozby, ktorým čelí
  - Požiadavky sú definované všeobecne a preto je štandard všeobecne použiteľný
  - Väčšina požiadaviek je povinných, ak chce organizácia certifikovať ISMS podľa ISO 27001

ISO/IEC normy radu 27000 (2)

základné

- **ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management**
- Definuje ciele pre jednotlivé oblasti IB a uvádza zoznam bezpečnostných funkcií/opatrení na dosiahnutie stanovených cieľov
- Pokrýva nasledujúce oblasti IB:
  - Bezpečnostná politika
  - Organizácia IB
  - Správa aktív
  - Personálna bezpečnosť
  - Fyzická bezpečnosť
  - Manažment vzťahov s dodávateľmi/poskytovateľmi služieb
  - Prevádzka systémov a komunikácie
  - Manažment aplikačných sieťových služieb
  - Riadenie prístupu
  - Obstarávanie, vývoj a údržba systémov
  - Riešenie bezpečnostných incidentov
  - Manažment kontinuity činnosti
  - Súlad s legislatívou

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

ISO/IEC normy radu 27000 (3)

základné

- **ISO/IEC 27005 Information technology — Security techniques — Information security risk management**
- Užitočný štandard, kompletná správa rizík
- Praktické návody
  - identifikácia aktív
  - Identifikácia hrozieb
  - Identifikácia a ohodnotenie zraniteľností
  - Ohodnotenie rizík

KPMG
cutting through complexity™

ISO/IEC normy radu 27000 (4)

implementácia ISMS

- Normy zamerané na zavedenie a posudzovanie účinnosti ISMS:
- **ISO/IEC 27003 Information technology — Security techniques — Information security management system implementation guidance**
- Rozsiahly štandard
- Návod na praktickú implementáciu ISMS podľa ISO 27001
  - Iniciovanie projektu ISMS
  - Definovanie pôsobnosti ISMS
  - Analýza bezpečnostných požiadaviek
  - Odhad rizík a plánovanie ošetrenia rizík
  - Návrh ISMS
- Podrobne sa rozpisujú aj samozrejmé veci

ISO/IEC normy radu 27000 (5)

meranie účinnosti a audit

- **ISO/IEC 27004 Information technology — Security techniques — Information security management — Measurement**
  - Vychádza z požiadavky ISO/IEC 27001 na pravidelné revízie účinnosti ISMS
  - Obsahuje návod na vývoj a používanie mier, ktoré umožňujú posúdiť účinnosť ISMS a bezpečnostných opatrení
  - Zavedenie Programu/programov merania bezpečnosti
- **ISO/IEC 27007 Information technology — Security techniques — Guidelines for information security management systems auditing**
- Stručná norma poskytujúca návody na
  - na manažment programov auditu a
  - Vykonanie interných a externých auditov ISMS podľa normy ISO 27001
  - Posúdenie kompetentnosti a ohodnotenie audítorov
- Vychádza zo všeobecnejšej normy ISO 19011 Guidelines for auditing management systems, ktorú upravuje na potreby auditu ISMS

ISO/IEC normy radu 27000 (6)

audit

- **ISO/IEC 27006 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems**
  - štandard by bol zaujímavý v prípade, keby MF SR, alebo iný štátny orgán požadoval audit a certifikáciu ISMS podľa ISO 27001
  - Základné požiadavky na organizácie vykonávajúce audit a certifikáciu sú v norme ISO/IEC 17021, táto norma stanovuje dodatočné požiadavky (kompetentnosť a spoľahlivosť) a návod pre takéto organizácie ako splniť požiadavky
  - Pre organizáciu prevádzkujúcu prvok CRITIS je zaujímavá keď dostane ponuku na certifikáciu svojho ISMS

ISO/IEC normy radu 27000 (7)

audit

- **ISO/IEC TR 27008 Information technology — Security techniques — Guidelines for information security management systems auditing**
  - TR poskytuje návod na audit vhodnosti a účinnosti bezpečnostných funkcií ISMS

ISO/IEC normy radu 27000 (8)

ISMS pre špecifické oblasti

- **ISO/IEC 27010 – Information technology – Security techniques -- Information security management for inter-sector communications**
- **ISO/IEC 27011 -- Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations**
- **ISO/IEC 27015 Information technology — Security techniques - Information security management guidelines for financial services**
- **ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002**

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

ISO/IEC normy radu 27000 (9)

rôzne

- **ISO/IEC 27013 Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1**
- **ISO/IEC TR 27016 Information technology — Security techniques — Information security management – Organizational economics**
- **ISO/IEC 27014 Information technology — Security techniques — Governance of information security**

KPMG
cutting through complexity™

Ďalšie ISO normy

ISO/IEC 13335 Management of Information and Communications Technology Security

- Všeobecný návod na inicializáciu a implementovanie procesu riadenia IB
- Inštrukcie, ale nie riešenia ako riadiť IB
- Klasika - základ riadenia IB
- V súčasnosti už len 3 časti
  - 1. Koncepty a modely pre riadenie bezpečnosti IKT
  - 2. techniky pre manažment IB rizík
  - 5. Manažérsky návod na sieťovú bezpečnosť
- ISO/IEC 15408 **Common Criteria**
  - Rozsiahly, voľne dostupný štandard pre certifikáciu systémov
  - Bezpečnostné požiadavky na systémy sa formulujú v podobe ST a PP podľa Common Criteria

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Vydáva dobre spracované, zrozumiteľné, voľne dostupné a použiteľné materiály
- Prepracovaný systém základných požiadaviek na IB : IT Grundschutz, podporený rozsiahlym manuálom a štandardami
- Momentálne 4 BSI štandardy, obsahujúce odporúčania BSI týkajúce sa metód, procesov, procedúr, prístupov a opatrení týkajúcich sa informačnej bezpečnosti
- Sú určené štátnym inštitúciám aj súkromným spoločnostiam
- Zohľadňujú medzinárodné normy
- Okrem štandardov – viacero špecializovaných publikácií, analýz, správ
- https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html

Štandardy BSI (1)

- **BSI Standard 100-1 Information Security Management Systems (ISMS)**
  - definuje všeobecné požiadavky na ISMS
  - Kompatibilný s ISO/IEC 27001
  - Zohľadňuje aj odporúčania ostatných noriem radu 27000
  - Detailnejšie a metodicky lepšie spracovaný dokument ako ISO normy
  - Kompatibilný s IT-Grundschutz prístupom
- **BSI-Standard 100-2: IT-Grundschutz Methodology**
  - Popisuje, ako zaviesť a prevádzkovať ISMS v praxi
  - Ako vytvoriť bezpečnostnú koncepciu, vybrať vhodné bezpečnostné opatrenia a realizovať bezpečnostnú koncepciu v praxi
  - Kompatibilný s ISO normami radu 27000

Štandardy BSI (2)

- **BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz**
  - Používajú sa štandardné („konfekčné“) bezpečnostné riešenia pre typické systémy so štandardnými nárokmi na IB (založené na katalógu IT-Grundschutz opatrení BSI)
  - Zvýšené/špecifické požiadavky – individuálny prístup
  - Analýza rizík (a návrh opatrení)
  - Štandard obsahuje metodiku pre analýzu rizík
  - Príloha: Katalóg elementárnych hrozieb
- **BSI-Standard 100-4: Business Continuity Management**
  - Systematicky popisuje, ako vyvinúť, zaviesť a udržiavať v organizácii systém na riadenie kontinuity činnosti

National Institute of Standards and Technology, NIST

- Americký štandardizačný inštitút
- V rezorte Ministerstva obchodu
- o.i. zodpovedný za štandardizáciu IB pre oblasť neklasifikovanej informácie
- Od konca 80-tych rokov
- Vydáva štandardy a metodické materiály (zoznam na CD v súbore CSD_DocsGuide)
- Primárne určené pre americké štátne organizácie a americké firmy, môžu byť užitočné aj v našich podmienkach
- Do pozornosti
  - NIST Special Publications 800
  - FIPS (Federal Information Processing Standard)
- Menovite SP 800-100 Information Security Handbook: A Guide for Managers

Medzinárodné inštitúcie

- OECD:
  - **The promotion of a culture of security for information systems and Networks in OECD countries**
  - **OECD Recommendation of the Council on the Protection of Critical Information Infrastructures**
- ENISA
  - Zatiaľ skôr prehľady a štúdie
  - http://www.enisa.europa.eu/publications#c2=publicationDate&reversed=on&c5=all&c0=10&b_start=0
- IETF: Vydávajú de facto štandardy pre Internet (RFC)
- ISACA, SANS Institute – de facto štandardy pre vzdelávanie odborníkov v IB
- Iné – napr. RSA laboratories: spravuje štandardy pre PKI (PKCS)

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Slovensko

- SÚTN, technická komisia pre IB
- Na dobrovoľnej báze
- Preberáme štandardy do STN
- problémy:
  - Terminologické
  - Kapacitné
  - Ekonomické
- Rozumnejšie je používať medzinárodné štandardy, resp. preberať ich do STN v origináli
- Využiť v štandardoch vydávaných št. orgánmi (Výnos o štandardoch ISVS)

* * *

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™