MFF UK
Praha, 29. duben 2008

Standardy a normy (informace o předmětu)

http://crypto-world.info/mff/mff_04.pdf

P.Vondruška

Telefónica

O2

Úvod

1. RFC (Request For Comment)
2. Standardy PKCS (Public-Key Cryptographic Standards)
3. České technické normy a svět
4. Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem
5. Přehled mezinárodních a národních normalizačních institucí
6. Přehled některých základních kritérií hodnocení bezpečnosti IT

Úvod (motivační)

1. Proč ? (různé subjekty)
2. Co ?
3. Kdo ?
4. Jak a podle čeho ?
5. Je to OK ?

Úvodní pojmy

Standardy v průmyslovém světě znamenají jednu ze zásadních cest předávání znalostí, snižování nákladů a umožnění vzájemné spolupráce a kompatibility produktů.

1. Standardy (kategorie)
2. Standardní x proprietární … kompatibilita
3. Standard de jure (kodifikován) a de facto (výrobci)
4. Norma (právní závaznost)

RFC (Request For Comment)

1969 - **IETF (*Internet Engineering Task Force)***

Proposed standards — ***Standards Track***

Draft standards

Internet standards (plné de facto normy)

Experimental — ***Off-Track***

Informational

Prototype

Historic

Public-Key Cryptographic Standards

PKCS #1:RSA Cryptography Standard

PKCS #3:Diffie-Hellman Key Agreement Standard

PKCS #5:Password-Based Cryptography Standard

PKCS #6:Extended-Certificate Syntax Standard

PKCS #7:Cryptographic Message Syntax Standard

PKCS #8:Private-Key Information Syntax Standard

PKCS #9:Selected Attribute Types

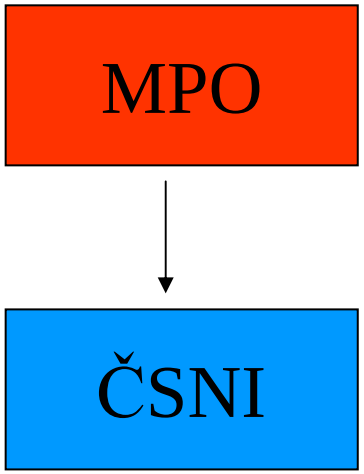
PKCS #10:Certification Request Syntax Standard

PKCS #11:Cryptographic Token Interface Standard

PKCS #12:Personal Information Exchange Syntax Standard

PKCS #13: Elliptic Curve Cryptography Standard

PKCS #15: Cryptographic Token Information Format Standard



Zákon č. 22/1997 Sb.

Ministerstvo průmyslu a obchodu

ČSNI - Českého normalizačního institutu

Česká technická norma

Harmonizovaná česká technická norma

Třídy ČSN (36,…)

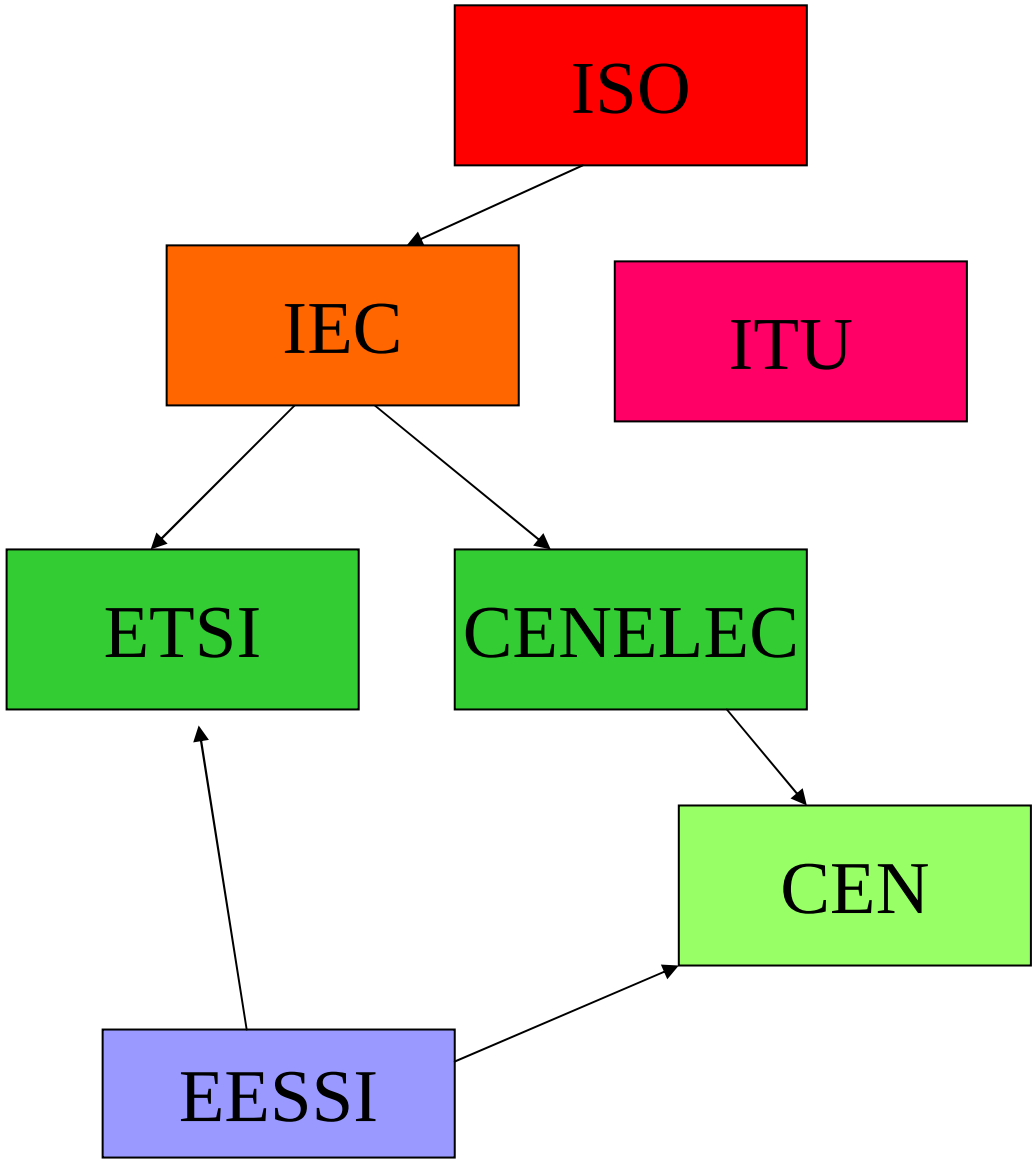
MICR

Zákon č.365/2000 Sb. (ÚVIS)

Ministerstvo informatiky České republiky

Standardy

Atestace



ISO - Mezinárodní organizace pro normalizaci

IEC - Mezinárodní elektrotechnická komise

ETSI - Evropský telekomunikační normalizační institut

CENELEC - Evropský výbor pro elektrotechnickou normalizaci

CEN - Evropský výbor pro normalizaci

EESSI: European Electronic Signature Standardization Initiative

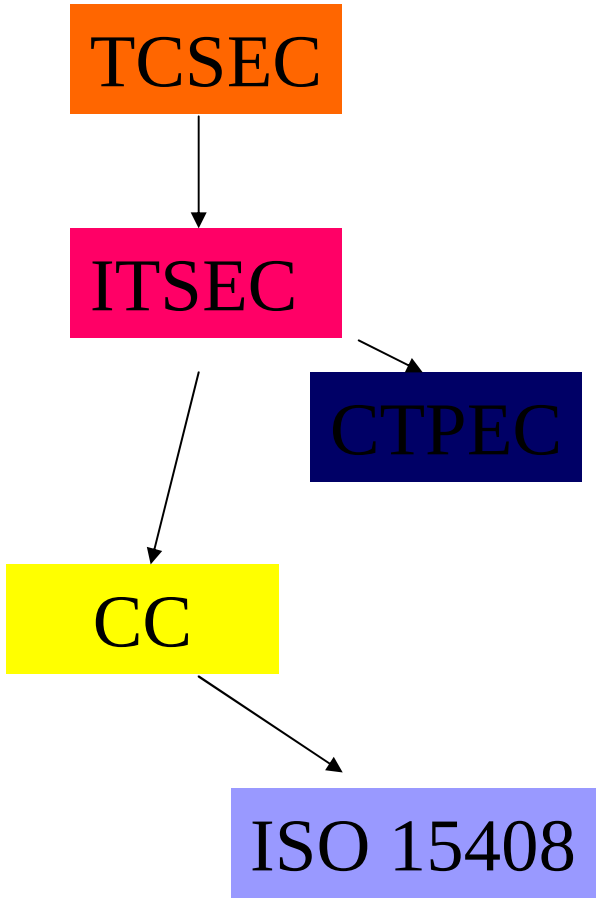
ČSNI - Českého normalizačního institutu

ITU - International Telecommunication Union

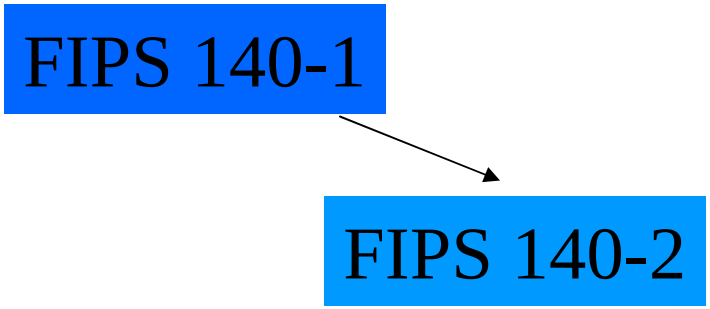
ČSNI

Telefónica

O2



1. Trusted Computer System Evaluation Criteria (TCSEC) - 1985
2. Information Technology Security Evaluation Criteria (ITSEC) - 1990
3. Canadian Trusted Computer Product Evaluation Criteria (CTPEC) - 1995
4. Common Criteria (CC) -1998
5. Kritéria pro hodnocení bezpečnosti IT - (ISO/IEC 15408) - 1999
6. Federal Information Processing Standard (FIPS 140-1 a FIPS 140-2) 1994/2001



ITSEC – Information Technology Security Evaluation Criteria (1)

1. Dosažená úroveň bezpečnosti se hodnotí dosaženou důvěryhodností ve 4 pohledech
   - Vývojový proces
     - forma specifikace požadavků, návrh architektury, detailní návrh, implementace
   - Vývojové prostředí
     - Jak probíhalo řízení projektu, použité programovací jazyky, použité kompilátory, aplikovaná bezpečnost při vývoji
   - Provozní dokumentace
     - dokumentace správce, dokumentace uživatele
   - Provozní prostředí
     - dodávka, distribuce, konfigurace, spuštění, provoz

ITSEC – Information Technology Security Evaluation Criteria (2)

1. **Výsledek** váženého hodnocení ve 4 pohledech
   - označení dosažené bezpečnosti škálované do šesti úrovní bezpečnosti E1 až E6
   - třídy zaručitelnosti bezpečnosti
2. Zařazení do třídy zaručitelnosti bezpečnosti se děje v závislosti na
   - způsobu specifikace vlastností
     (formálně, polo-formálně, neformálně)
   - způsobu prokazování bezpečnostních vlastností
     (testování jen funkcí, testování funkcí i mechanismů)
   - Dosažení předepsaných vlastnosti pro danou třídu zaručitelnosti bezpečnosti

ITSEC – třídy zaručitelnosti bezpečnosti (1)

E0

- nedostatečná zaručitelnost bezpečnosti, hodnocení nelze provést

E1

- musí být dodán bezpečnostní cíl a neformální popis hodnoceného předmětu a testování bezpečnostních funkcí musí indikovat, že hodnocený předmět splňuje bezpečnostní cíl

E2

- navíc proti E1 se požaduje dostupnost neformálního popisu detailního návrhu hodnoceného předmětu a hodnotiteli se musí dodat důkazy testování; musí se provádět správa konfigurace a musí být zaveden proces dodávky hodnoceného předmětu

E3

- navíc proti E2 se požaduje dostupnost detailního návrhu a zdrojové texty programů bezpečnostních funkcí

ITSEC – třídy zaručitelnosti bezpečnosti (2)

E4

- bezpečnostní politika hodnoceného předmětu musí být vyjádřena formálním modelem, požaduje se semi-formální popis architektury a detailního návrhu hodnoceného předmětu a provedení analýzy zranitelnosti na této úrovni

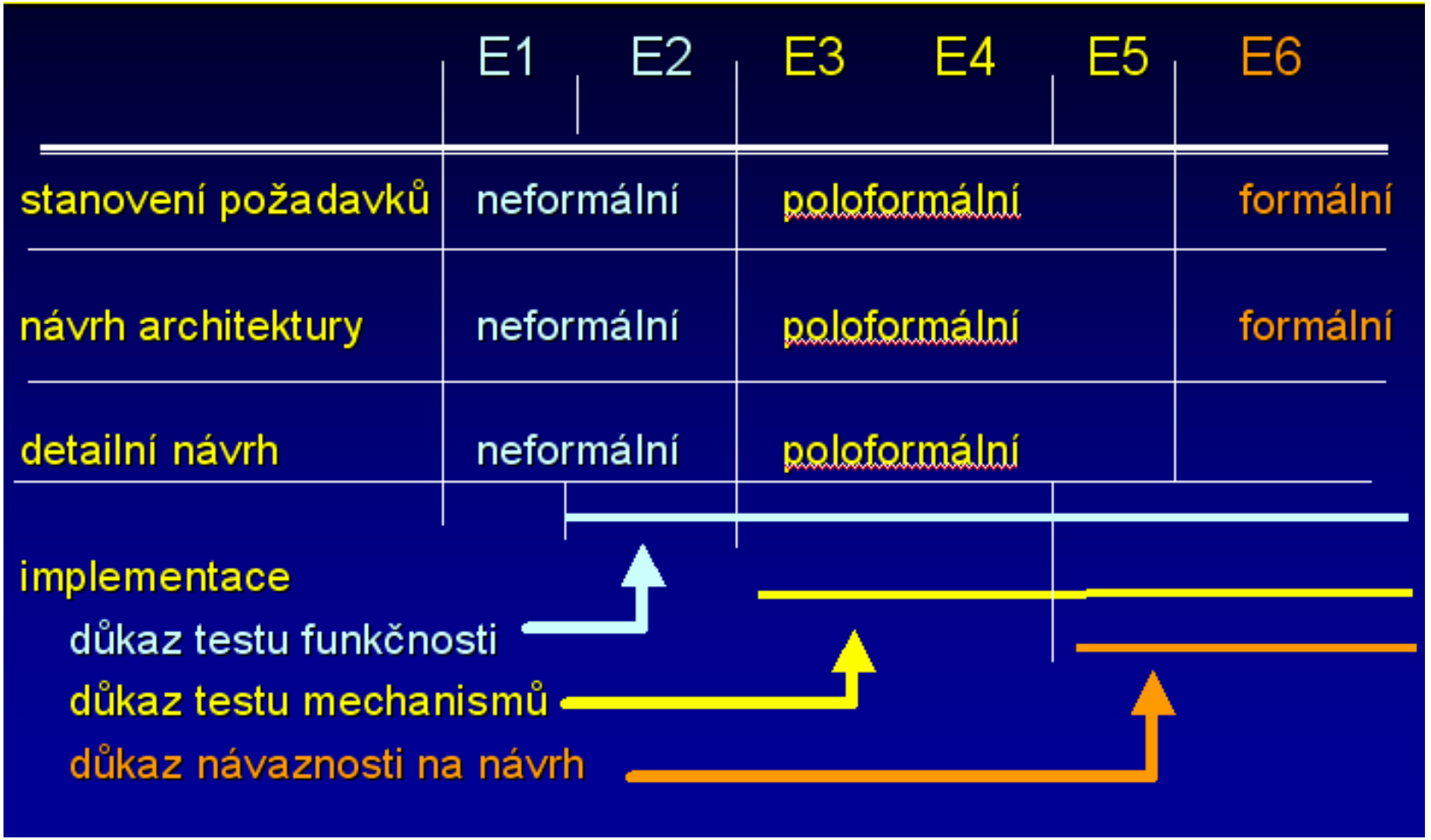
E5

- musí se prokázat úzká souvislost mezi detailním návrhem a implementací na úrovni zdrojových textů programů a provedení analýzy zranitelnosti na této úrovni

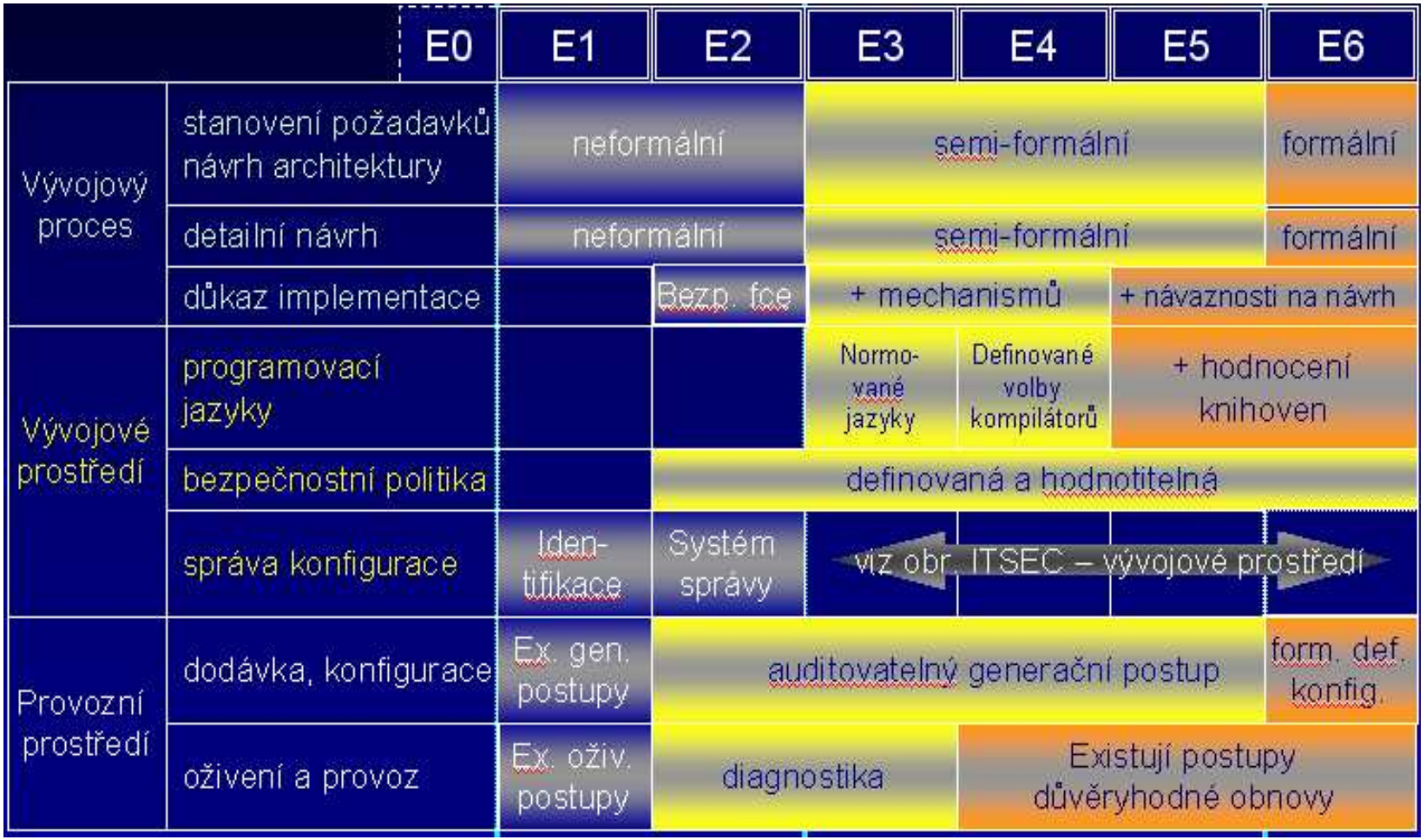
E6

- požaduje se formální popis bezpečnostní architektury hodnoceného předmětu konzistentní s formálním modelem bezpečnostní politiky; musí být jednoznačně prokazatelná souvislost výkonných (binárních) programů s jejich zdrojovými formami.

ITSEC – vývojový proces – příklad pohledu



Celkový přehled důvěryhodnosti podle ITSEC



Nová řada norem ISO/IEC 27000

Řada ISO 27000 byla organizací ISO **I**nternational **O**rganization for **S**tandardization rezervována pro normy z oblasti bezpečnosti informací. (Podobně, jako tomu je u norem pro řízení kvality série ISO 9000)

Cílem je zavedení jednotného systému řízení pro všechny oblasti a umožnění budování integrovaného systému řízení.

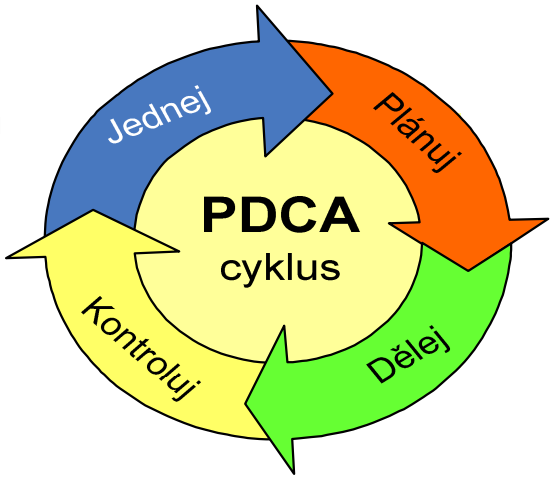
1. **ISO 27000** – *slovník a definice pojmů*
2. **ISO 27001 "Information Security Management Systems"**
3. **ISO 27002 "Code of practice for information security management"**
4. **ISO 27003** - *implementační příručka*
5. **ISO 27004 "Information Security Management Metrics and Measurement"**
6. **ISO 27005 "Information Security Risk Management"**
7. **ISO 27006 "Guidelines for information and communications technology disaster recovery services"**

ISO/IEC 27001 "Information Security Management Systems"

- Norma prosazuje procesní budování a provozování systému řízení informační bezpečnosti
- Jsou uplatněny stejné principy budování a zdokonalování ISMS postavené na základě PDCA cyklu:

- Schválení zlepšování ISMS
- Řízení a realizace nápravných/preventivních kroků

- Kontrola účinnosti aplikovaných protiopatření
- Přezkoumání ISMS vedením



- Stanovení politiky, cílů, rozsahu působnosti ISMS
- Analýza rizik

- Řízení rizik
- Aplikace politiky ISMS, opatření, procesů a postupů

- Efektivní řízení bezpečnosti informačních aktiv realizované na základě výsledků analýzy rizik:
  - Nutný proces: **identifikace aktiv – analýza rizik – řízení rizik**

- Dle této normy se provádí certifikace ISMS

- Nová řada ISO 27000 norem v CZ: http://www.iso27000.cz/

Pavel Vondruška
Crypto-World
http://crypto-world.info
mobil +420 602 560 963
