

# SW Process Audit vs. SW Process Assessment

(úvod do problematiky)

**Ing. Dávid Piskáček**  
**fakulta BERG, Technická univerzita Košice**

**QIT 2005**

# Agenda

**1. Rozdelenie Auditu IS**

**2. Audit kvality podľa ISO 9000**

**3. Audit podľa ISO 19 011**

**4. Audit podľa COBIT (ISACA)**

**5. Audit podľa BS 7799**

**6. Audit podľa CMMI**

**7. Audit podľa BSA**

**8. Personálny Audit IS podľa zákona 428/2002 Z.z.**

**9. Záver**

# 1. Rozdelenie Auditu IS

- **AUDIT IS – legálnosť SW (BSA)**
- **AUDIT KVALITY – systém kvality organizácie**
- **Účtovný AUDIT – dodržiavanie legislatívnych pravidiel**
- **AUDIT IS – ISACA (IT Governance)**
- **Security AUDIT IS**
- **Informačný AUDIT - ???**
- **Personálny AUDIT - ???**

# 1. Rozdelenie Audit IS



## 2. Audit kvality podľa ISO 9000

### Informačné zdroje:

- *STN EN ISO 9000:2000*  
*„Systémy manažérstva kvality. Základy a slovník.“*
- *STN EN ISO 9001:2000*  
*„Systémy manažérstva kvality. Požiadavky.“*
- *ISO/IEC 90003:2004*  
*„Software and system engineering - Guidelines for the application of ISO 9001:2000 to computer software.“*

## 2. Audit kvality podľa ISO 9000

### Audit kvality (ISO 9000:2000)

- Audity sa využívajú na určenie rozsahu, v akom sa splnili požiadavky systému manažérstva kvality. Zistenia auditu sa môžu použiť na posúdenie efektívnosti systému manažérstva kvality a na identifikáciu príležitostí na zlepšenie.

Návod na audit popisuje norma ISO 19011.

# 2. Audit kvality podľa ISO 9000

## Vyhodnocovanie procesov (ISO 9000:2000)

4 základné otázky:

- Je proces identifikovaný a primerane opísaný?
- Priradili sa zodpovednosti?
- Zaviedli sa a udržiavajú sa postupy?
- Je proces pri dosahovaní požadovaných výsledkov efektívny?

Spoločné odpovede na tieto otázky môžu určiť výsledok vyhodnocovania. Vyhodnocovanie systému manažérstva kvality môže mať rozličné zameranie a môže zahŕňať rad činností, ako je audit, preskúmanie systému manažérstva kvality a samohodnotenie.

## 2. Audit kvality podľa ISO 9000

### (ISO 9000:2000) Termíny súvisiace so zhodou

- **zhoda:** splnenie požiadavky
- **nezhoda:** nespĺnenie požiadavky
- **chyba:** nespĺnenie požiadavky
- **preventívna činnosť:** činnosť na odstránenie príčiny potenciálnej nezhody
- **nápravná činnosť:** činnosť na odstránenie príčiny zistenej nezhody
- **prepracovanie:** činnosť vykonaná na nezhodnom produkte s cieľom urobiť ho zhodným s požiadavkami
- **oprava:** činnosť vykonaná na nezhodnom produkte s cieľom urobiť ho prijateľným na zamýšľané používanie

## 2. Audit kvality podl'a ISO 9000

### Meranie (ISO 9003:2004):

#### 3.7 measure, verb

- make a measurement
- [ISO/IEC 14598-1:1999, definition 4.17]

#### 3.8 measure, noun

- variable to which a value is assigned as the result of measurement
- [ISO/IEC 15939:2002, definition 3.14]

#### 3.9 measurement

- set of operations having the object of determining a value of a measure
- [ISO/IEC 15939:2002, definition 3.17]

# 3. Audit podľa ISO 19 011

## Informačné zdroje:

Návod na auditovanie systému manažérstva kvality a/alebo systému environmentálneho manažérstva STN EN ISO 19011

## Definície: Audit

Systematický, nezávislý a zdokumentovaný proces získavania dôkazov auditu a ich objektívneho vyhodnocovania s cieľom určiť rozsah, v akom sa plnia kritéria auditu

## Definície: Interný Audit

Interné audity, niekedy označované ako audity vykonávané prvou stranou, vykonáva sama organizácia alebo niekto v jej zastúpení na účely preskúmania manažmentom alebo na iné interné účely a môžu tvoriť základ vyhlásenia o zhode samou organizáciou. V mnohých prípadoch, najmä v malých organizáciách, možno nezávislosť preukázať neexistujúcou zodpovednosťou za auditovanú činnosť.

# 3. Audit podľa ISO 19 011

## Definície: Externý Audit

Externé audity zahŕňajú audity všeobecne označované ako audity vykonávané druhou alebo treťou stranou. Audity vykonávané druhou stranou vykonávajú strany, ktoré sa zaujímajú o organizáciu, ako sú zákazníci alebo ďalšie osoby v ich zastúpení. Audity vykonávané treťou stranou vykonávajú externe nezávislé audítorské organizácie, ako sú organizácie poskytujúce registráciu alebo certifikáciu zhody s požiadavkami podľa normy ISO 9001 alebo ISO 14001.

## Definície:

- Audítor (angl. auditor): osoba s kompetentnosťou vykonávať audit
- klient auditu (angl. audit client): organizácia alebo osoba požadujúca audit
- auditovaná organizácia (angl. auditee): organizácia, ktorá sa audituje

# 4. Audit podľa ISACA

## Informačné zdroje:

- [www.isaca.sk](http://www.isaca.sk)
- [www.isaca.org](http://www.isaca.org)
- 010.010.010 Audit Charter
- 060.020.030 Audit Evidence Requirement
- COBIT® 3rd Edition Audit Guidelines

## ISACA

ISACA je so svojimi viac ako 28.000 členmi vo viac ako 100 krajinách renomovanou profesijnou organizáciou a lídrom v oblasti riadenia, bezpečnosti a kontroly informačných technológií. Bola založená v roku 1969 ako EDP Auditors Association.

**Ciel': vývoj a šírenie štandardov pre audit IS**

# 4. Audit podľa ISACA

## Compliance Audit IS (ISACA)

Audit IS (ISACA)- zahŕňa previerku a ohodnotenie všetkých aspektov systémov na automatické spracovanie transakcií, vrátane s nimi spojených manuálnych procesov a väzieb medzi nimi.

## Maturity Audit (ISACA)

Hodnotenie zrelosti procesov IT (ISACA)- zahŕňa previerku a klasifikáciu všetkých procesov IT a väzieb medzi nimi z pohľadu požiadaviek modelu CobiT v rozsahu 0-5 úrovni zrelosti procesov IT.

# 4. Audit podľa ISACA

## Štandardy

- stanovujú povinné požiadavky na audit IS a správy z auditov IS

## Smernice

- poskytujú návod na aplikovanie Štandardov pre audit IS.
- Cieľom Smerníc pre audit IS je poskytnúť ďalšie informácie o tom, ako dosiahnuť súlad so Štandardmi pre audit IS.

## Pracovné postupy

- poskytujú príklady postupov, ktorými sa audítor IS môže riadiť pri výkone auditu.
- Cieľom Pracovných postupov pre audit IS je poskytnúť ďalšie informácie o tom, ako dosiahnuť súlad so Štandardmi pre audit IS.

# 4. Audit podľa COBIT (ISACA)

**CobiT® „Control Objectives for Information and related Technology“**

Prostriedky štandardu CobiT® sa majú používať ako usmernenie vychádzajúce z najlepšej praxe. Každá z ďalej uvedených súčastí je organizovaná podľa procesov riadenia IT tak, ako je to definované v časti CobiT Framework.

Celkový rámec metodiky COBIT zahrňuje užívateľov, manažérov a auditórov. Mal by pomôcť v nasledujúcich oblastiach:

- **Manažment**
- **Užívateľia**
- **Auditori**

# 4. Audit podľa COBIT (ISACA)

## CobiT® - využitie vo firme

Executive Manager  
Business Manager

IT Manager

Project Manager

Developer

Operations

User

Information Security

Auditor

- General IT governance model
- Communication with IT
- Service Level Agreements
- Baseline for control objectives/external certifications
- Communication with business function
- Service Level Agreements
- Performance Measures
- IT related policies and norms
- Project standards
- Quality assurance standards
- Controls within development process
- Controls to be built into system
- Controls for service delivery and support
- Controls to be fully operational / built into system
- Integrate security with IT objectives
- IT audit universe
- IT control reference

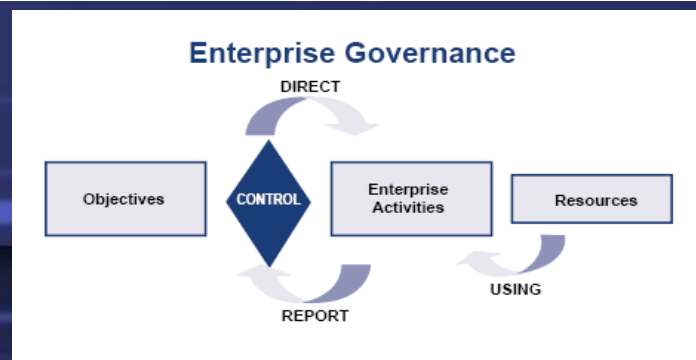
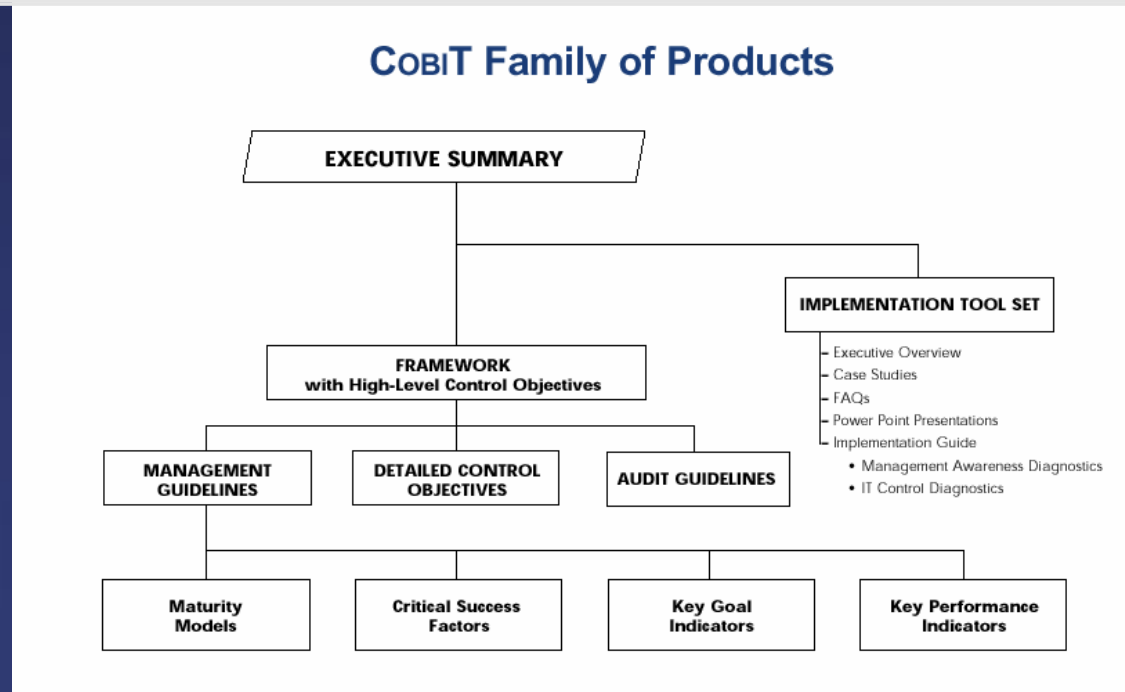
# 4. Audit podľa COBIT (ISACA)

## CobiT® „Control Objectives for Information and related Technology“

- COBIT je nezávislý na technologických platformách použitých v podniku
- Podniková informatika je v COBIT rozdelená na funkčné domény (plánovanie, implementácia, prevádzka, monitoring). Domény obsahujú konkrétne procesy.
- Procesy sú pomenované 7 informačnými kritériami (efektívnosť, výkonnosť, dôvernosť, integrita, dostupnosť, súlad, spoľahlivosť).
- Zistenia sú tiež priradené 5 zdrojom (personál, aplikácia, technológia, vybavenosť, dáta).
- Výsledkom je normovaný (a vzájomne porovnateľný) pohľad na spôsob riadenia informatiky podniku a jeho dosiahnutú úroveň (0-5).

# 4. Audit podľa COBIT (ISACA)

## COBIT – štruktúra dokumentácie



# 4. Audit podľa COBIT (ISACA)

## COBIT – obsah dokumentácie

### Executive Summary

- “There is a Method...” Summary of CobIT Concepts
- Framework
  - “The Method Is...” ..... 34 IT processes and 7 Information Criteria
- Control Objectives
  - “Minimum Controls Are...” ..... 300+ Control Objectives
- Audit Guidelines
  - “Here’s How You Audit...”
- Management Guidelines
  - “Here’s How You Measure Your Performance...”
  - approx. 500 KGI’s, KPI’s, CSF’s
- Implementation Guide
  - “Here’s How You Implement...”

# 4. Audit podľa COBIT (ISACA)

## COBIT – štruktúra auditu

- Identifikácia a dokumentácia
- Hodnotenie
- Test zhody
- Test skutočnosti

IT procesy sú auditované:

- Získaním a pochopením požiadaviek, rizík a kontrolných opatrení
- Hodnotením kontroly
- Posudzovaním zhody testovaním či kontrola pracuje presne a súvisle
- Formulovaním rizika

# 5. Audit podľa BS 7799

## Informačné zdroje:

- BS 7799-1:1999 Part 1: Code of practice for information security management
- BS 7799-2:1999 Part 2: 1999 Specification for information security management system
- STN ISO/IEC 17799:2002 - Informačné technológie – Súbor postupov pre riadenie informačnej bezpečnosti

# 5. Audit podľa BS 7799

## Štandard:

- obsahuje najlepšie praktiky pre riadenie bezpečnosti informácií v organizáciách
- vymedzuje organizačné predpoklady pre správu bezpečnosti informácií v organizáciách
- zabezpečuje dôveru spolupracujúcich organizácií v bezpečnosti pri spracovaní informácií
- je návodom na vytvorenie firemnej informačnej bezpečnostnej politiky, ako aj ďalších bezpečnostných dokumentov
- Zachovanie: dôvernosti, integrity a dostupnosti informácií.

# 6. Audit podľa CMMI

## Informačné zdroje:

Capability Maturity Model® Integration (CMMISM), Version 1.1

## Assessment

posudzovanie existujúcich procesov s procesmi podľa referenčného modelu

- verifikácia - potvrdenie splnenia určených požiadaviek
- validácia - potvrdenie splnenia požiadaviek na zamýšľané použitie

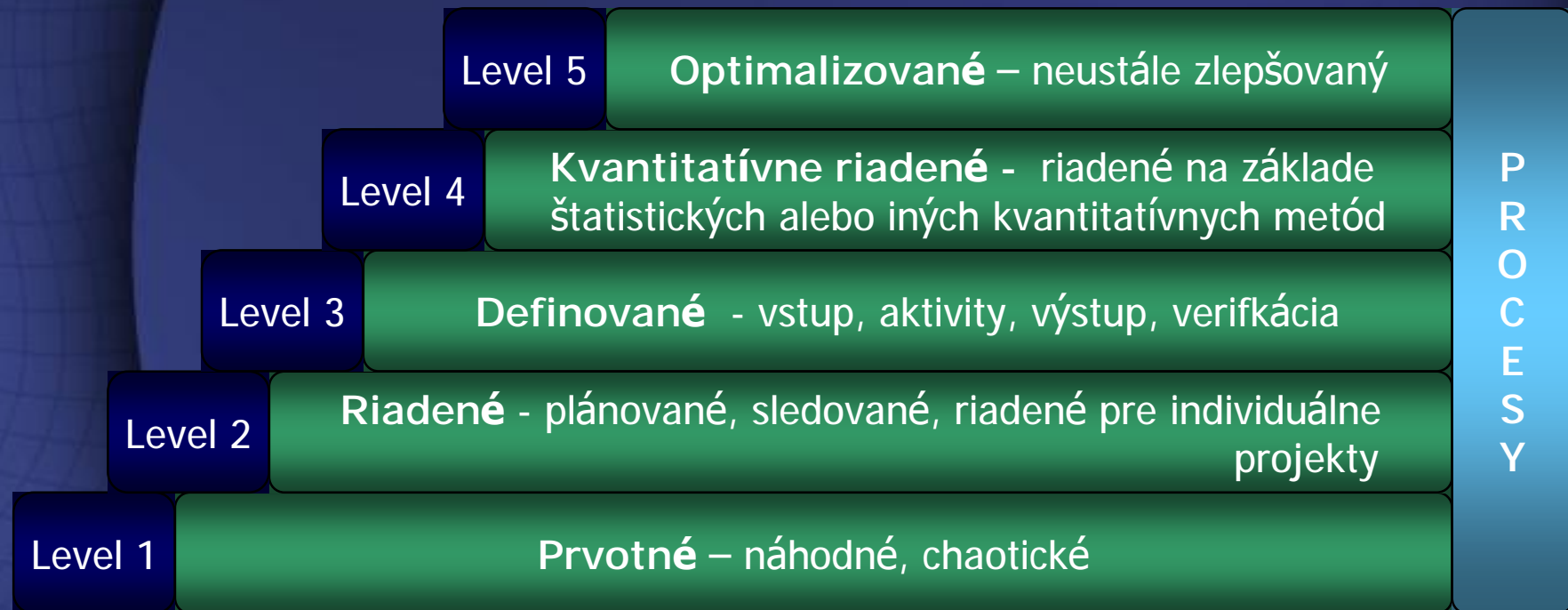
# 6. Definície podľa CMMI

## Capability Maturity Model Integration (Integrovaný model spôsobilosti a zrelosti procesov)

- Kvalita softvérového produktu je determinovaná kvalitou procesov, ktoré sa používajú pri jeho vývoji a neskoršej údržbe.
- Spôsobilosť (Capability) označuje úroveň akou je organizácia schopná riadiť procesy, kontrolovať náklady a časový plán v rámci jednej procesnej oblasti alebo špecifickej praxe.
- Zrelosť (Maturity) označuje úroveň akou je organizácia schopná riadiť procesy, kontrolovať náklady a časový plán v rámci celého súboru procesných oblastí naprieč celou organizáciou.

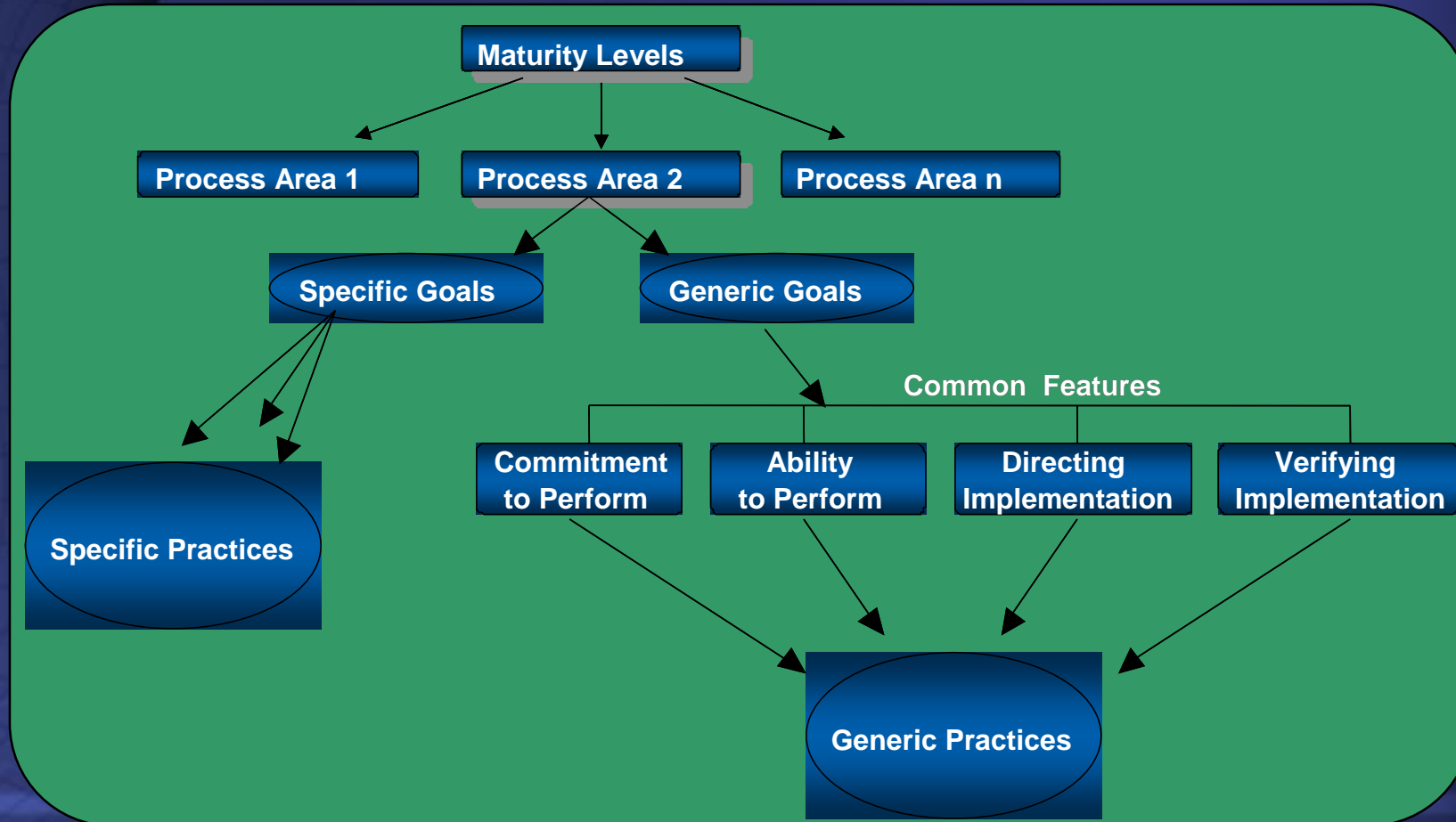
# 6. Definície podľa CMMI

Model definuje 5 úrovní zrelosti (Maturity Levels) na základe spôsobilosti procesov.



# 6. Definície podľa CMMI

## Štruktúra CMMI



# 7. Audit podľa BSA

## Informačné zdroje:

- [www.microsoft.com](http://www.microsoft.com)
- [www.bsa.sk](http://www.bsa.sk)

## Audit podľa BSA:

- dôkladná inventarizácia softvéru
- je základným nástrojom softvérového manažmentu, ktorý komplexne rieši problematiku správy licencií k softvéru v organizácii

# 8. Audit IS podľa zákona 428/2002

## Informačné zdroje:

- Zbierka zákonov Slovenskej republiky, zákon č. 428/2002 Z.z. o ochrane osobných údajov

## Audit IS na ochranu osobných údajov podľa zákona 482/2002 Z.z. o ochrane osobných údajov

- ochrana osobných údajov fyzických osôb pri ich spracúvaní
- zásady spracúvania osobných údajov
- bezpečnosť osobných údajov
- registráciu a evidenciu informačných systémov

# 8. Audit IS podľa zákona 428/2002

## Bezpečnostný projekt (§16, ods. 1 zákona č. 428/2002 Z.z.)

Bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

# 8. Audit IS podľa zákona 428/2002

## Bezpečnostný projekt (§16, z.č. 428/2002 Z.z.)

- Bezpečnostný zámer

Vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému, v ktorom sú spracúvané osobné údaje, pred ohrozením a narušením jeho bezpečnosti.

- Analýza bezpečnosti informačného systému

Obsahuje podrobný rozbor stavu bezpečnosti informačných systémov. Na základe analýzy ohrození, nežiadúcich dopadov a stanovení rizík, sú popísané spôsoby použitia bezpečnostných štandardov, metód a prostriedkov ochrany osobných údajov nachádzajúcich sa v predmetných informačných systémoch.

# 8. Definície podľa zákona 428/2002

## Bezpečnostný projekt (§16, z.č. 428/2002 Z.z.)

- Bezpečnostná smernica

Obsahuje aplikáciu záverov bezpečnostného zámeru a analýzy bezpečnosti do podoby vykonávacích pokynov pre manažment predmetných informačných systémov

# 9. Záver

ISO 9000 - Audit kvality  
ISO 90003 - metriky  
ISO 19011 - Návod Auditů

BS 7799  
STN ISO/IEC 17799:2002  
Security audit IT

COBIT  
Štandard pre auditovanie  
IT

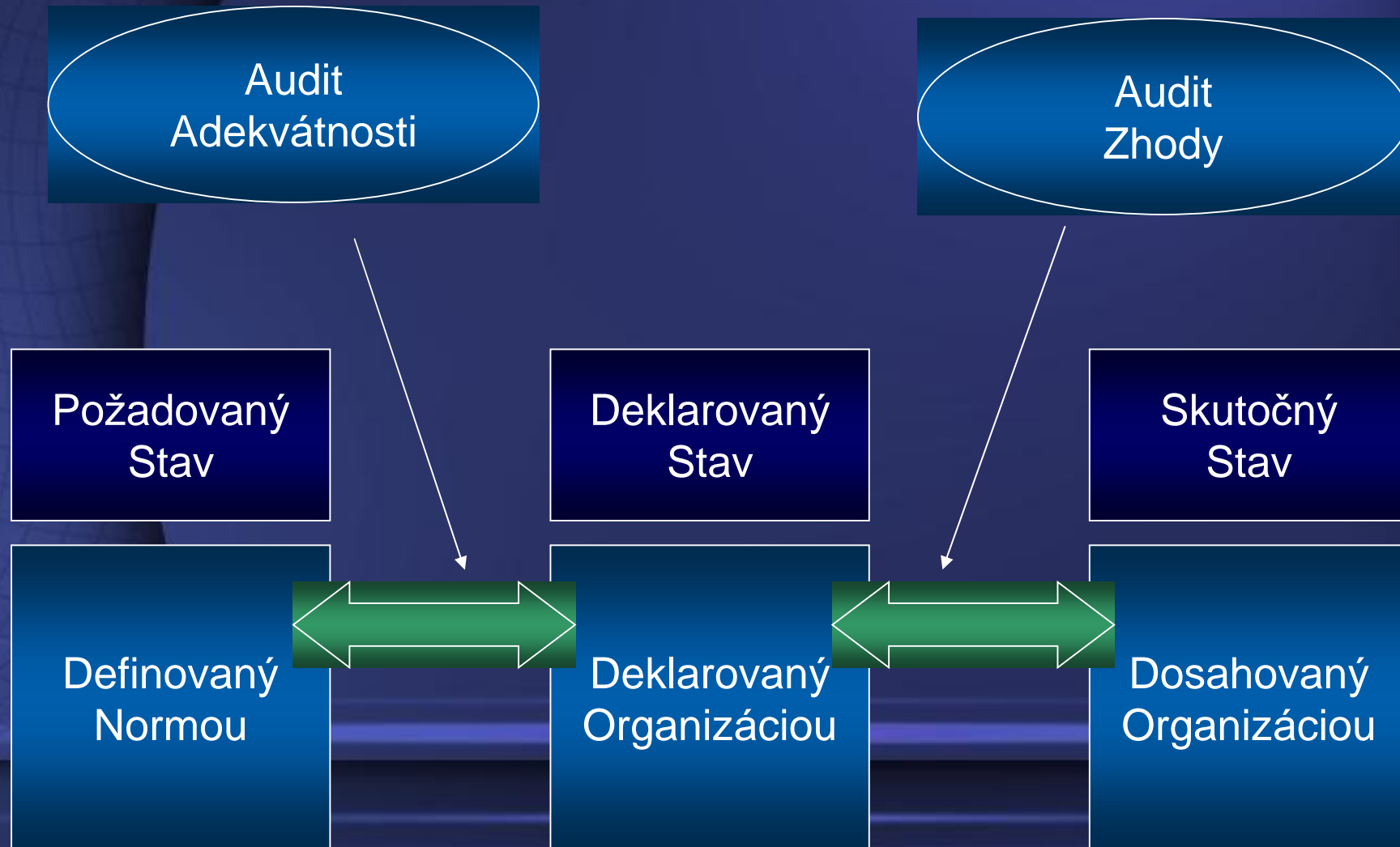
A  
U  
D  
I  
T  
  
I  
S

BSA  
Audit legálnosti SW

Ochrana osobných údajov  
Personálny audit

CMMI  
Posudzovanie  
Kvality SW

# 9. Záver



# 9. Závěr

	Audit adekvátnosti	Audit zhody
ISO 9000	Y	N
ISO 19 011	Y	N
COBIT	N	Y
COBIT	N	Y
BS 7799	Y	N
Zákon 428/2002 Z.z.	Y	N

# 9. Záver

Audit	Výstup	Výsledky
ISO 9000	Protokol	Zistenia
ISO 19 011	Správa	Nálezy
BSA (legálnosť)	Protokol	Nálezy
COBIT	Protokol	Zistenia
BS 7799	Certifikát	Posúdenie rizík
Zákon 428/2002 Z.z.	Správa	Zistenia

# 9. Záver

## CMM vs. COBIT

CMMI	COBIT
<b>Assessment spôsobilosti + zrelosti</b>	<b>Assessment zrelosti</b>
<b>Kľúčové procesné oblasti (4)</b>	<b>Procesné domény (6)</b>
<b>Procesné oblasti (25)</b>	<b>Procesy IT (37)</b>
<b>Spôsobilosť/zrelosť procesov L1-L5</b>	<b>Zrelosť procesov IT L0-L5</b>
<b>Kvalita procesov vývoja SW</b>	<b>Úroveň riadenia procesov IT</b>
<b>Neaudituje sa</b>	<b>Audit zhoda - nezhoda</b>

Ďakujem za pozornosť!