



# **AUDIT INFORMAČNÍ BEZPEČNOSTI**

**BIVŠ: Řízení kvality (audit) IS**

# OSNOVA:

1. Terminologie
2. Audit informační bezpečnosti (normy)
3. Životní cyklus řízení auditu informační bezpečnosti
4. Certifikační audit informační bezpečnosti
5. Obecné audity informační bezpečnosti
  1. Technologický audit informační bezpečnosti



# 1. TERMINOLOGIE:

Akreditace ??? Atestace ??? Certifikace



# AKREDITACE

- **Akreditace** je proces udílení oprávnění provádět atestace nebo certifikace
- **Atestace:**
  - probíhají podle novely zákona č.365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění jeho novely č. 81/2006 Sb.
  - atestem správci ISVS dokládají splnění povinností uložených platnou legislativou (ministerstva, státní orgány, správní úřady i orgány územní samosprávy, stejně jako dodavatelé, kteří pro tyto orgány zajišťují dodávky či provoz informačního systému)
  - atestační střediska pověřuje Ministerstvo vnitra ČR
  - atestace:
    - Stanovení shody **dlouhodobého řízení** informačních systémů veřejné správy s požadavky zákona
    - Stanovení shody způsobilosti k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím **referenčního rozhraní**

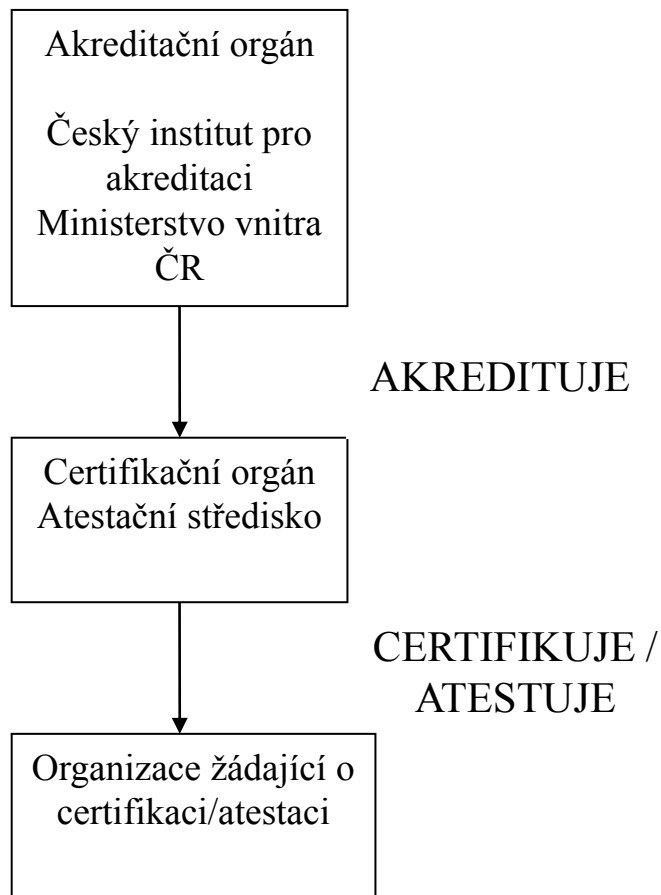


# CERTIFIKACE

- proces prověřování a případně následného udělení osvědčení o tom, že daná organizace splňuje požadavky některé z norem ISO (International Organization for Standardization)
- vysvědčení, kterým společnost dokládá svým zákazníkům, že všechny její činnosti jsou v souladu s příslušnou normou ISO
- certifikace nebo certifikační audit
- certifikaci provádějí nezávislé společnosti akreditované u Českého institutu pro akreditaci (ČIA)



# VZTAHY MEZI AKREDITACÍ, ATESTACÍ A CERTIFIKACÍ



# DRUHY CERTIFIKACÍ

## Obecně

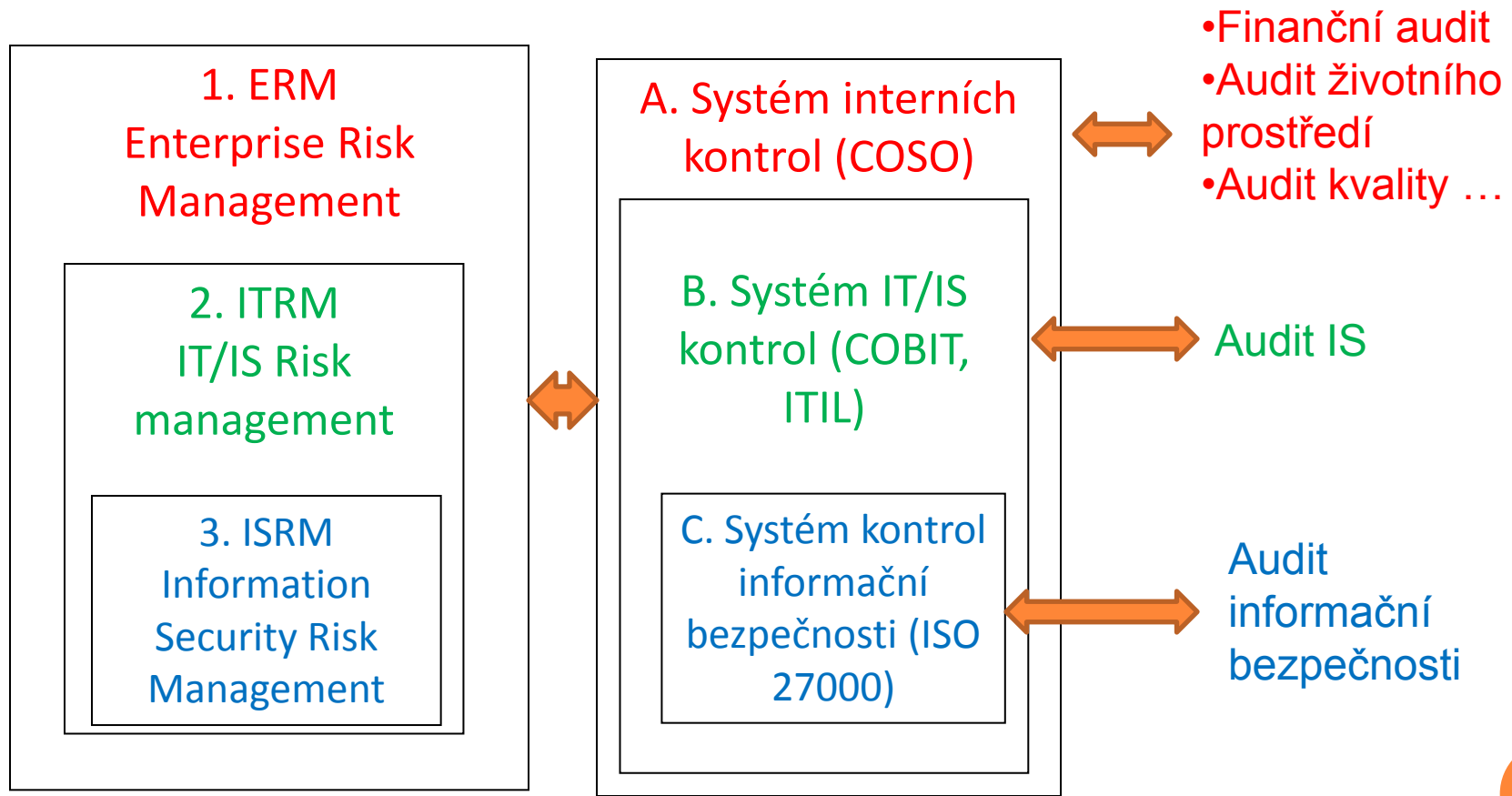
- 1. certifikace **produktů**
- certifikace organizací
  - 2. certifikace **služeb**
  - 3. certifikace **systemů řízení**
- 4. certifikace **osob**

## Oblast informační bezpečnosti

- 1. certifikace **produktů** (ISO 15408)
- certifikace organizací
  - 2. certifikace **služeb** (ISO 20000)
  - 3. certifikace **systemů řízení** (ISO 27001)
- 4. certifikace **osob** (ISACA, ITIL)

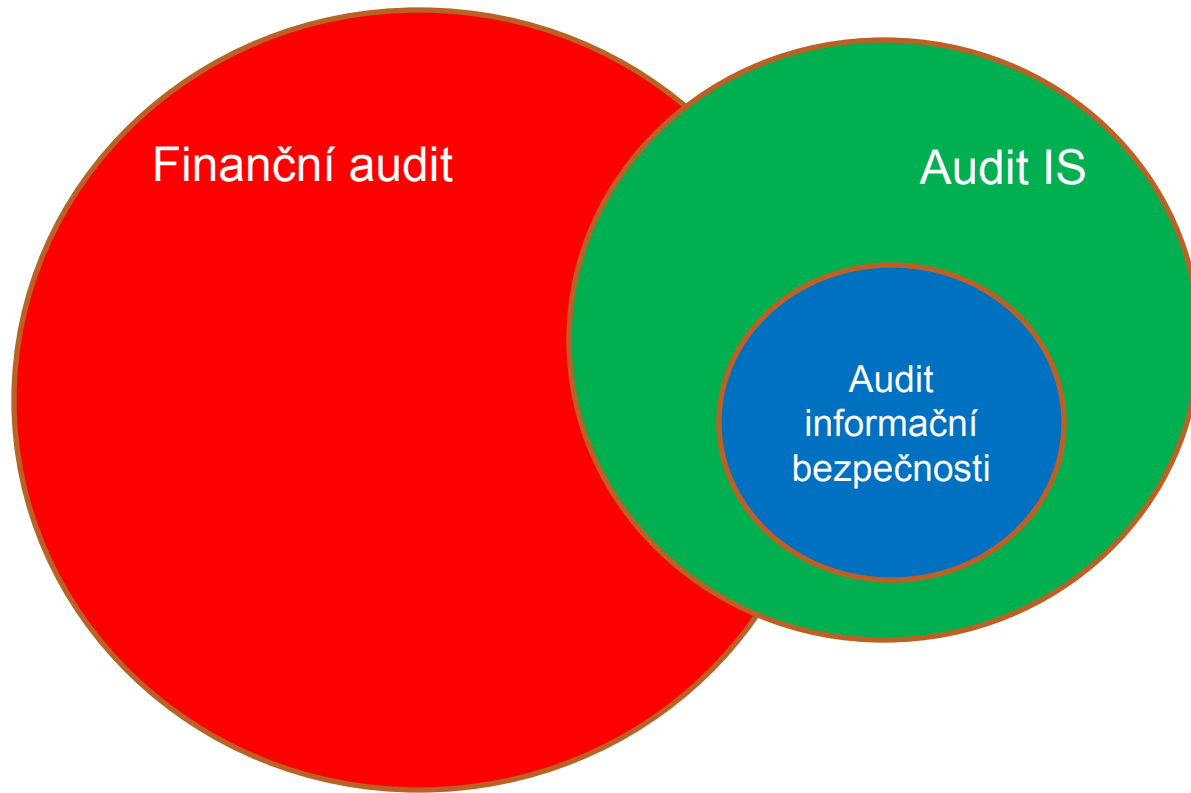


# VZTAHY MEZI RŮZNÝMI DRUHY AUDITU





# VZTAHY MEZI RŮZNÝMI DRUHY AUDITU



# AUDIT INFORMAČNÍ BEZPEČNOSTI

- specifický druh auditu informačního systému, který se zaměřuje na jeden z významných aspektů informačních systémů – bezpečnost (Cobit):
  - **bezpečnost**: důvěrnost, integrita, dostupnost
  - **kvalita**: efektivita, účinnost
  - **důvěryhodnost**: spolehlivost, soulad s legislativou
- nedílná součást systémové bezpečnostní politiky:
  - plán obnovy a havarijní plán,
  - implementace bezpečnostního systému,
  - monitoring (průběžné sledování účinnosti bezpečnostního systému)
  - řešení bezpečnostních incidentů,
  - audit ( následné sledování účinnosti bezpečnostního systému)
- hodnotí úroveň bezpečnosti neinvazivním způsobem, pasivní sběr informací o konfiguraci a nastavení zařízení a následné vyhodnocení těchto informací a vyvození závěrů
- měl být vždy prováděn za asistence odborníků – informatiků v auditované společnosti (nejlépe administrátorů), výjimky: black-box audit

# POSTUP AUDITU

- Obecný životní cyklus **řízení** auditu – společný pro všechny audity informační bezpečnosti
- Specifické životní cykly auditu
  - **certifikační audit informační bezpečnosti**
  - **obecný audit informační bezpečnosti**



### 3. ŽIVOTNÍ CYKLUS ŘÍZENÍ AUDITU

- ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing
- Vydaná 24.11. 2011
- Obsahuje doporučení k provádění auditů ISMS podle ISO/IEC 27001
- Vazba na ISO 19011:2011, *Guidelines for auditing management systems*
- vhodná pro interní auditory, akreditované společnosti, třetí strany



# ŽIVOTNÍ CYKLUS ŘÍZENÍ AUDITU PODLE ISO 27007

7 etap:

## 1. Zahájení auditu:

- stanovení vedoucího týmu,
- definování cílů auditu, rozsahu a kritérií,
- hodnocení proveditelnosti auditu,
- vytvoření auditorského týmu
- navázání prvního kontaktu s auditovanou stranou.

## 2. Analýza dokumentů

- studium relevantní dokumentace systému řízení (včetně elektronických záznamů) a hodnocení jejich adekvátnosti vzhledem k použitým kritériím,

## 3. Příprava na audit v místě zákazníka

- příprava plánu auditu,
- rozvržení úkolů členům týmu,
- příprava pracovních materiálů (check listy, formuláře pro záznam z jednání, plány tvorby vzorků apod.)



# ŽIVOTNÍ CYKLUS ŘÍZENÍ AUDITU PODLE ISO 27007 (POKR.)

## 4. Realizace auditu v místě zákazníka

- úvodní setkání se zákazníkem (představení členů týmu, cíle a rozsahu auditu, stanovení způsobů komunikace, zajištění místa a potřebných zařízení apod.),
- komunikace se zákazníkem (způsob referování o postupu auditu zákazníkovi, řešení problémů, změn),
- role a odpovědnosti průvodců a pozorovatelů (nejsou součástí týmu, obvykle jde o osoby určené auditovanou stranou pro asistenci auditorům),
- shromažďování a ověřování dokumentace,
- formulování nálezů (nálezy mohou potvrdit soulad nebo nesoulad s určenými kritérii; v případě, že je cílem auditu i návrh opatření na zlepšení, formulují se nálezy včetně těchto opatření),
- příprava závěrů auditu (auditorský tým předběžně projednává formulované nálezy auditu a diskutuje další postup auditu),
- organizování uzavřeného jednání o závěrech auditu (auditorský tým společně se zástupci auditované strany prezentují výsledky auditu a řeší opatření pro případ, že existují nějaké důvody vedoucí ke snížení spolehlivosti závěru auditu)



# ŽIVOTNÍ CYKLUS ŘÍZENÍ AUDITU PODLE ISO 27007 (POKR.)

## 5. Příprava, odsouhlasení a distribuce auditorské zprávy

- příprava auditorské zprávy,
- odsouhlasení a distribuce auditorské zprávy  
(auditorská zpráva je vlastnictvím auditované strany a musí se zachovávat určená pravidla jejího utajení)

## 6. Ukončení auditu.

## 7. Kontrola plnění doporučených opatření



# OBSAH AUDITORSKÉ ZPRÁVY

## Základní údaje:

- Cíle auditu
- Rozsah auditu, zvláště identifikaci auditovaných organizačních a funkčních jednotek nebo procesů a časový úsek, ve kterém audit proběhl
- Identifikace klienta
- Identifikaci vedoucího auditora a jeho týmu
- Data a místa, ve kterých proběhla šetření v místě zákazníka
- Kriteria auditu
- Nálezy auditu
- Závěry auditu



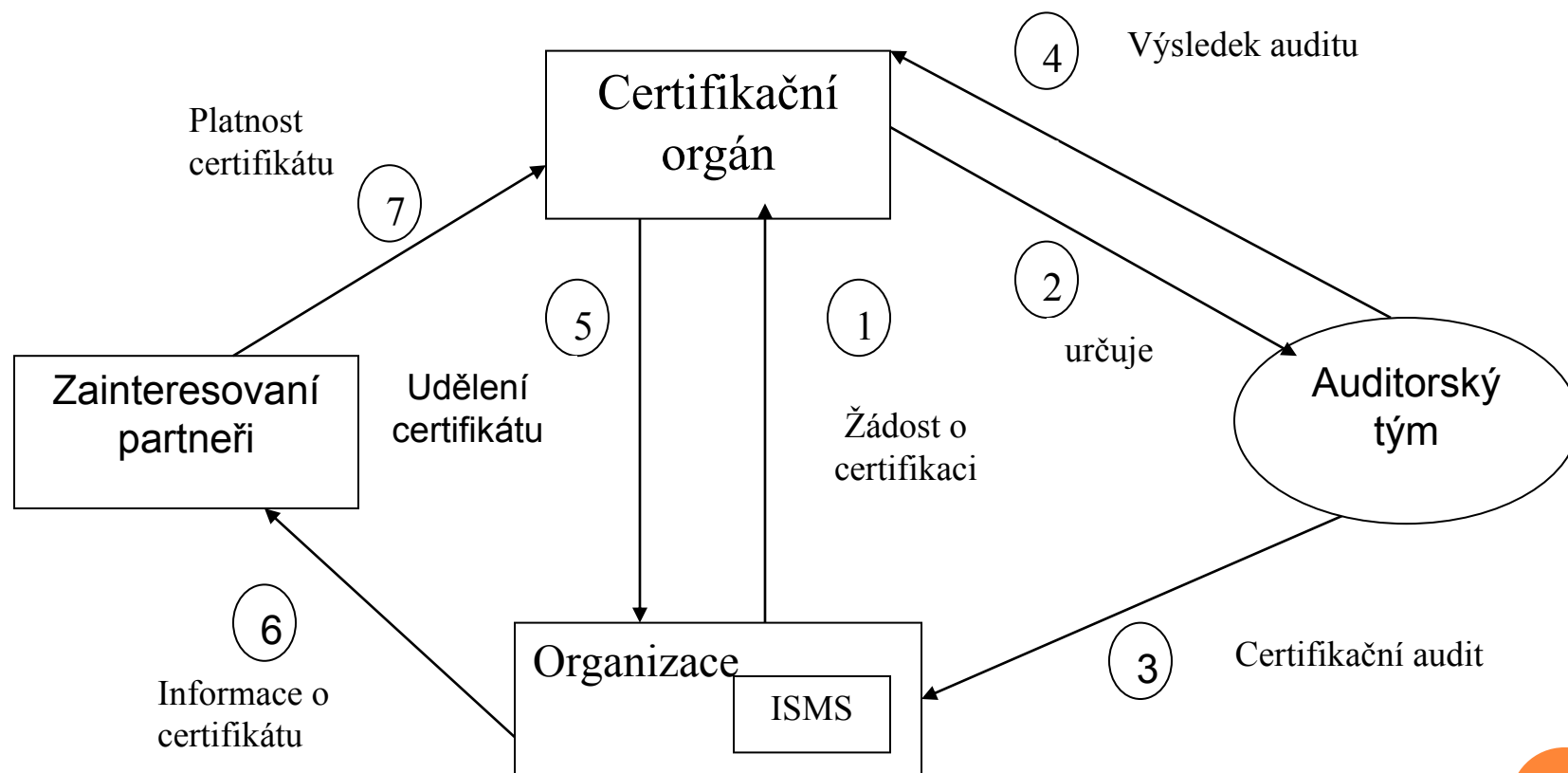


# OBSAH AUDITORSKÉ ZPRÁVY (POKR.)

- Doplnkové údaje:
  - Plán auditu
  - Seznam lidí, kteří spolupracovali na straně zákazníka s auditory
  - Přehled realizovaných akcí/procesů auditu a případné okolnosti, které vedly ke snížení spolehlivosti závěrů auditu.
  - Potvrzení o tom, že bylo dosaženo definovaných cílů auditu.
  - Přehled oblastí, které byly zahrnuty v plánu a nebyly auditovány
  - Popis nevyřešených rozdílných názorů mezi auditorským týmem a auditovanou stranou.
  - Přehled doporučení ke zlepšení, pokud byly součástí cílů auditu.
  - Odsouhlasený plán realizace nápravných doporučení (pokud existuje).
  - Prohlášení o zachování mlčenlivost o získaných údajích.
  - Seznam příjemců auditorské zprávy a způsob jejího doručení.



## 4. CERTIFIKAČNÍ AUDIT INFORMAČNÍ BEZPEČNOSTI

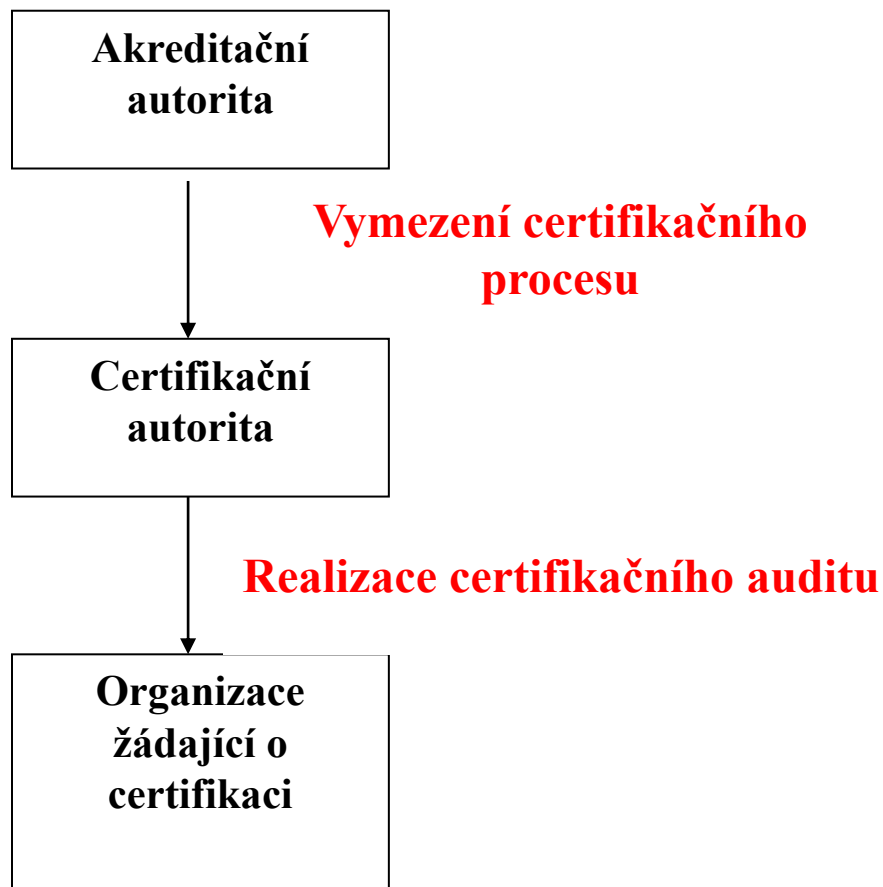


# NORMY CERTIFIKAČNÍHO AUDITU BEZPEČNOSTI

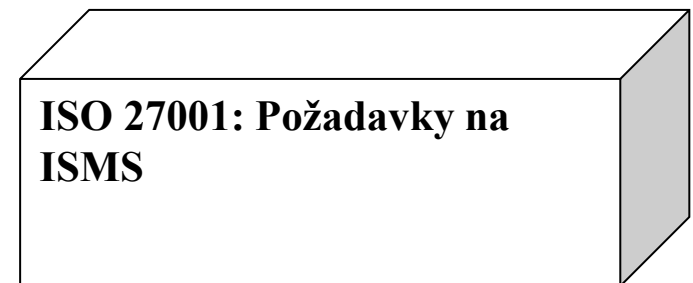
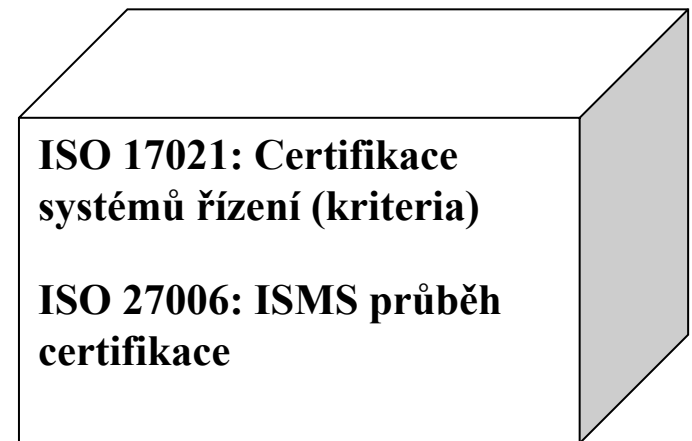
- Základ:
  - ISO 27006:2007,
  - ISO/IEC 17021 a
  - ISO/IEC 27001:2005
- **ISO 27006** Informační technologie- Bezpečnostní techniky –požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
  - poskytuje doporučení zejména akreditovaným certifikačním autoritám, týkající se průběhu certifikace ISMS
  - Cíl: „specifikovat obecné požadavky, které by měly být dodržovány akreditovanými autoritami při certifikacích/registracích ISMS“
  - doplňuje normu ISO/IEC 17021 pro oblast certifikace ISMS
- **ISO/IEC 17021** „Posuzování shody – Požadavky na orgány provádějící audit a certifikaci systémů managementu“
  - definuje kriteria pro ty organizace, které poskytují služby auditu a certifikace obecně na systém řízení
- **ISO/IEC 27001: 2013** Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky
  - Základním dokumentem pro certifikační audit bezpečnosti informačních systémů
  - Certifikační audit jako závěrečná etapa dlouhodobého procesu zavádění systému řízení informační bezpečnosti (ISMS)



# VAZBY MEZI NORMAMI



## POUŽITÉ NORMY



# POSTUP CERTIFIKAČNÍHO AUDITU



# AKTIVITY PŘEDCHÁZEJÍCÍ AUDIT

- **Analýza současného stavu zajišťování bezpečnosti informací**  
Posouzení a dokumentování výchozího stavu, upřesnění dalšího postupu.
- **Uspořádání úvodního semináře o ISMS**  
Pro vedení společnosti a vybrané pracovníky pro objasnění smyslu ISMS a jednotlivých požadavků, způsobu realizace praktických důsledků.
- **Poradenství v procesu vytváření a dokumentování ISMS**  
Konzultační spolupráce v oblasti identifikace, ocenění a klasifikace informačních aktiv, stanovení úrovně bezpečnosti, stanovení rozsahu aplikovatelnosti, určení způsobu řízení rizik v oblasti informací a zpracovávání dokumentace.
- **Kurz interních auditorů ISMS**  
Příprava na provádění interních auditů ISMS.
- **Poradenství v procesu implementace ISMS**  
Průběžné prověřování stavu zavádění ISMS v praxi, konzultace při odstraňování nedostatků a optimalizace podnikových procesů týkajících se bezpečnosti informací
- **Vstupní audit pro certifikační řízení (poradenský předcertifikační)**  
Prověření celkového stavu ISMS a posouzení jeho certifikovatelnosti v plánovaném termínu.
- **Příprava na certifikační audit**  
Pomoc při odstraňování zjištěných odchylek a doladování ISMS.



# PRIMÁRNÍ – ÚVODNÍ CERTIFIKACE



# PRIMÁRNÍ – ÚVODNÍ CERTIFIKACE

## 1. Příprava projektu certifikace

- vyjasnění detailních potřeb zákazníka
- projednání a uzavření smlouvy
- vystaví se na žádost potvrzení o probíhajícím procesu zavedení systému řízení s předpokladem ukončení projektu v odpovídajícím termínu - možné předložit např. při výběrových řízeních

## 2. Vstupní analýza

- poznat způsob práce organizace, klienty, jaká je představa kvalitních podnikatelských procesů, klíčové bezpečnostní dokumenty organizace
- možné zúžit záběr auditu vytipováním 3 – 5 oblastí, na které se audit zaměří (struktura systému řízení)
- Zpracování zprávy a její prezentace vrcholovému vedení





# POSTUP CERTIFIKAČNÍHO AUDITU (POKR.)

## 3. Přezkoumání dokumentace

- Standardy definují povinné náležitosti dokumentace, ne však pro vše
- Dokumentace má sloužit zákazníkovi (stručná, jasná, lehce aktualizovatelná)
- Zpracovává auditor (ev. poradce) společně s odpovědným pracovníkem
- Přezkoumání dokumentace může být provedeno před nebo společně s úvodní návštěvou. Na základě výše uvedeného se navrhuje rozsah certifikace a program auditu.
- Poradce poskytuje všem odpovědným pracovníkům inspirační dokumenty, které mohou pomoci při přípravě dokumentů, zdroj např. portál [www.eiso.cz](http://www.eiso.cz)
- Zpracování zprávy hodnotící dokumentaci a připravenost organizace na certifikaci



# POSTUP CERTIFIKAČNÍHO AUDITU (POKR.)

## 4. Zkušební provoz

- většina kvalitních certifikačních společností vyžaduje 2 až 3 měsíční „zkušební“ provoz systému řízení
- poradce společně se jmenovanými pracovníky provede interní audit, při kterém prověří to, zda připravená dokumentace vyhovuje praxi a zda jsou splněny všechny požadavky příslušné normy
- nedostatky jsou zaznamenány, jsou stanoveni odpovědní pracovníci a termíny jejich odstranění
- druhý interní audit, který kontroluje odstranění problémů, které vznikly při předcházejícím auditu
- výstupní audit, který je možno kombinovat s předcertifikačním auditem, který provádí poradce společně s certifikačním auditorem



# POSTUP CERTIFIKAČNÍHO AUDITU (POKR.)

## 5. Certifikační audit

- neformální rozhovory, zkoušky a pozorování systému v činnosti
- hodnotí se stupeň shody systému řízení s požadavky dané normy a také stav systému v jednotlivých oblastech zaměření
- přítomen poradce, který v případě problémů nebo nepochopení komunikuje s certifikačním auditorem
- práce poradce nekončí certifikačním auditem, ale až vydáním certifikátu, to znamená, že poradce pomůže s nápravou případných problémů vzniklých při certifikaci.



# UDRŽOVÁNÍ CERTIFIKÁTU

## 6. Pravidelné audits

- certifikát má životnost 3 roky
- plán pravidelných auditů v průběhu tříleté periody
- doporučuje se alespoň jeden takový audit ročně

## 7. Audit pro obnovení certifikace (recertifikační audit)

- prodloužení prostřednictvím recertifikačního auditu




# ORGANIZACE POSKYTUJÍCÍ SLUŽBU AUDITU INFORMAČNÍ BEZPEČNOSTI

- CIS - Certification & Information Security Services s centrálou ve Vídni
  - Mezinárodně uznávaná
  - komplexita služeb a specializací na problematiku ISO 27001 (ISMS - systém řízení bezpečnosti informací ) včetně ICT a ISO 20000 (management IT služeb)
- V České republice existuje celá řada firem, které službu certifikačního auditu bezpečnosti mají ve svojí nabídce



# POČET VYDANÝCH CERTIFIKÁTŮ ISO 27001

ZDROJ: [HTTP://WWW.ISO27001CERTIFICATES.COM/](http://www.iso27001certificates.com/)

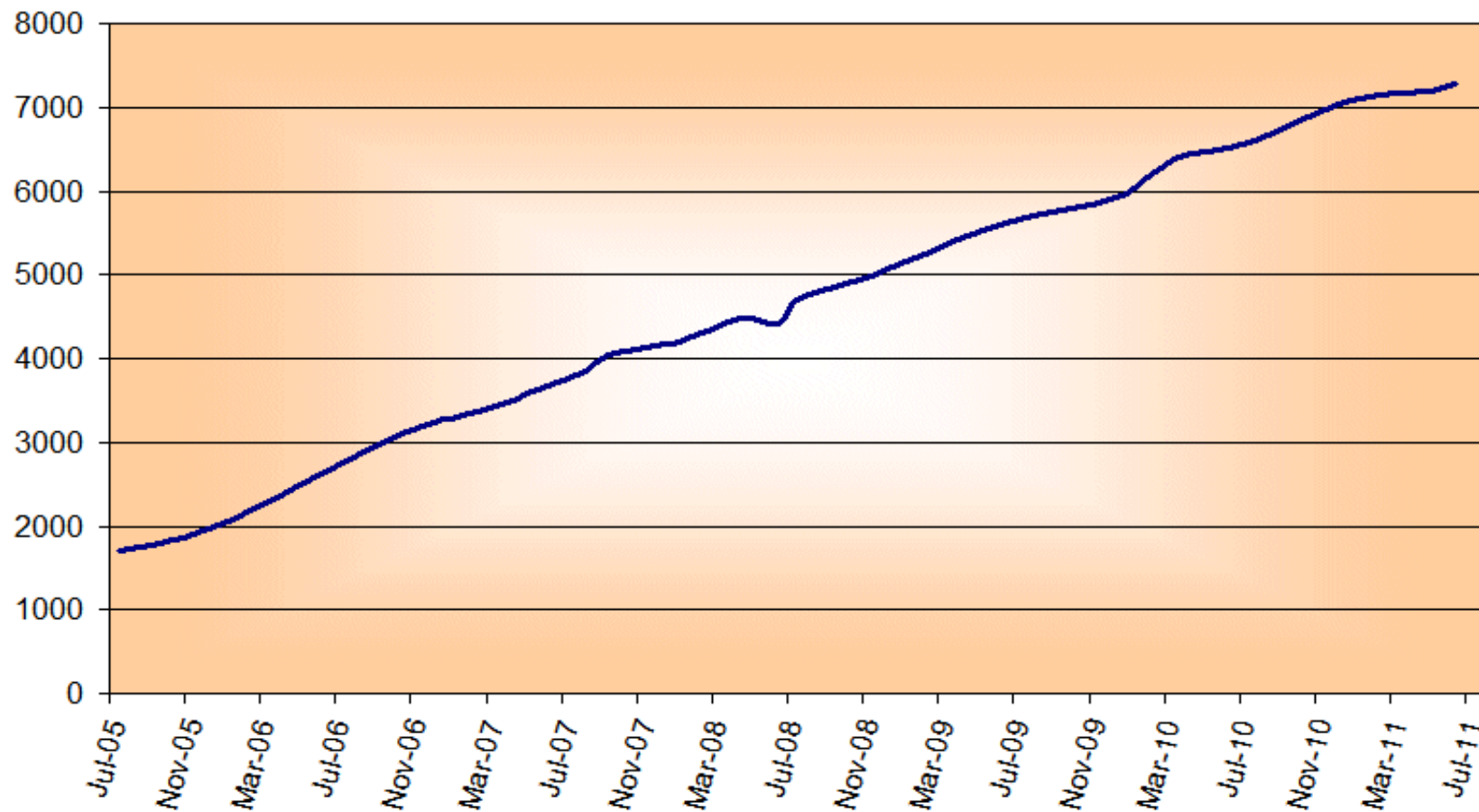


Japan	4152	Netherlands	24	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
Czech Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Hungary	71	Russian Federation	14	Macedonia	2
Malaysia	66	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2
Greece	50	Canada	10	Armenia	1
Ireland	48	Norway	10	Bangladesh	1
Austria	42	Sweden	10	Belarus	1
Turkey	35	Switzerland	9	Bolivia	1
Turkey	35	Bahrain	8	Denmark	1
France	34	Peru	7	Estonia	1
Hong Kong	32	Chile	5	Kyrgyzstan	1
Australia	30	Egypt	5	Lebanon	1
Singapore	29	Oman	5	Moldova	1
Croatia	27	Qatar	5	New Zealand	1
Slovenia	26	Sri Lanka	5	Sudan	1
Mexico	25	South Africa	5	Uruguay	1
Slovakia	25	Dominican Republic	4	Yemen	1
Brazil	24	Morocco	4	<b>Total</b>	<b>7940</b>

# POČET VYDANÝCH CERTIFIKÁTŮ V PRŮBĚHU LET 2005 - 2011;

ZDROJ: [HTTP://WWW.ISO27001SECURITY.COM/HTML/27001.HTML](http://www.iso27001security.com/html/27001.html)

**Number of ISO/IEC 27001 (or equivalent) certificates**



# CENY CERTIKAČNÍHO AUDITU

- Cena stanovena dohodou. Výši ceny zpravidla ovlivňují následující faktory:
  - Velikost a organizační členění organizace,
  - lokální umístění organizace/ počet poboček a jejich rozmístění,
  - předmět a rozsah výstavby systému managementu,
  - rozsah pomoci **poradcem při výstavbě systému managementu.**





# CENY CERTIFIKAČNÍHO AUDITU (ISO 9001 BEZ DPH 19%)

Rok	2007	2008	2009	2010	2011
		1.	2.		
Počet zaměstnanců	Certifikační audit	Dozorový audit	Dozorový audit	Recertifikační audit	1. Dozorový audit
1 – 10	33 500	10 500	10 500	21 500	10 500
11 - 25	48 000	14 500	14 500	31 500	14 500
26 - 45	62 500	19 000	19 000	40 000	19 000
46 - 65	82 000	25 000	25 000	52 500	25 000
66 - 85	96 500	29 000	29 000	62 500	29 000
86 - 125	115 000	33 000	33 000	72 000	33 000

# PŘEHLED CEN CERTIFIKAČNÍCH AUDITŮ

- Firma do 10 zaměstnanců s jednou pobočkou
- Ceny se liší podle předmětu podnikání o 20%
- Podle certifikačních orgánů o 30%
- Kontrolní audit 40% ceny certifikačního auditu
- Cena recertifikační = certifikační

Pozn. ISO 14001 - Systém environmentálního managementu (EMS)

Fáze auditu	ČSN 9001	ČSN 14001
Předaudit	8000	7000
Prověrka dokumentace	6000	5000
Audit na místě	18000	18000
Auditní zpráva	4000	4000
Registrace, certifikace	2000	2000
Celkem	38000	36000



# ŽÁDOST O CERTIFIKACI



Název společnosti:		IČ:
		DIČ:
Sídlo společnosti:		Tel.:
		Fax:
		E-mail:
Adresa provozovny: (Pozn.: vyplňte pouze v případě není-li shodná se sídlem společnosti)		Korespondenční adresa: (Pozn.: vyplňte pouze v případě není-li shodná se sídlem společnosti)
Banka:	Číslo účtu:	
Vedoucí firmy:		
Pracovník zmocněný pro styk s certifikačním orgánem:		Tel.:
		E-mail:
Počet pracovníků, na něž se vztahuje certifikace:	Předpokládaný termín certifikačního auditu:	
Slovní návrh oboru, který chcete mít na certifikátu (uved'te co nejpřesněji): ..... ..... ..... .....		
Předmět certifikace (zaškrtněte podle vašich požadavků): SMJ dle normy ČSN EN ISO 9001:2001 SMJ dle normy ČSN EN ISO 9001:2001 ve spojení s ČSN EN ISO 3834-2 EMS dle normy ČSN EN ISO 14001:2005 BOZP dle normy ČSN OHSAS 18001:2008 ISMS dle normy ČSN ISO/IEC 27001:2006 Jiné (např. SJ – PK, prosíme upřesnit) .....		
Návrh provedení certifikátu (zaškrtněte podle vašich požadavků):		
Certifikáty kombinované („integrovane“) (platí pouze v případě certifikace více systémů managementu) ANO	Certifikáty v Čj ANO	
Certifikáty pro každý systém odděleně (platí pouze v případě certifikace více systémů managementu mimo certifikaci dle ISO 3834-2) ANO	Jiná jazyková mutace (V ceně již zahrnuty 2ks Čj. Ostatní jazyky a počet ks nad rámec 2 je za příplatek). ANO, uveďte jaká:	

<b>Prvek normy 4 – SYSTÉM MANAGEMENTU BEZPEČNOSTI INFORMACÍ</b>			
Je ustaven, zaveden, udržován a monitorován ISMS?	ANO	NE	Pozn.:
Je určen rozsah a hranice ISMS?	ANO	NE	Pozn.:
Je definována politika ISMS?	ANO	NE	Pozn.:
Je zpracována metodika analýzy rizik?	ANO	NE	Pozn.:
Jsou vybrány cíle a opatření z přílohy a normy?	ANO	NE	Pozn.:
Je k dispozici Prohlášení o aplikovatelnosti?	ANO	NE	Pozn.:
Je formulován a zaveden plán zvládání rizik?	ANO	NE	Pozn.:
Provádí organizace přezkoumání účinnosti ISMS?	ANO	NE	Pozn.:
Provádí organizace interní audity ISMS?	ANO	NE	Pozn.:
Obsahuje dokumentace ISMS jednotlivé dokumenty dle požadavků písm. a) až i) čl.3.1 normy?	ANO	NE	Pozn.:
Je zpracován účinný a dokumentovaný postup pro řízení dokumentů a záznamů?	ANO	NE	Pozn.:
<b>Prvek normy 5 – ODPOVĚDNOST VEDENÍ</b>			
Jsou stanoveny role, povinnosti a odpovědnosti v oblasti ISMS?	ANO	NE	Pozn.:
Je zajištěna odborná způsobilost pracovníků včetně odpovídajících školení a udržování příslušných záznamů?	ANO	NE	Pozn.:
<b>Prvek normy 6 – INTERNÍ AUDITY ISMS</b>			
Je zajištěno provádění interních auditů ISMS včetně dokumentovaného postupu a odborné způsobilosti auditorů?	ANO	NE	Pozn.:
<b>Prvek normy 7 – PŘEZKOUMÁNÍ ISMS VEDENÍM ORGANIZACE</b>			
Je zajištěno provádění přezkoumání ISMS alespoň 1x ročně včetně vyhodnocení možnosti zlepšení a příslušných záznamů?	ANO	NE	Pozn.:
Zahrnují vstupy pro přezkoumání požadavky uvedené v čl. ) až i) ?	ANO	NE	Pozn.:
Zahrnují výstupy z přezkoumání požadavky uvedené v čl. ) až e) ?	ANO	NE	Pozn.:
<b>Prvek normy 8 – ZLEPŠOVÁNÍ ISMS</b>			
Je zpracován dokumentovaný postup nápravných a preventivních opatření?	ANO	NE	Pozn.:
Udržujete záznamy o povaze neshod a přijatých opatření k nápravě?	ANO	NE	Pozn.:



## 5. OBECNÝ AUDIT INFORMAČNÍ BEZPEČNOSTI

- Rozdíl od certifikačního auditu: hlavním kritériem hodnocení není konkrétní ISO norma, ale bezpečnostní politika dané organizace
- Důležité primární hledisko dekompozice auditu:
  - Hledisko prvků bezpečnosti: důvěrnost, dostupnost, integrita, prokazatelnost, pravost, spolehlivost
  - Hledisko komponent informatiky: hardware, software, infrastruktura, data, dokumentace,
  - Hledisko procesů a služeb informatiky (respektují současně kontrolní cíle a životní cyklus služeb: plánování, návrh a pořízení, implementace a testování, provozování a údržba, monitorování a zlepšování; např. podle ITIL nebo COBIT).



# DRUHY OBECNÝCH AUDITŮ (1)

1. **Personální audit informační bezpečnosti (security assurance)** zahrnuje prověření bezpečnostní politiky a jejích procedur, školení v oblasti bezpečnosti a celkové povědomí zaměstnanců o informační bezpečnosti, správu systému řízení informační bezpečnosti, fyzickou bezpečnost a personální bezpečnost (postupy pro přijímání správců systému, oddělení odpovědností).



## DRUHY OBECNÝCH AUDITŮ (2)

### **2. Technologický audit informační bezpečnosti**

klade důraz na prověření efektivnosti pořizování informačních technologií (testování produktů, certifikace), ochrany sítí (enkrypce, monitorování), ochrany systémů před externím prostředím (firewally, IDS – Intrusion Detection Systems), vstupů do systémů ( identifikace, autorizace, autentizace).



## DRUHY OBECNÝCH AUDITŮ (3)

- 3. Provozní audit informační bezpečnosti** se zaměřuje na denní aktivity provozování systémů, např. řízení změn, instalace bezpečnostních záplat, aktualizace antivirových programů, sledování přístupů do systémů, monitorování a reakce na aktuální hrozby a útoky, zálohování a obnovu systémů





# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI (VAZBA NA ANALÝZU RIZIK)

## 1. Definování rozsahu auditu: vytvoření seznamu aktiv a bezpečnostního perimetru

- Perimetr- oblast společnosti obsahující aktiva, která je třeba chránit (ev. cíl počítačových narušitelů)
- Příklady aktiv:

počítače a laptopy, routery a síťová zařízení, tiskárny, kamery digitální i analogové s citlivými záznamy, data, smartphones/PDA, VoIP telefony, IP PBX, návazné servery, telefonní a VoIP záznamy, e-mail, logy se záznamy denních aktivit zaměstnanců, webové stránky, zvláště ty, které vyžadují od zákazníků detailní data a ty, které jsou propojeny s databázemi, webový server, bezpečnostní kamery, přístupové karty zaměstnanců, vstupní místa (např. scannery kontrolující vstup do místnosti)



# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI (POKR.)

## 2. Vytvoření seznamu hrozeb

- *Hesla pro přístup do systému (počítačů a sítí):* existuje log pro záznam všech lidí majících hesla? Jak je bezpečný ACL (Access Control List) a jak bezpečná jsou hesla?
- *Fyzická aktiva:* mohou být počítače a laptopy přemístěny zaměstnanci nebo návštěvníky mimo perimetr?
- *Záznamy na fyzických nosičích:* existují a jsou zálohovány?
- *Datové zálohy:* jaké zálohy existují, jak se provádějí, kde se ukládají a kdo je řídí?
- *Logy přístupu k datům:* zaznamenává se každý přístup k datům? Kdo to řídí?
- *Přístup k citlivým datům zákazníků (např. informacím o kreditních kartách):* Kdo má přístup? Jak se přístup kontroluje? Je možný tento přístup z vnějšku organizace?
- *Přístup k seznamům zákazníků:* Umožňuje webová stránka přístup do databáze klientů? Může být tento přístup zneužit?
- *Volání na velké vzdálenosti:* Jsou tato volání zakázána, nebo ne? Mají být zakázána?
- *Emaily:* Filtrují se spamy? Jsou zaměstnanci informováni o tom, jak identifikovat a zacházet se spamy a phishing emaily? Existuje ve společnosti politika, že odchozí emaily nesmí obsahovat určité typy odkazů?

# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI

## 3. **Předpověď budoucího vývoje**

- Mapování minulých hrozeb
- Předpověď budoucích (odborná literatura, výzkumy, specifika sektoru podnikání)

## 4. **Přiřazení priorit aktivům a určení jejich slabin**



# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI (POKR.)

## 5. Implementování kontrol přístupu do sítě

- Kontroly přístupu do sítě (NAC – Network Access Controls) prověřují každého uživatele, který se chce připojit k síti
- Součástí efektivního NAC je
  - seznam uživatelských práv (ACL – Access Control List), který určuje, kdo má právo přístupu k jakým informačním zdrojům (autorizace)
  - další opatření, jako je enkrypce, elektronický podpis, ověřování IP adres, uživatelských jmen a prověřování cookies webových stránek.

Pozn.:

"Cookie" je malý textový soubor, který lze použít například ke sběru informací o aktivitě na webovém serveru. Některé cookies a jiné technologie mohou sloužit k získání osobních údajů, které webový uživatel dříve poskytl. Většina webových prohlížečů umožňuje řídit zpracování cookies, včetně možnosti jejich povolení, zákazu nebo odstranění.



# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI

## 6. Implementování ochrany proti narušení

- > systémy pro prevenci narušení (v angličtině IPS – Intrusion Prevention Systems) chrání aktiva před útoky z vnějšku organizace
- > nejčastější formou IPS jsou firewally druhé generace: první generace - obsahové filtry, navíc obsahují filtry četnosti
- > provádějí analýzu vlastností provozu webu nebo sítě a reagují na mimořádné situace



# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI (POKR.)

## 7. Implementování kontrol identity a přístupu

- › Řízení identity a přístupu (IAM – Identity and Access Management) zahrnuje soubor opatření umožňujících kontrolu přístupu uživatelů k určitým informačním zdrojům (identifikace a autentizace)



# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI (POKR.)

## 8. Vytváření záloh

- *Zálohy v místě („Onsite“ zálohy) organizace:*
  - Data na paměťových nosičích (např. přenositelné hard disky) v protipožárně chráněných místnostech
  - data na hard discích v rámci sítě, ale měly by být oddělené od okolního světa pomocí tzv. demilitarizované zóny.
- *Zálohy mimo organizaci (Offsite zálohy) mimo budovu organizace pro případ hrozeb působení prostředí*
  - fyzickým převozem
  - přes Internet pomocí VPN (Virtual Private Network)
- *Bezpečný přístup k zálohám, např. pomocí různých klíčů, karet, hesel*
- **DMZ – demilitarizovaná zóna je komplexnější řešení, plní roli firewallu, založené na použití určitého "mezistupně" mezi oběma světy, které mají být řízeným způsobem propojeny - tedy mezi chráněnou privátní sítí, a nechráněným Internetem.**



# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI (POKR.)

## ◉ *Plánování záloh:*

- > maximální automatizace
- > stanovení parametrů zálohování:
  - **Bod obnovy – Recovery Point Objective (RPO)**, tj. bod v čase, ke kterému musejí být data aplikace obnovena (časový úsek od okamžiku výpadku chodu aplikace do minulosti, ke kterému musejí být data aplikace obnovena, jak daleko do minulosti můžeme o data v případě havárie přijít). Např. zálohujeme každý den. Potom v případě havárie můžeme přijít o data za posledních 24 hodin.
  - **Doba obnovy – Recovery Time Objective (RTO)**, tj. doba, která uplyne od bodu selhání do doby obnovy dat a uvedení aplikace do stavu on-line (nejdelší časový úsek, po který si můžeme dovolit aplikaci nevyužívat a věnovat se obnově její funkčnosti (např. 48 hodin).





# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI

## 9. Ochrana emailu a filtrování

- > šifrování citlivých emailů posílaných zaměstnancům nebo zákazníkům mimo interní síť,
- > využívání steganografie v kombinaci se šifrováním,
- > neotevírat neznámé emaily a přílohy.
- > **Steganografie je metoda ukrytí citlivých dokumentů jejich zakomponováním do digitálního obrázku. Tajná zpráva může být zakódována na místo nepodstatného šumu v souborech se zvuky, obrázky, videem a podobně.**



# TECHNOLOGICKÝ AUDIT INFORMAČNÍ BEZPEČNOSTI

## 10. Fyzická ochrana

- ◉ vloupání se do kanceláře – instalace detekčních systémů (kamery),
- ◉ zcizení laptopu – enkrypcie pevného disku (např. Microsoft Encrypt File System – EFS),
- ◉ ukradení smart telefonů a PDA - speciální služby, které při ukradení telefonu bez znalosti autorizačních kódů zařízení zablokují, vymažou uložená data a telefon začne vydávat ostrý hlasitý signál, po obnově funkčnosti se do telefonu zpět nahrají data ze vzdáleného serveru  
?? v ČR??
- ◉ děti a domácí mazlíčci při práci doma – vhodná politika pro domácí plnění pracovních povinností (zamezení neautorizovaného přístupu),
- ◉ interní sledování webových stránek ( nevhodné klikání na reklamy může vést k zablokování účtu) – školení zaměstnanců a blokování



# 6. NÁSTROJE AUDITU INFORMAČNÍ BEZPEČNOSTI

## ○ Klasické (checklisty)

## ○ Automatizované:

- Nástroje pro odhalování slabín sítí
- Skenování portů
- Nástroje pro audit sítí
- Testování lokálních slabín (Host-based audit)
- Nástroje na prolomení hesel (password cracking)
- Forenzní nástroje
- Analýza logů
- Nástroje pro audit programového vybavení
- Testování webových aplikací
- Audit procesů

## ○ Hledisko dostupnosti:

- Volně dostupné (open source)
- komerční



# NÁSTROJE VOLNĚ DOSTUPNÉ (1)

- ◉ Nástroje pro odhalování slabin sítí
  - > Nesprávná konfigurace, nedůsledné záplaty, upgrady
  - > **Nessus**
  - > **SATAN** (Administrator's Tool for Analyzing Network)
- ◉ Skenování portů
  - > činnost, při které se propojují různé porty s daným systémem a určuje se, který odpovídá na požadavek
  - > **Nmap**: mapuje síť a zjišťuje jaké stroje jsou k ní připojeny a jaké operační systémy a síťové služby na nich běží; „white hat“ nástroj pro vnitřní potřeby, ale i po hledání slabin zvnějšku



# NÁSTROJE VOLNĚ DOSTUPNÉ (2)

## ◉ Nástroje pro audit sítí

- > testování bezpečnosti síťových prvků, jako např. firewallů a routerů, stejně jako testování síťových parametrů operačních systémů serverů
- > Testování dvou různých aspektů:
  - obecná konfigurace síťových prvků
  - kontroly přístupů, které se využívají
- > *Hping2* (<http://www.hping.org/>).
- > *Firewalk*
- > *Testování Microsoft Windows (protokol NetBIOS): Enum od Bindview, NAT*



# NÁSTROJE VOLNĚ DOSTUPNÉ (3)

## ○ Testování lokálních slabin (Host-based audit)

- testování lokálních zranitelností (host-based audit) zahrnuje skenování a identifikaci nezáplatovaných a chybně nakonfigurovaných lokálních systémů
- komplexnější než nástroje pro odhalování síťových slabin, protože mají lepší přístup k informacím systému
- prověřování slabých autorizací u kritických souborů a adresářů, hesel apod.
- *COPS, Tiger*

## ○ Nástroje na prolomení hesel (password cracking)

- Slovníkový útok (dictionary attack): nástroje mají uložený slovník (wordlist), každý výraz ze slovníku zašifrují a vzniklý hash porovnávají s daty nalezenými v souboru hesel systémů
- Útok hrubou silou (brute force): využívají permutací čísel, písmen a zvláštních znaků a zkouší prolomit heslo kombinací všech možných znaků
- *Alec Muffet, John the Ripper*



# NÁSTROJE VOLNĚ DOSTUPNÉ (4)

## ○ Forenzní nástroje

- analyzují systém, který mohl být napaden
- systém se audituje off-line a zkoumá se, kdo a jakým způsobem ho mohl ohrozit
- pro výzkumné účely i v rámci soudních řízení

## ○ *TCT (The Coroner's Toolkit)*

## ○ *Lsof (LiSt of Open Fines)*, vyžaduje velké znalosti



# NÁSTROJE VOLNĚ DOSTUPNÉ (5)

## ○ **Nástroje pro analýzu logů**

- Nástroje pro vytváření logů mají všechny Unixové i Windows systémy
- Obsah velmi obsáhlý a je pracné ho auditovat, proto existují speciální utility

## ○ **Nástroje pro audit programového vybavení**

- pro rychlé vyhledání programových chyb
- **Rough Auditing Tool for Security (RATS)**





## NÁSTROJE VOLNĚ DOSTUPNÉ (6)

### ○ **Nástroje pro testování webových aplikací**

- testování internetových a intranetových stránek společnosti na obecné slabiny webových aplikací (skenovací nástroje)
- *Whisker*, vývoj omezen
- *Nikto*, využívá knihovnu testů z *Whisker*



# NÁSTROJE VOLNĚ DOSTUPNÉ (7)

## ○ Audit procesů

- podporují různé typy získávání informací, musí umožňovat ukládat dokumenty do databáze a porovnávat je s obsahem dokumentů s předchozího auditu
- **ASSET** (the Automated Security Self-evaluation Tool) je nástroj pro hodnocení bezpečnosti vytvořený organizací US National Institute of Standards and Technology (NIST)

