MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj pro inovace

Bezpečnost informací

seminář uchazečů o grantovou podporu MŠMT a řešitelů grantových projektů

Praha – 10.10. 2012

Ing. Miroslav Fryšar

Soudní znalec v oboru ochrany osob, majetku a informací, utajovaných informací a bezpečnosti informačních systémů

FSC® BEZPEČNOSTNÍ PORADENSTVÍ

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

Motto:

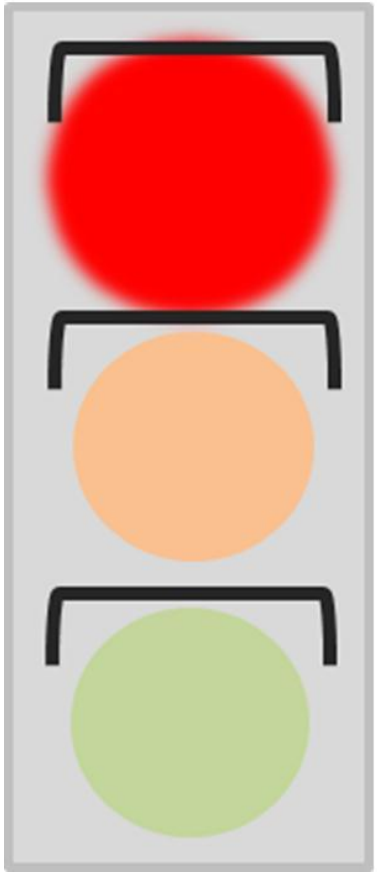
„Informace znamená všechno, za války jako v míru, politice jako ve finanční sféře“

Stefan Zweig

Mají-li informace tak zásadní význam v našem životě, pak si zaslouží, abychom jejich ochraně věnovali pozornost!

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Jak se ve vztahu k informacím chováme?



Jako děti !
Pádíme bez rozhlížení !
Pak pláčeme.

Pozdě !!!

Následky „informačního karambolu“ mohou být stejně bolestné, jako dopravní nehoda !

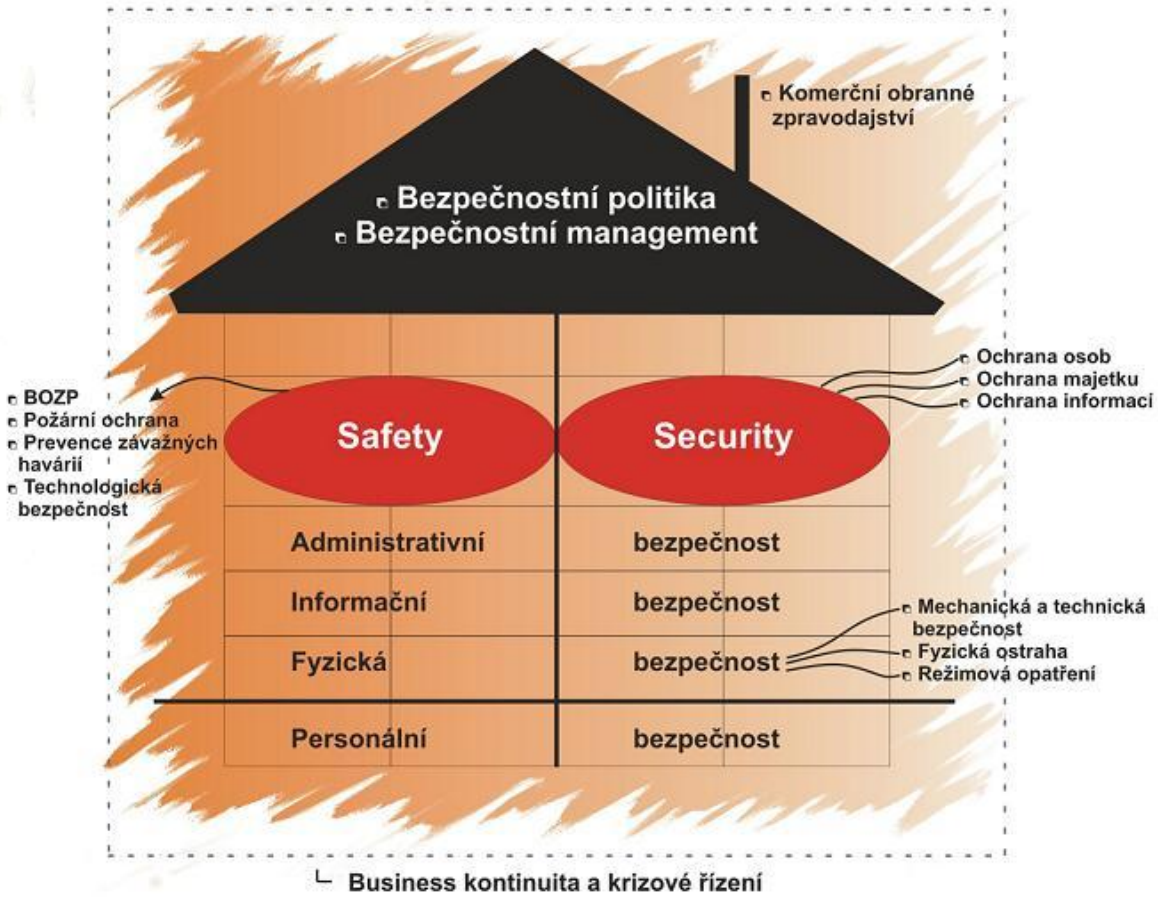
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Proč se zabývat informační bezpečností

— **Splnění požadavků právních norem**
(eliminace rizika **sankcí** ze strany orgánů státního dozoru)
— **Ochrana předmětu výzkumu** (před konkurencí, cizí mocí, obchodníky s informacemi ……)
— **Zajištění odolnosti/funkčnosti IS** (vnitřní / vnější útok)
— **Ochrana před kriminálními činy**
— **Naplnit obecný požadavek „odpovědného hospodáře“**

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Místo OI v systému bezpečnostních procesů organizace



O čem budeme hovořit

1. **Bezpečnost informací – obecný úvod do problematiky**
2. **Bezpečnost informací z pohledu subjektů účastných na grantových projektech**
3. **Závěr**

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

Proč právě já o těchto otázkách hovořím?

Ing. Miroslav Fryšar

Předseda představenstva
a generální ředitel
frysarm@fsc-ov.cz

F.S.C.®
BEZPEČNOSTNÍ PORADENSTVÍ

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

Organizace

- 13:30 - 15:30
- 13:30 - 14:45 přednáška
- 14:45 - 15:00 dotazy
- 15:00 – 15:30 vyplnění dotazníku

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

1.
Bezpečnost informací – obecný úvod do problematiky

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Bezpečnost – pracovní definice

Bezpečnost chápeme jako otevřený proces permanentní identifikace a analýzy rizik a práce s riziky, zaměřené na snížení rizikové zátěže na akceptovatelnou úroveň.

- ✓ **Preventivní opatření**
- ✓ **Represivní opatření**
- ✓ **Standardní bezpečnostní situace**
- ✓ **Nestandardní bezpečnostní situace (MU; KS; mobilizační potenciál BS)**

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Základní otázky, které si klademe

- ✓ **Co** chránit
- ✓ **Proti čemu** chránit
- ✓ **Jak** to chránit
- ✓ **Metody, prostředky, postupy** efektivní ochrany
- ✓ **Jak ochranu řídit v čase**

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Informace jako aktivum

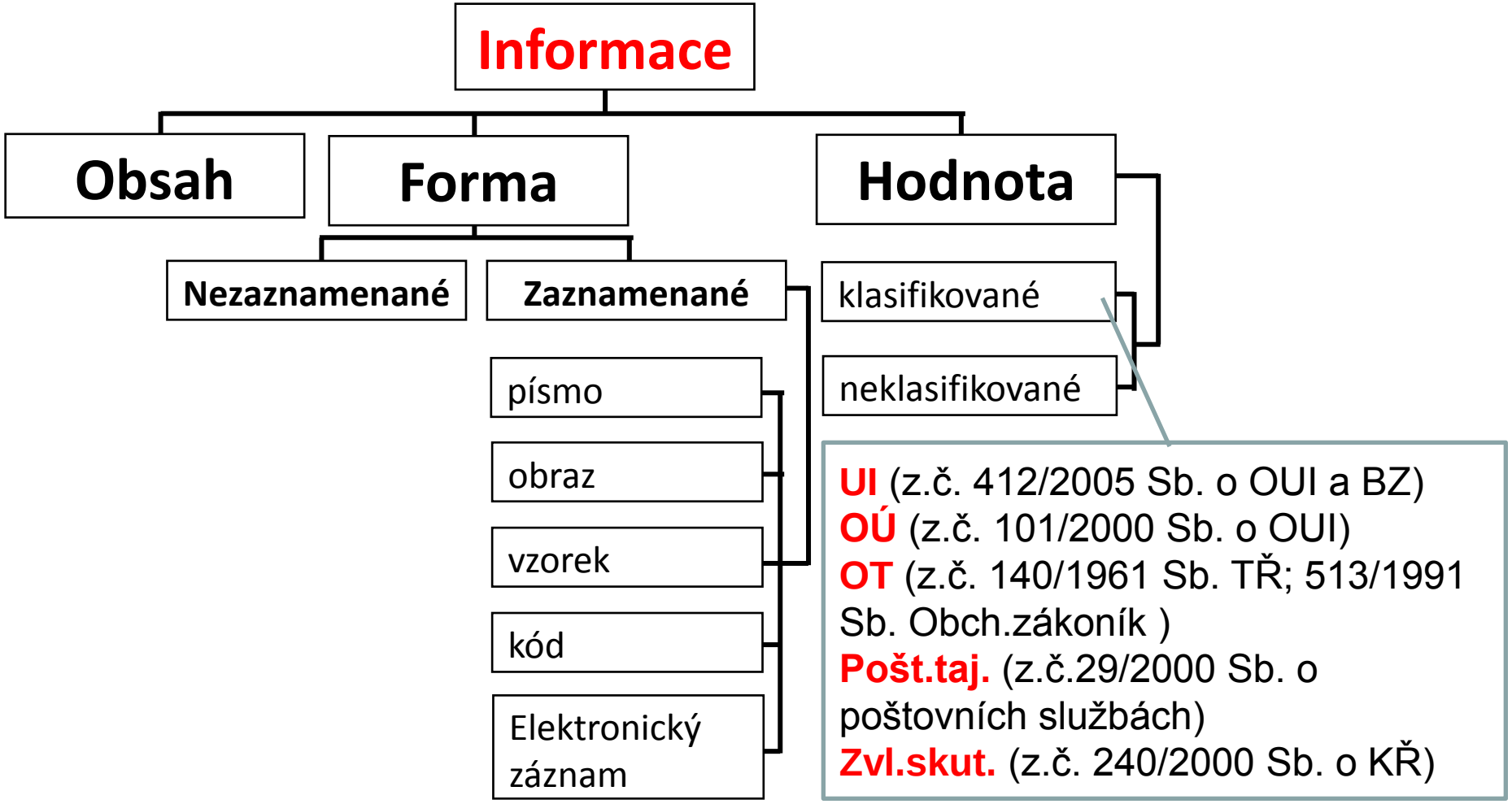
V nejobecnějším smyslu je informace chápána jako **údaj** o prostředí, o jeho stavu a procesech v něm probíhajících.

IN: WikipediE

Z čeho vychází konkrétní přístup k ochraně informací ?

- ✓ **Základní znaky informace**
- ✓ **Dislokace informačních aktiv**
- ✓ **Správa informačních aktiv**

Znaky informace



MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Dislokace a správa informačních aktiv

Dislokace aktiv

— Vlastní úložiště
— Outsourcované úložiště
— Cloud

Správa informačních aktiv

— Existuje definovaný systém
— Je stanovena adresná odpovědnost
— Je stav průběžně monitorován?
— Pracuje se s poznatky
— Je systém průběžně zdokonalován

Ochrana utajovaných informací

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění novelizovaného nařízení vlády č. 240/2008 Sb.

Utajovaná informace

informace v jakékoliv podobě, zaznamenaná na jakémkoliv nosiči, **označená v souladu s tímto zákonem**, jejíž vyzrazení nebo zneužití může způsobit **újmu zájmu České republiky** nebo může být pro tento zájem nevýhodné, a která je **uvedena v seznamu utajovaných informací**

Stupně utajení

Utajovaná informace se klasifikuje stupněm utajení: (§ 4, zákona č. 412/5005 Sb. o OUI)

a) **Přísně tajné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,
b) **Tajné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,
c) **Důvěrné**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,
d) **Vyhrazené**, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.

Systém OUI

Druhy zajištění ochrany utajovaných informací

§ 5 zákona č. 412/2005 o OUI

Personální bezpečnost

Hlava 2 zákona č. 412/2005 o OUI
Vyhláška č. 363/2011 Sb.

Průmyslová bezpečnost

Hlava 3 zákona č. 412/2005 o OUI
Vyhláška č. 405/2011 Sb.

Administrativní bezpečnost

Hlava 4 zákona č. 412/2005 o OUI

Vyhláška č. 433/2011 Sb.

Fyzická bezpečnost

Hlava 5 zákona č. 412/2005 o OUI
Vyhláška č. 454/2011 Sb.

Bezpečnost IS a KS

Hlava 6 zákona č. 412/2005 o OUI
Vyhláška č. 453/2011 Sb.

Kryptografická ochrana

Hlava 7 zákona č. 412/2005 o OUI
Vyhláška č. 432/2011 Sb.
V vyhláška č. 434/2011 Sb.

Prokazování oprávnění k přístupu

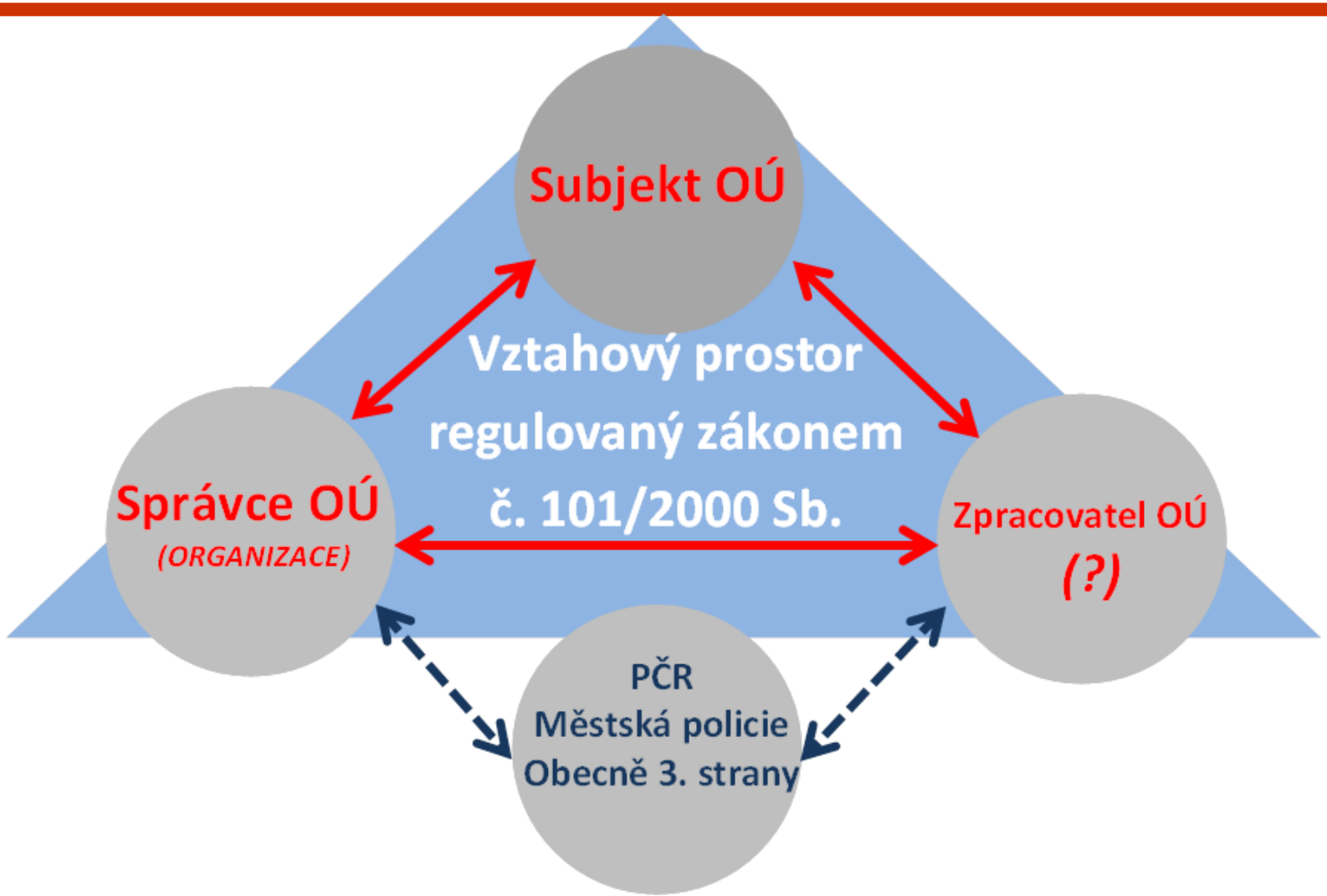
Subjekt	Stupeň utajení	
	Vyhrazené	Důvěrné – Přísně tajné
Fyzická osoba	**Oznámení** o splnění podmínek pro přístup k UI **Poučení**	**Osvědčení fyzické osoby**
Podnikatel	**Prohlášení** schopnosti zabezpečit ochranu utajovaných informací	**Osvědčení podnikatele**

Ochrana osobních údajů (1)

Právní normy:

- **Ústavní zákon číslo 2/1993 Sb.**, o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
- **Směrnice Evropského parlamentu a Rady 95/46/ES** o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- **Zákon číslo 101/2000 Sb.** o ochraně osobních údajů a o změně některých zákonů

Ochrana osobních údajů (2)

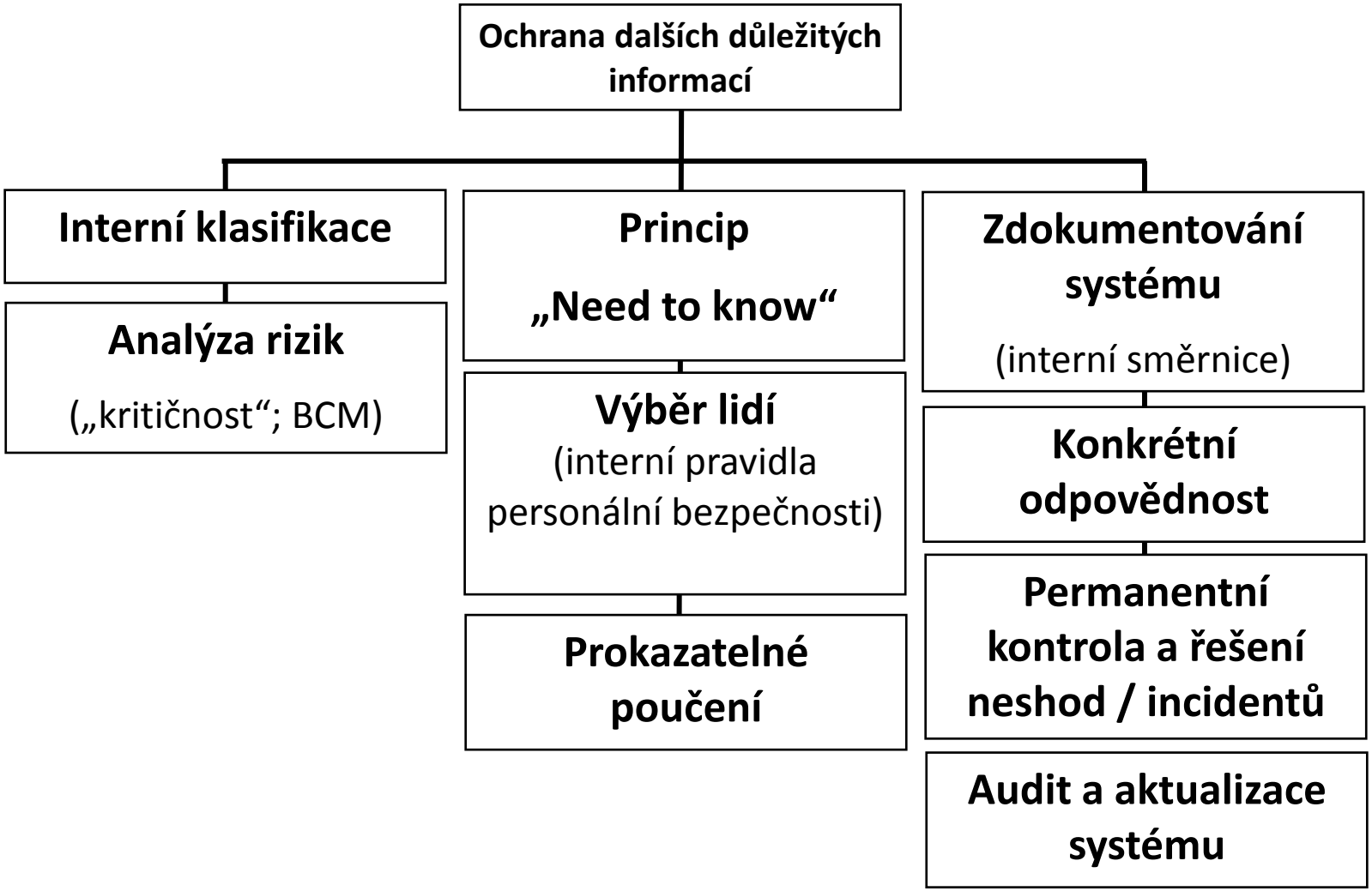


Zavedení a řízení systému OOÚ

- ❑ Vyhodnotit výskyt OÚ ve zpracování a klasifikovat je (**OÚ** / CÚ)
- ❑ Identifikovat hrozby

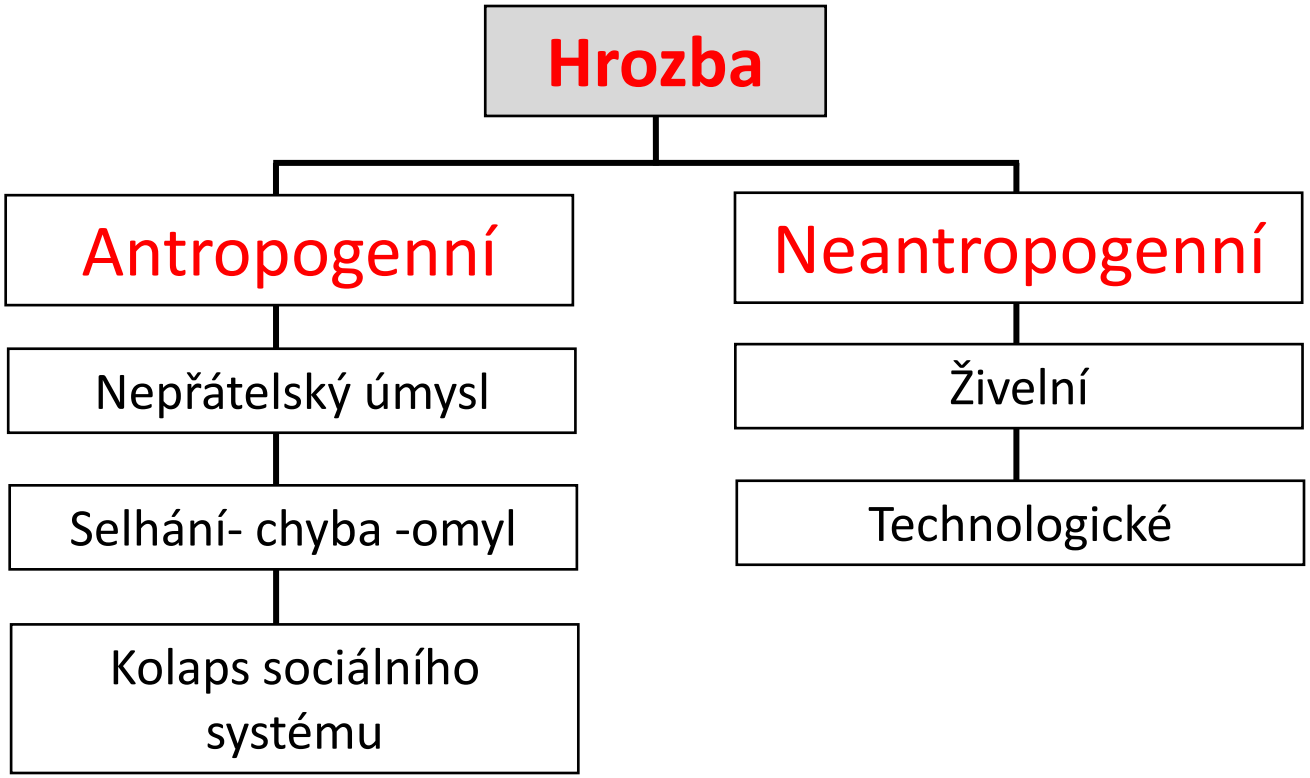
1. **Zpracovat analýzu rizik**
2. **Zdokumentovat přijatá technicko-organizační opatření OOÚ**
3. **Zpracovat „Směrnici pro ochranu osobních údajů “**
   - ❑ Prokazatelně seznámit dotčené osoby
4. CCTV se záznamem – splnit registrační povinnost
5. **Řídit systém ochrany OÚ**
   - ❑ Kontrolovat a posuzovat účinnost
   - ❑ Identifikovat změny podmínek
   - ❑ Přijímat opatření

Ochrana dalších důležitých informací



Proti čemu chránit (hrozba / riziko)

Hrozba – potenciální zdroj rizika



Proti čemu chránit (hrozba / riziko)

Riziko – potenciál naplnění hrozby

Ústředním problémem analýzy rizik je jejich operacionalizace.

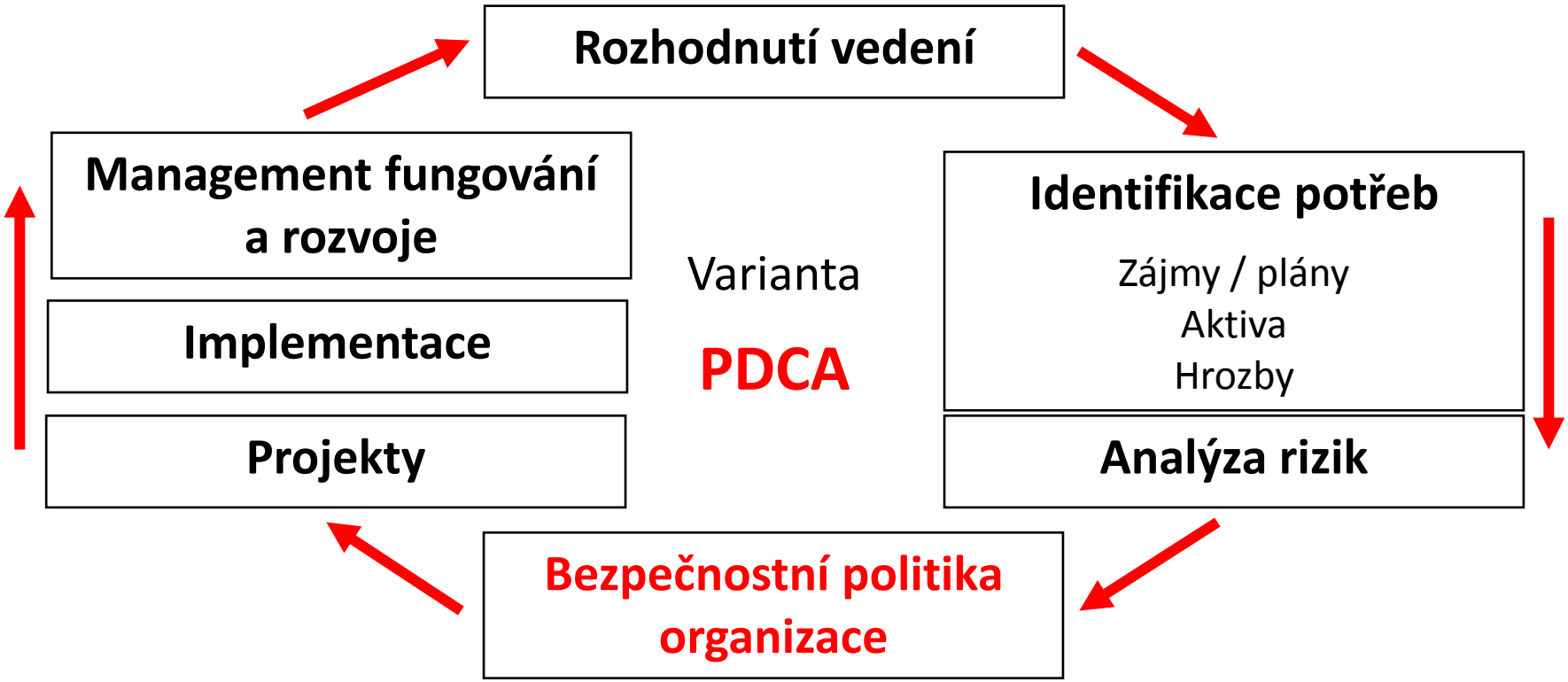
- ✓**Pojmová** (Např. „extrémní – vysoká – nízká – zanedbatelná“)
- ✓**Numerická**

Metody analýzy rizik (řada; princip „best practice“; omezená universálnost)

CRAMM – analýza rizik v informačních systémech

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Budování bezpečnostního systému organizace



Bezpečnostní politika

Shrnuje odpovědi na všechny otázky (včetně zbývajících- „jak, metody, prostředky, postupy, jak ochranu řídit“)

Bezpečnostní politiku (BEPO) chápeme jako dokument koncepčního charakteru, kterým se vedení organizace, hlásí ke kultuře bezpečnosti a k budování interního bezpečnostního systému.

- **Dlouhodobě platný dokument** vrcholového řízení
- **Závazný pro všechny**

Hlavní funkce BEPO:

- ✓ Bezpečnostní
- ✓ Programovou
- ✓ Organizační
- ✓ Kulturní
- ✓ Politickou

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

Obsah BEPO obecně

1) **Cíle organizace a cíle BEPO**
2) **Analýza rizik**
3) **Bezpečnostní systém**

a) **Bezpečnostní priority**

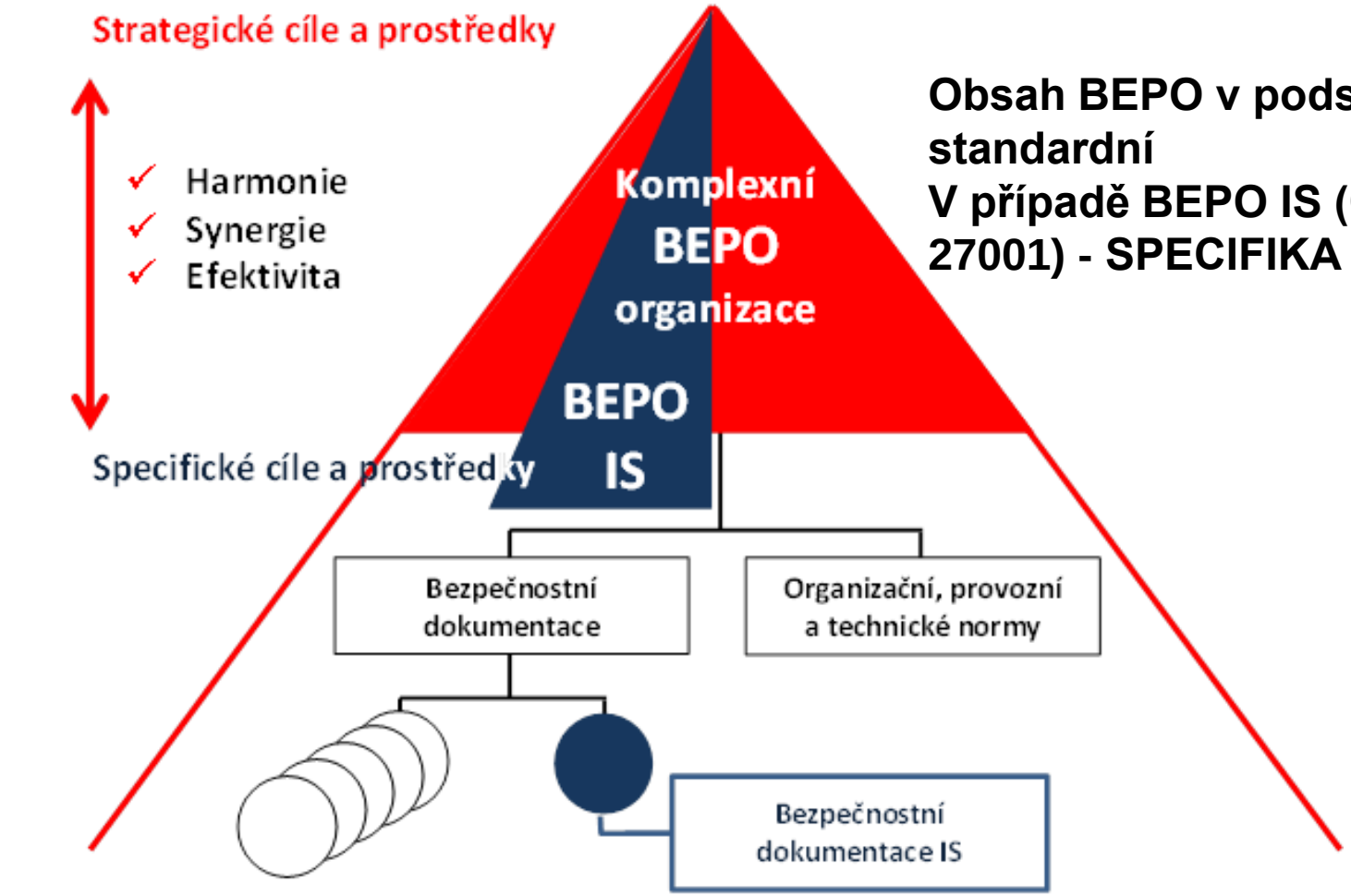
b) **Práce s riziky**
(zabránění rizikům; snížení rizik; akceptace rizik; převod rizik; rozložení rizik)

c) **Prvky bezpečnostního systému a jejich výstavba**
(etapy; finanční, lidské a organizační zdroje; rozsah outsourcingu služeb)

4) **Management bezpečnosti**
(organizační složení; personální obsazení; plánování zdrojů; pravomoci; bezpečnostní dokumentace; metrika hodnocení účinnosti bezpečnostního systému)

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

BEPO a bezpečnostní dokumentace (zdokumentování systému)



Obsah BEPO v podstatě standardní
V případě BEPO IS (ČSN ISO/IEC 27001) - SPECIFIKA (viz: dále)

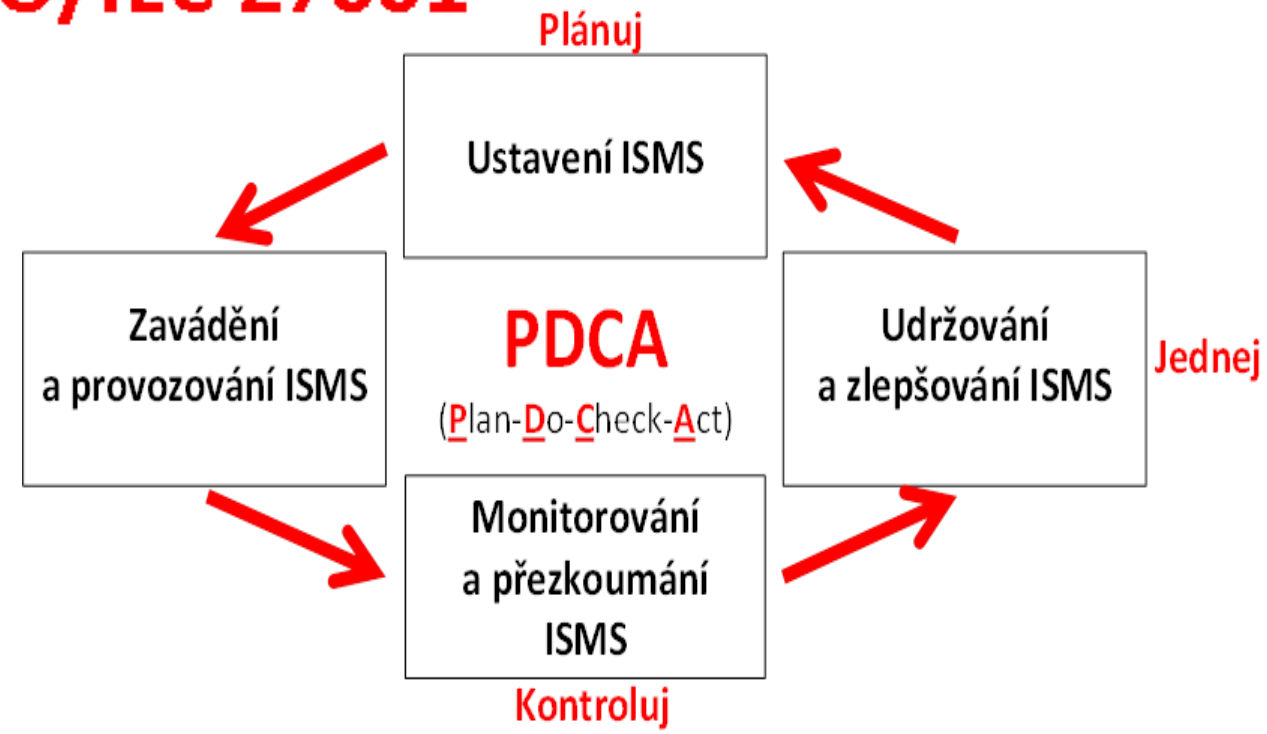
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

ISMS

Systém managementu bezpečnosti informací (ISMS)

(Information Security Management System)

ČSN ISO/IEC 27001



MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

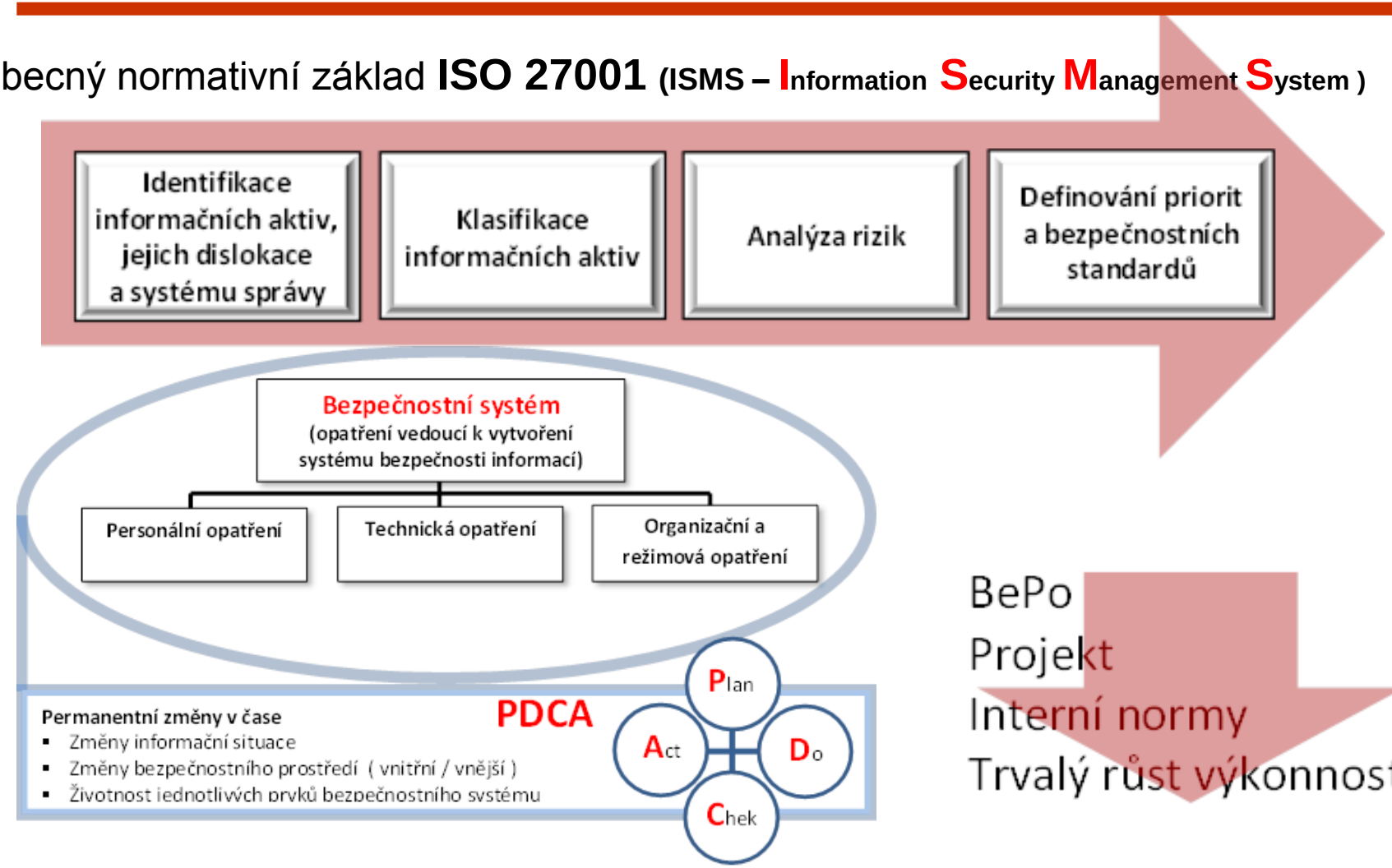
ISMS - preambule

1) **Deklarace závaznosti**
2) **Vůle vedení naplňovat napříč všemi ostatními procesy**
3) **Vazba na strategické cíle společnosti**
4) **Cíle BEPO IS**
5) **Strategie zlepšování**
6) **Soulad s právními normami**

Tato část BEPO bývá zveřejňována samostatně jako „bezpečnostní politika“. Plní přednostně funkce posilování image organizace, informovanosti a mobilizace zaměstnanců. Nezaměňovat za vlastní BEPO.

ISMS – shrnutí základních zásad

Obecný normativní základ **ISO 27001** (ISMS – **I**nformation **S**ecurity **M**anagement **S**ystem)



MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

2.
Bezpečnost informací z pohledu subjektů účastných na grantových projektech

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

Opatření k ochraně informací v rámci grantových projektů

Nezbytnou součástí výstupů projektů typu „projekt- výstavba – provoz zařízení“ by mělo být:

- ✓ **projektování způsobu zajištění ochrany před protiprávním nakládáním s informacemi**
  (v obecné rovině před protiprávními činy; v přiměřeném rozsahu prezentovaného).
  - — **Vlastními silami**
  - — **Subdodavatelem**

Nejčastější chyby při ochraně informací

- Není provedena analýza bezpečnostních rizik
- Není definována odpovědnost za bezpečnost IS
- Chybí bezpečnostní směrnice pro uživatele IS
- Nejsou splněny podmínky pro ochranu klasifikovaných informací
- Není řešena bezpečnost zálohy dat
- Není nastavena bezpečnostní politika práce s přenosnými médií pro ukládání dat

Nejčastější chyby při ochraně informací

- Nedůsledné zajištění přístupových oprávnění k jednotlivým IS a jejich částem
- Není nastaven postup při řešení bezpečnostních incidentů
- Bezpečnost IS není prověřován audity a penetračními testy
- Absence bezpečnostních školení pro uživatele IS
- Nedostatky v zajištění fyzické bezpečnosti IS
- Pořizování nelegálních SW
- Neaktualizované antivirové SW

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007-13
OP Výzkum a vývoj pro inovace

3.
Závěr

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

MŠMT vnímá tuto problematiku jako VYSOCE ZÁVAŽNOU!

Proto zorganizovalo tento seminář.

Nyní je na Vás jak se s touto problematikou vypořádáte.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

Memento ochrany informací

Změna postoje

Vyhodnocení situace

Opatření

Nenechat se ukolébat

Efektivita

Konzultovat s odborníky

ZVONEK Vám nedovolí zaspat správný čas !

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007-13
OP Výzkum a vývoj pro inovace

Děkuji za pozornost

Případné dotazy zasílejte na adresy:

fscsekretaria@fsc-ov.cz

nebo

haisz@fsc-ov.cz