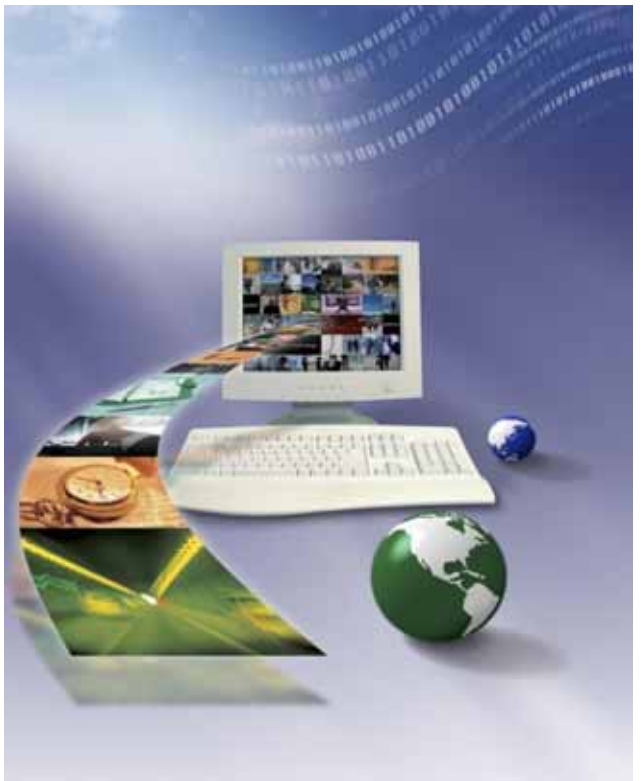
Certifikace systému managementu bezpečnosti informací dle ISO/IEC 27001

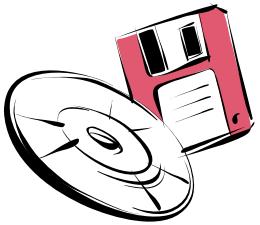


Hradec Králové– duben 2009

Choose certainty.
Add value.

Informace versus Bezpečnost informací

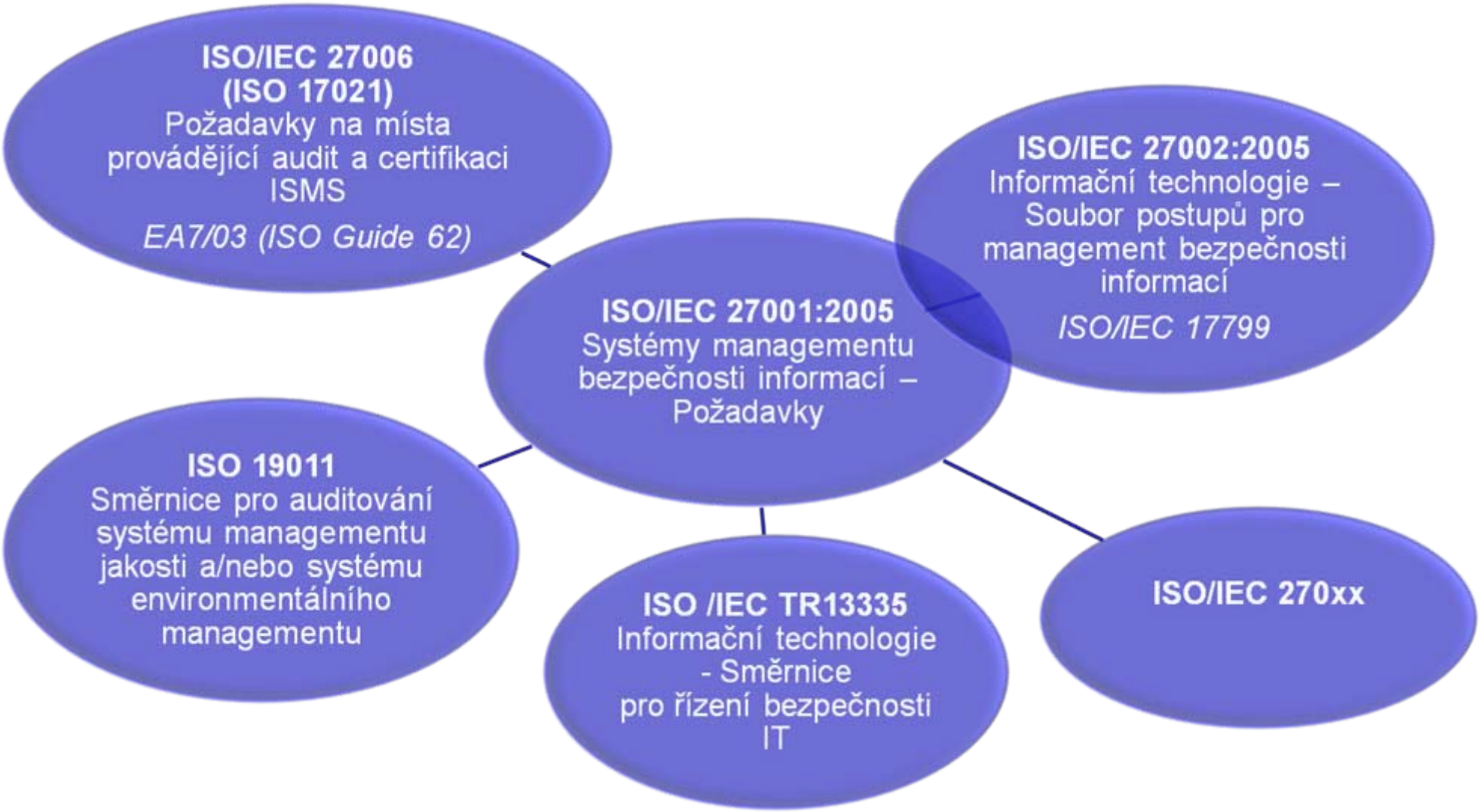
Informace (aktivum) - vše, co má hodnotu pro organizaci

Bezpečnost informací - zachování **důvěrnosti, integrity a dostupnosti** informací a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost

Ref.: ISO/IEC 27001

Vztahy mezi normami pro oblast ISMS



Normy v oblasti ISMS

ISO 27000 – **ISMS, Základy a slovník**

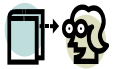
ISO 27001 – **ISMS, Požadavky**

ISO 27002 – **ISMS, Soubor postupů (předchozí ISO 17799)**

ISO 27003 – **ISMS, Metriky a měření**

ISO 27004 – **ISMS, Návod pro implementaci**

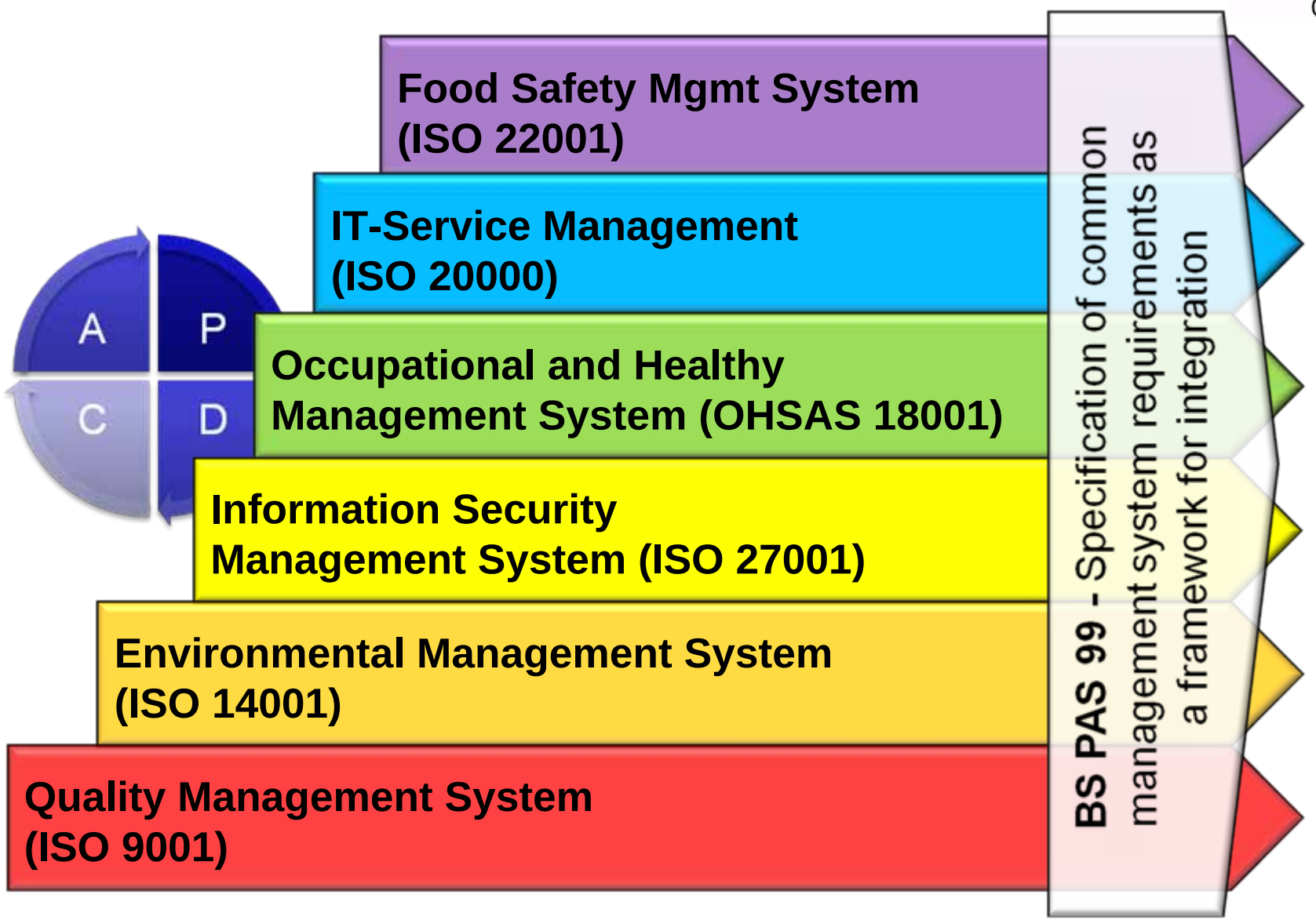
ISO 27005 – **ISMS, Management rizik (předchozí BS7799-3)**



ISO 27006 – **ISMS, Požadavky na místa provádějící audit a certifikaci ISMS**

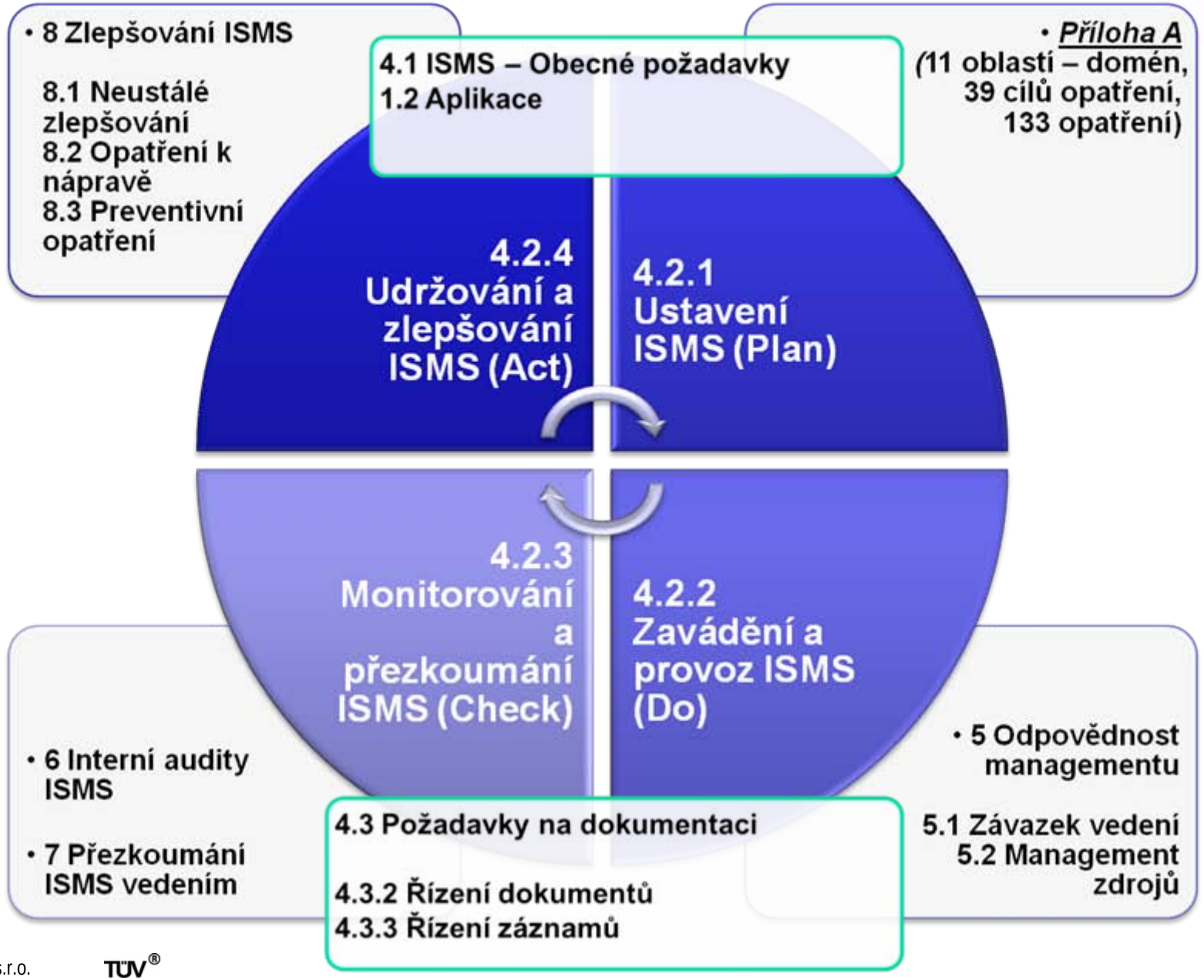
ISO 27007..9 – **ISMS, další oblasti, včetně kompetencí ISMS auditorů**

Vztah k jiným systémům managementu



Struktura normy ISO/IEC 27001:2005

Czech



4.2.1 Ustavení ISMS

Organizace musí:

a) definovat rozsah a hranice ISMS,

b) definovat politiku ISMS,

c) definovat systematický přístup k ohodnocení rizik,

d) identifikovat rizika,

e) analyzovat a vyhodnoť rizika,

f) identifikovat a ohodnotit varianty pro zvládání rizik,

g) vybrat cíle opatření a opatření pro zvládání rizik,

h) získat souhlas managementu s navrhovanými zbytkovými riziky,

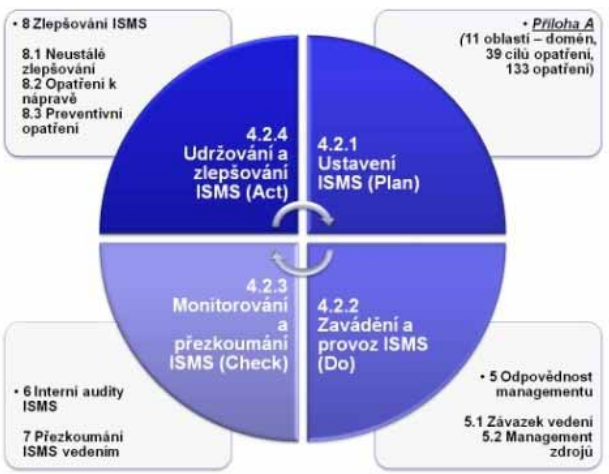
i) získat souhlas vedení k zavedení a provozu ISMS,

j) připravit Prohlášení o aplikovatelnosti.

4.2.2 Zavedení a provoz ISMS

Organizace musí:

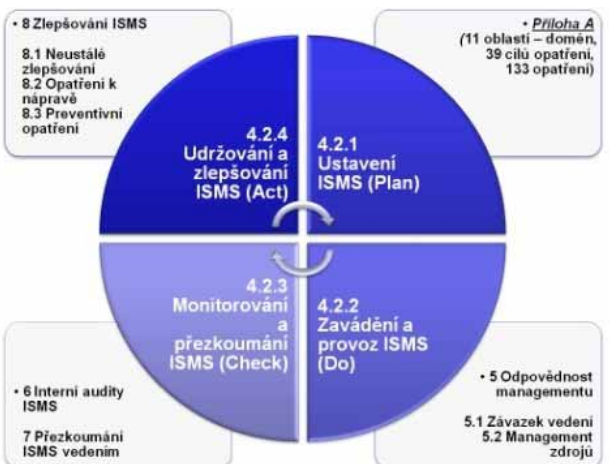
- formulovat plán zvládání rizik (viz kapitola 5),
- zavést plán zvládání rizik,
- určit, jakým způsobem bude měřit účinnost vybraných opatření,
- zavést bezpečnostní opatření vybraná v 4.2.1 g) pro dosažení (naplnění) cílů těchto opatření,
- zavést programy školení a programy zvyšování informovanosti (viz kapitola 5.2.2),
- řídit provoz ISMS,
- řídit zdroje ISMS (viz kapitola 5.2),
- zavést postupy a další opatření pro rychlou detekci a postupy reakce na bezpečnostní incidenty.



4.2.3 Monitorování a přezkoumání ISMS

Organizace musí:

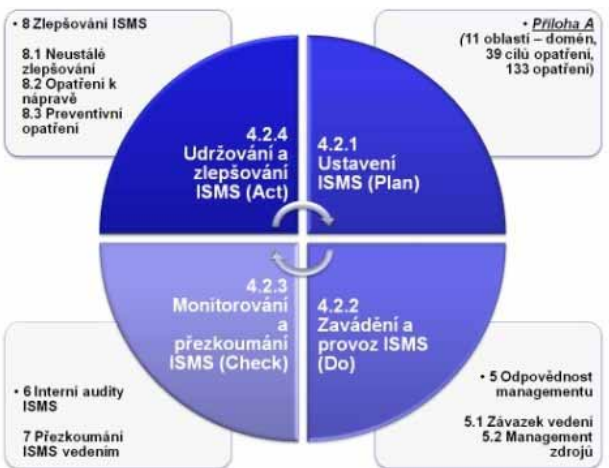
- monitorovat, přezkoumávat a zavést další opatření,
- pravidelně přezkoumávat účinnost ISMS,
- měřit účinnost zavedených opatření,
- provádět přezkoumání hodnocení rizik a přezkoumávat zbytková rizika a úroveň akceptovatelného rizika,
- provádět interní audity ISMS (viz kapitola 6),
- pravidelně přezkoumávat ISMS (viz kapitola 7.1),
- aktualizovat bezpečnostní plány,
- zaznamenávat všechny činnosti a události, s dopadem na účinnost nebo výkonnost ISMS.



4.2.4 Udržování a zlepšování ISMS

Organizace musí:

- Zavádět identifikovaná zlepšení ISMS,
- Provádět odpovídající nápravné a preventivní činnosti v souladu s 8.2 a 8.3,
- Projednávat činnosti a návrhy na zlepšení na požadované úrovni detailu se všemi zainteresovanými stranami a domluvit další postup,
- Zaručit, že zlepšení dosáhnou předpokládaných cílů.

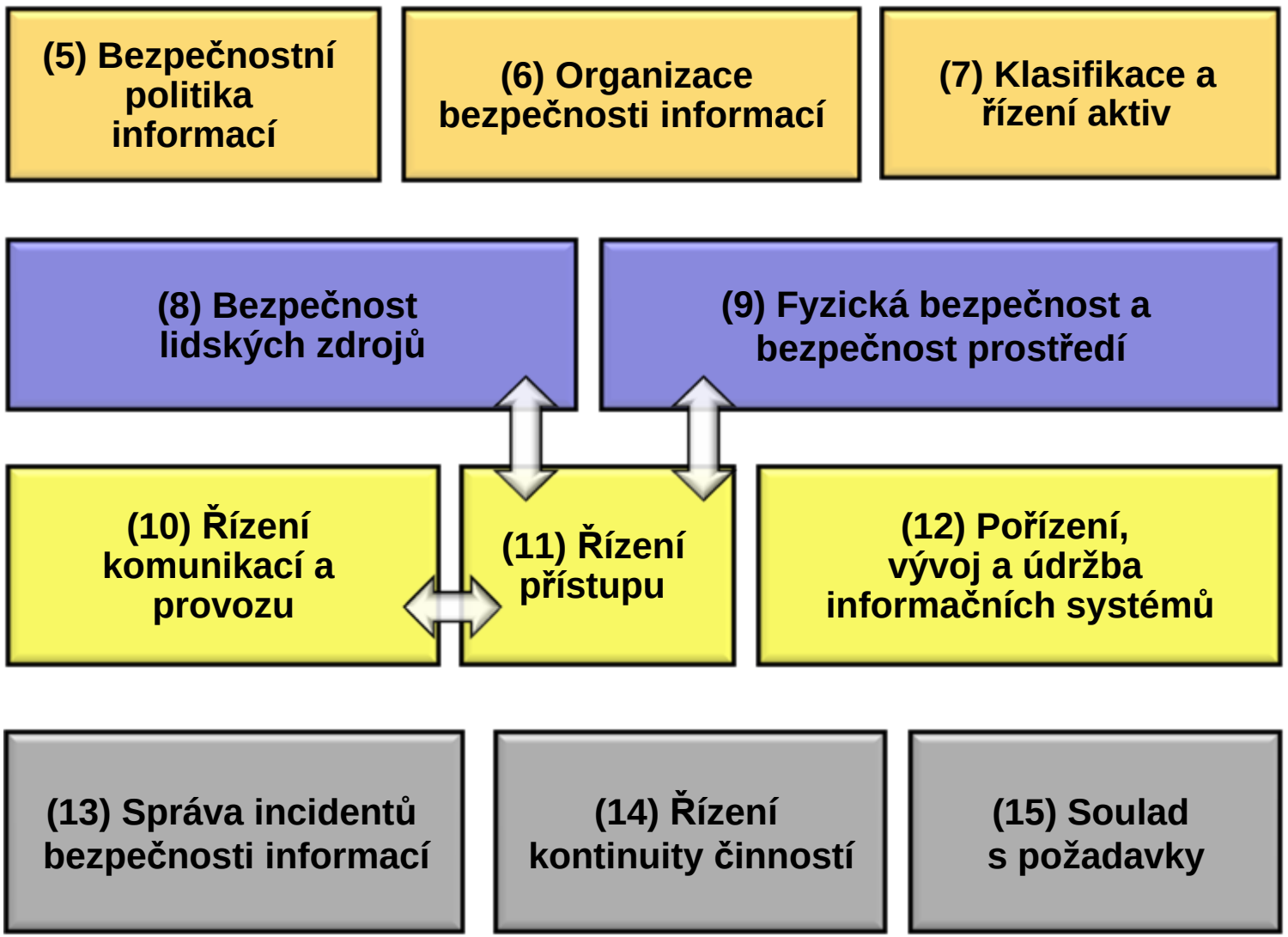


4.3 Požadavky na dokumentaci

Dokumentace ISMS musí obsahovat následující:

- dokumentovaná prohlášení politiky a cílů ISMS,
- rozsah ISMS,
- postupy a opatření podporující ISMS,
- popis použitých metodik hodnocení rizik,
- zprávu o hodnocení rizik,
- plán zvládání rizik,
- dokumentované postupy nezbytné pro zajištění efektivního plánování, provozu a řízení procesů bezpečnosti informací organizace a popis měření účinnosti zavedených opatření [viz 4.2.3 c)],
- záznamy vyžadované normou ISO/IEC 27001,
- prohlášení o aplikovatelnosti (SoA).

Opatření v příloze A normy ISO/IEC 27001:2005



Proces certifikace

Cíl: Získat certifikát vydaný certifikační společností akreditované podle ISO 17021, ISO 27006

- Platnost certifikátu – 3 roky
- Certifikační audity – audit 1. a 2. stupně
- Dozorové audity – roční, tolerance -3/+0 měsíce závislé na datu certifikačního auditu
- Po 3 letech probíhají recertifikační audity
- Pokud je potřebné změnit, rozšířit obor platnosti certifikace, je vhodné toto provést během plánovaných auditů.

Aplikace požadavků na bezpečnost informací

- **Implementované a certifikované ISMS** – projektové a konstrukční organizace, poskytovatelé internetu, poskytovatelé IT služeb, softwarové firmy, telekomunikační operátoři, zdravotnické organizace, finanční organizations, datová centra, státní subjekty, státní organizace & nevýdělečné organizace.

Požadavky ISMS jsou certifikovány TÜV SÜD Czech například v:

KSRZIS

Koordinační středisko pro resortní zdravotnické informační systémy

GHC GENETICS

Aplikace požadavků na bezpečnost informací

- **Hodnocení a certifikace safer shopping (e-shopy)** – organizační požadavky, postupy pro nakupování, bezpečnost a ochrana údajů
- **Hodnocení a certifikace služby** – hotely, lázně, cestovní kanceláře - organizační požadavky, postupy pro poskytování služby, bezpečnost a ochrana údajů

Ochrana osobních údajů

- **Legislativa –** zákon č. 101/2000 Sb. v platném znění
- **Požadavky –** jsou stanoveny požadavky pro zpracovatele a správce osobních údajů, např.: **stanovit a dokumentovat bezpečnostní opatření pro ochranu osobních údajů** na základě hodnocených rizik
- **Autorita –** Úřad pro ochranu osobních údajů, dohlíží, udržuje registr, vyjádření a stanoviska jsou na www.uoou.cz
- **Pokuty –** mohou být 5 -10 million Kč pro organizaci, až 100.000,- Kč pro osobu a nepodmíněný trest až na 3 roky podle paragrafu 178, odst. 1 novely Trestního zákoníku

Ing. Roman Prášek, Ph.D.

Auditor

TÜV SÜD Czech s.r.o.
Novodvorská 994
CZ – 142 21 Praha 4

Tel: +420 725 707 296
E-mail: roman.prasek@tuv-sud.cz

www.tuv-sud.cz

Choose certainty.
Add value.