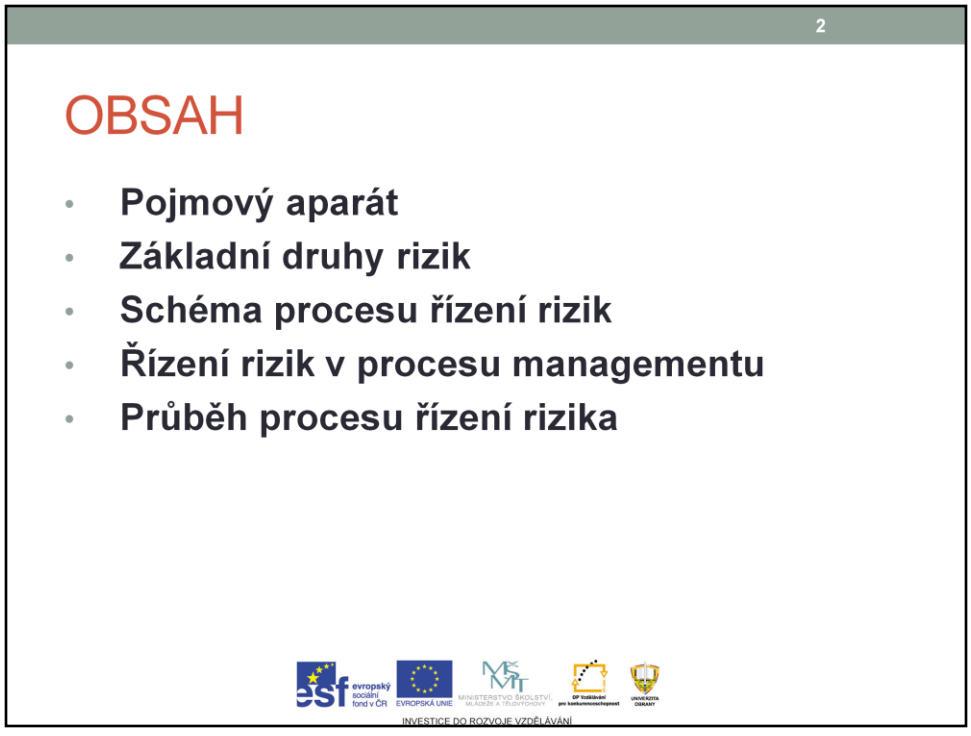
Řízení rizik, zvládání rizik, ovlivňování rizik či minimalizace rizik a další podobné pojmy jsou v současné době stále více používány a skloňovány v nejrůznějších podobách a souvislostech. Každá organizace nebo podnik čelí v rámci svého působení nebo v oblasti svého podnikání rizikům, které mohou vést ke snížení hodnoty organizace, případně až k jejímu ochromení nebo úplnému zničení. Proto se každý manažer snaží negativnímu působení těchto rizik předcházet a v případě, že již došlo k jejich působení, tak alespoň snížit tento dopad na nejnižší možnou míru.

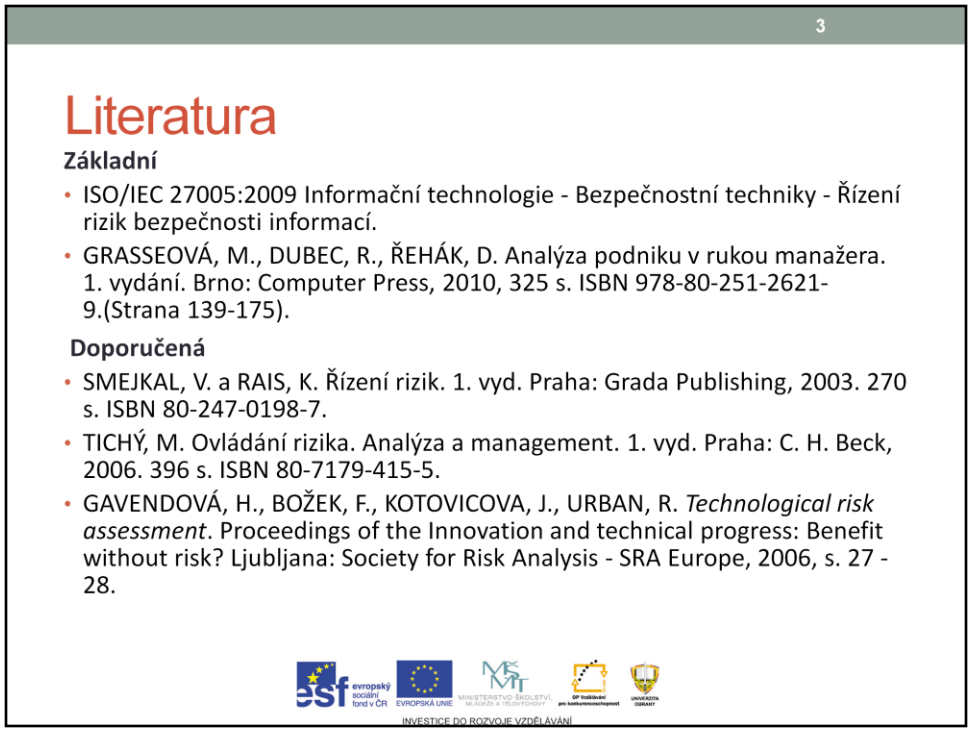
V případě strategické úrovně naplňování cílů organizace se pak řízení rizik jeví jako existenční nutnost a životní zájem každé organizace. Proto můžeme říct, že řízení rizik nyní zažívá oprávněný rozvoj a přitahuje pozornost všech významných manažerů. S jeho využitím je možné předcházet ztrátám a škodám velkého rozsahu, které mohou mít pro organizaci až fatální následky.

Řízení rizik bezpečnosti informací podporuje všeobecná pojetí specifikovaná v různých

normách poskytuje návod pro implementaci procesně orientovaného přístupu k řízení rizik, aby tak pomohla uspokojivě implementovat a naplnit požadavky na řízení rizik bezpečnosti informací.



Základním předpokladem úspěšného řešení každé problematiky je přesné a jednoznačné vymezení terminologického rámce a případných existujících odchylek v definování či chápání některých pojmů. K těmto odchylkám dochází jednak v důsledku nesystémového řešení dané problematiky, ale především následkem jejího neustálého vývoje. A právě tímto problémem je zatížena také oblast řízení rizik. Na základě toho je v následující části provedeno vydefinování základních pojmů v souladu s mezinárodními normami ISO/IEC 27 XXX.



Pro studium této problematiky mezi základní literaturu patří – viz snímek číslo 3. Pro zájemce mohu doporučit i další normu vztahující se k přednášené problematice jako například:

ISO/IEC 27001 *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací -Požadavky*

Tato mezinárodní norma specifikuje požadavky na ustavení, implementaci, provozování, monitorování, přezkoumávání a zlepšování formálně schválených systémů řízení bezpečnosti informací (ISMS) v **kontextu celkových obchodních rizik organizace**. Specifikuje požadavky na implementaci bezpečnostních kontrolních opatření upravených podle potřeb jednotlivých organizací nebo jejich částí. **Tato mezinárodní norma je univerzální pro všechny druhy organizací (tj. komerční podniky, vládní úřady, neziskové organizace).**

Účelem této normy je poskytnout normativní požadavky na vývoj a provoz ISMS, **včetně sady kontrolních opatření pro řízení a zmírnění rizik spojených s**

informačními aktivy, které organizace vyhledává, aby je chránila provozováním ISMS.

ZÁKLADNÍ POJMY

Hrozba [Threat, Hazard]

- představuje označení možného zdroje nebo příčiny nežádoucí události

Aktivum [Asset]

- hodnota pro subjekt či společnost, která může být snížena působením hrozby (např. nemovitost, personál)

Riziko [Risk]

- pravděpodobnost vzniku nežádoucí události plynoucí z existence jisté hrozby
- je historický výraz pocházející údajně ze 17. století, kdy se objevil v souvislosti s lodní plavbou. Slovo pochází z italštiny a označovalo úskalí, kterému se museli plavci vyhnout

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

ZÁKLADNÍ POJMY

dopad *(impact)*

- nepříznivá změna ovlivňující úroveň dosažených cílů organizace.

riziko bezpečnosti informací *(information security risk)*

- možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiva způsobí škodu organizaci
- Je stanoveno na základě kombinace pravděpodobnosti dané události a jejich následků.
- **vyhnutí se riziku** *(risk avoidance)*
- rozhodnutí nedopustit zapojení se do rizikových situací, nebo je vyloučit.

ZÁKLADNÍ POJMY

komunikace rizik *(risk communication)*

- výměna nebo sdílení informací o riziku mezi tím, kdo rozhoduje a ostatními zúčastněnými stranami
- [ISO/IEC Guide 73:2002]

odhad rizik *(risk estimation)*

- proces k určení hodnot pravděpodobnosti a následků rizika

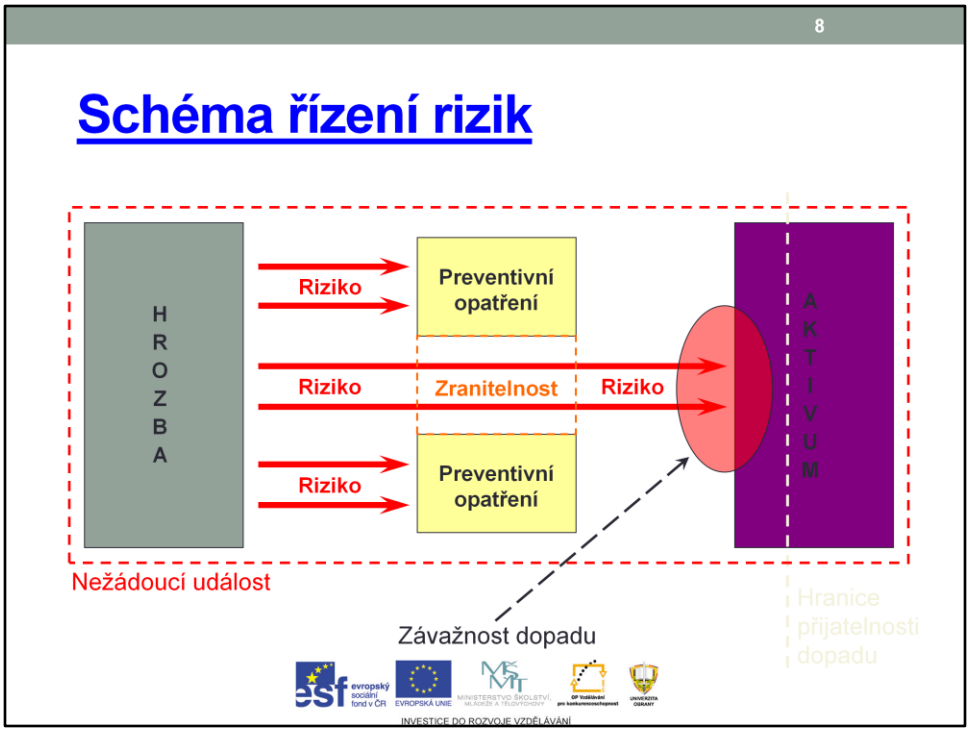
ZÁKLADNÍ POJMY

identifikace rizik *(risk identification)*

- proces hledání, sepsání a charakterizování prvků rizika

redukce rizik *(risk reduction)*

- činnosti ke snížení pravděpodobnosti, negativních následků nebo obou těchto parametrů spojených s rizikem
- **podstoupeni rizik** *(risk retention)*
- přijetí břemene ztráty nebo prospěchu ze zisku vyplývajícího z určitého rizika
- **přenos rizik** *(risk transfer)*
- sdílení nákladů ze ztrát s jinou stranou nebo sdílení prospěchu ze zisku vyplývajícího z rizika



Vztah mezi základními definovanými termíny řízení rizik je znázorněn na obrázku 8. Stěžejním prvkem problematiky řízení rizik jsou aktiva, která se vyskytují na strategické a provozní úrovni organizace. Aktiva jsou ohrožována vnějšími a vnitřními hrozbami a tyto hrozby jsou aktivovány zdroji hrozeb, tj. vnější činitelé nebo vnitřní prvky organizace. Podstatou hrozby je využít zranitelností organizace, překonat protiopatření a působit na aktivum, kde způsobí škodu. Riziko je pak kvantifikací působení hrozeb na aktiva a zbytkové riziko představuje riziko, které stále zůstává i po zavedení protiopatření.

Aktivum [Asset]

Aktivem rozumíme vše, co má pro danou organizaci nějakou hodnotu, která může být zmenšena působením hrozby. Aktiva můžeme členit do dvou základních kategorií, a to na aktiva strategické úrovně organizace (aktiva této úrovně chápeme jako organizací definované strategické cíle) a aktiva provozní úrovně organizace (aktiva této úrovně chápeme jako procesy a zdroje organizace) obrázek.

Na obou úrovních se mohou vyskytovat aktiva hmotná (např. finanční prostředky,

cenné papíry, nemovitosti) a aktiva nehmotná (např. informace, kvalita personálu, autorská práva). Aktivem však může být také sám subjekt organizace, poněvadž hrozba může působit na celou jeho existenci. Vůči působení hrozby se aktivum vyznačuje určitou zranitelností nebo je chráněno protiopatřeními. Pro členění **aktiv strategické úrovně organizace** do druhových oblastí je nejvhodnější využít metodu Balanced Scorecard.

Zdroj hrozby [Threat Source]

Zdrojem hrozby je jakýkoli faktor, který může ovlivnit cíle, procesy nebo projekty organizace. Jedná se tedy o vnější činitele (např. vnější legislativní prostředí, vnější politické prostředí) nebo vnitřní prvky organizace (např. procesy, zaměstnanci, nemovitosti), které aktivují konkrétní hrozby a jejichž vývoj nebo činnost (případně nečinnost) jsou příčinami možných nežádoucích dopadů na aktiva organizace.

Hrozba [Threat]

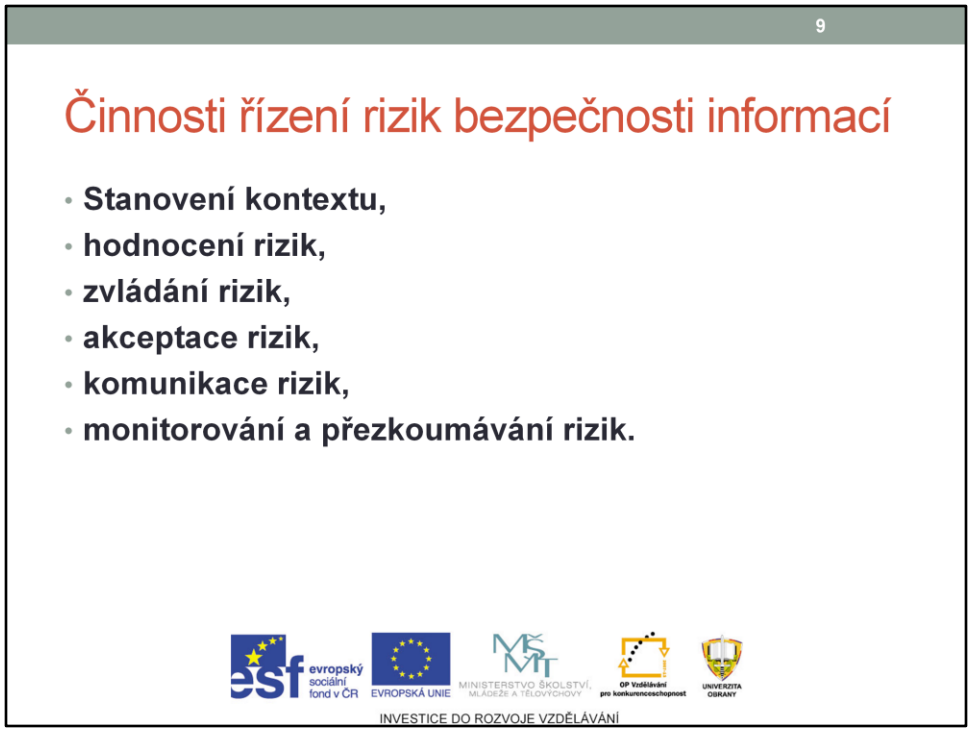
Hrozbou rozumíme sílu, událost, aktivitu nebo osobu, která má nežádoucí vliv na činnost organizace. Hrozba působí přímo na aktivum nebo na protiopatření s cílem získat přístup k aktivu. Podstatou hrozby je tedy využít zranitelnosti, překonat protiopatření a působit na aktivum, kde způsobí škodu (dopad). Aby mohla hrozba působit, musí být nejprve aktivována, k čemuž slouží zdroj hrozby. Alternativním termínem zejména v oblasti technologických a zdravotních rizik je pojem nebezpečí.

Riziko [Risk]

Riziko vzniká vzájemným působením hrozby a aktiva a vyjadřuje se kombinací (resp. součinem) pravděpodobnosti výskytu nežádoucí události a jejího dopadu na dané aktivum. Riziko můžeme tedy chápat jako kvantifikaci působení hrozby na aktivum. Rovněž můžeme konstatovat, že riziko je možnost, že při zajišťování činnosti organizace s určitou pravděpodobností nastane určitá událost, jednání nebo stav s následnými nežádoucími dopady na plnění schválených záměrů a cílů této organizace.

Zranitelnost [Vulnerability]

Zranitelnost představuje nedostatek, slabinu nebo stav analyzovaného aktiva, který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Zranitelnost vzniká tam, kde dochází k interakci mezi hrozbou a aktivem, přičemž základní charakteristikou zranitelnosti je její úroveň. Ta je stanovována podle dvou základních faktorů, a to citlivosti (náchylnost aktiva být poškozeno danou hrozbou) a kritičnosti (význam aktiva pro analyzovanou organizaci).



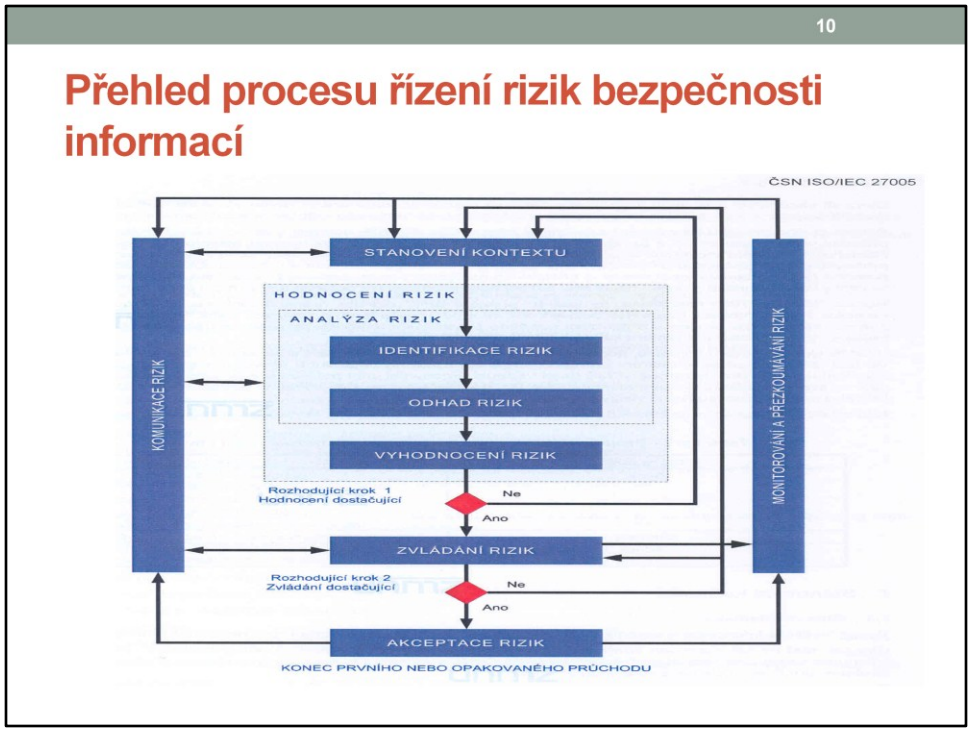
K identifikaci potřeb organizace vyplývajících z řízení rizik a vytvoření účinného systému řízení bezpečnosti informací (ISMS) je nutný systematický přístup k řízení rizik bezpečnosti informací. Tento přístup by měl být vhodný pro prostředí organizace a měl by být zejména v souladu s celkovým řízením rizik organizace. Úsilí dosáhnout bezpečnosti by se mělo účinně a včas vypořádat s riziky kde a kdy je to zapotřebí. Řízení rizik bezpečnosti informací by mělo tvořit nedílnou součást činností řízení bezpečnosti všech informací a mělo by se používat jak pro zavedení, tak pro další provozování ISMS.

Řízení rizik bezpečnosti informací by mělo být nepřetržitým procesem. Tento proces by měl stanovit kontext, vyhodnotit rizika a zvládat rizika za použití plánu zvládání rizik pro zavedení doporučení a rozhodnutí. Řízení rizik analyzuje, co se může stát a jaké mohou být případné důsledky, před rozhodnutím, co by se mělo provést a kdy za účelem redukce rizika na přijatelnou úroveň.

Řízení rizik bezpečnosti informací by mělo přispět k tomu, aby:

- byla provedena identifikace rizik
- bylo provedeno hodnocení rizik z hlediska jejich důsledků na činnosti organizace a pravděpodobnosti jejich výskytu
- byla pravděpodobnost a důsledky těchto rizik komunikovány a chápány
- bylo při zvládání rizik stanoveno pořadí priorit
- byla stanovena priorita u činností vedoucích k redukci výskytu rizik
- byly do rozhodnutí o řízení rizik zapojeny i zainteresované strany, a aby o stavu řízení rizik byly stále informovány
- byla sledována účinnost zvládání rizik
- byla rizika a procesy zvládání rizik sledovány a pravidelně přezkoumávány
- byly získávány informace k zlepšení přístupu k řízení rizik
- byli vedoucí pracovníci i zaměstnanci školeni v oblasti rizik a opatření přijímaných k jejich zmírnění.

Proces řízení rizik bezpečnosti informací lze používat pro organizaci jako celek, jakoukoliv samostatnou část organizace (například oddělení, fyzické místo, službu), jakýkoliv informační systém, stávající nebo plánované nebo konkrétní aspekty opatření (například plánování kontinuity činností organizace).



Jak ukazuje obrázek 10, proces řízení rizik bezpečnosti informací se může u činností hodnocení rizik a/nebo zvládání rizik opakovat. Opakující se přístup k provádění hodnocení rizik může při každém opakování hloubku a podrobnosti hodnocení zvyšovat. Opakující se přístup zajišťuje správnou rovnováhu mezi minimalizací času a vynaloženého úsilí potřebného k identifikaci opatření, přičemž stále zajišťuje, že vysoká rizika jsou náležitě hodnocena.

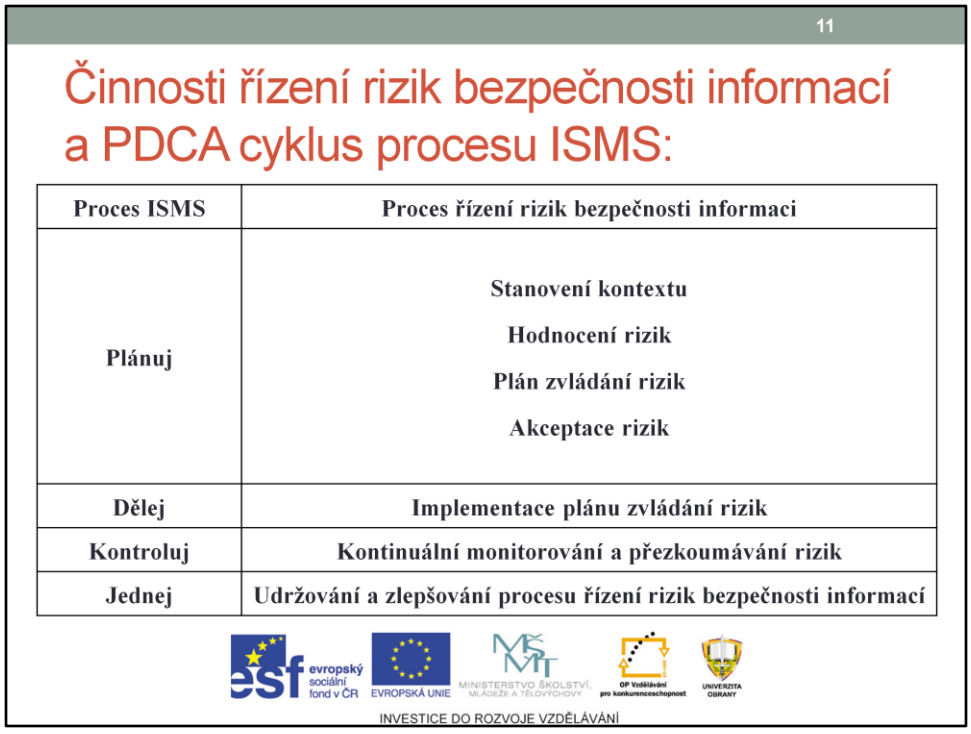
Nejdřív se stanoví kontext. Pak se provádí hodnocení rizik. Pokud toto poskytne dostatek informací pro efektivní určení akcí nutných pro redukci rizik na přijatelnou úroveň, pak je úkol dokončen a následuje zvládání rizik. Jestliže jsou informace nedostatečné, musí být provedeno další opakování hodnocení rizik s revidovaným kontextem (například kritérii hodnocení rizik, kritérii akceptace rizik nebo kritérii dopadu), možná jen na omezených částech celkového rozsahu (viz obrázek 10, bod rozhodnutí o riziku).

Účinnost zvládání rizik závisí na výsledcích hodnocení rizik. Je možné, že zvládání rizik nepovede okamžitě k přijatelné úrovni zbytkového rizika. V takové situaci může být v

případě nutnosti provedeno opakované hodnocení rizik se změněnými parametry kontextu (například kritérii vyhodnocení rizik, akceptace rizik nebo kritérii dopadu), po němž bude následovat další zvládání rizik (viz obrázek 10, bod rozhodnutí o riziku 2).

Činnosti akceptace rizik musí zajistit, aby vedoucí pracovníci organizace zbytková rizika explicitně přijali. To je důležité zejména v situaci, kdy je zavedení opatření opomenuto nebo odloženo, například kvůli nákladům.

Během celého procesu řízení rizik bezpečnosti informací je důležité, aby byli o rizicích a jejich zvládání informováni příslušní vedoucí pracovníci a zaměstnanci provozu. I před zvládáním rizik mohou být informace o identifikovaných rizicích pro zvládání incidentů velmi cenné a mohou pomoci snížit potenciální škodu. Informovanost vedoucích pracovníků a zaměstnanců o rizicích, charakteru přijatých opatření ke zmírnění rizik a oblastech zájmu organizace pomáhá řešit incidenty a neočekávané události co nejúčinnějším způsobem. Měly by být zaznamenány podrobné výsledky každé činnosti procesu řízení rizik bezpečnosti informací a z pohledu těchto dvou bodů rozhodnuto o riziku.



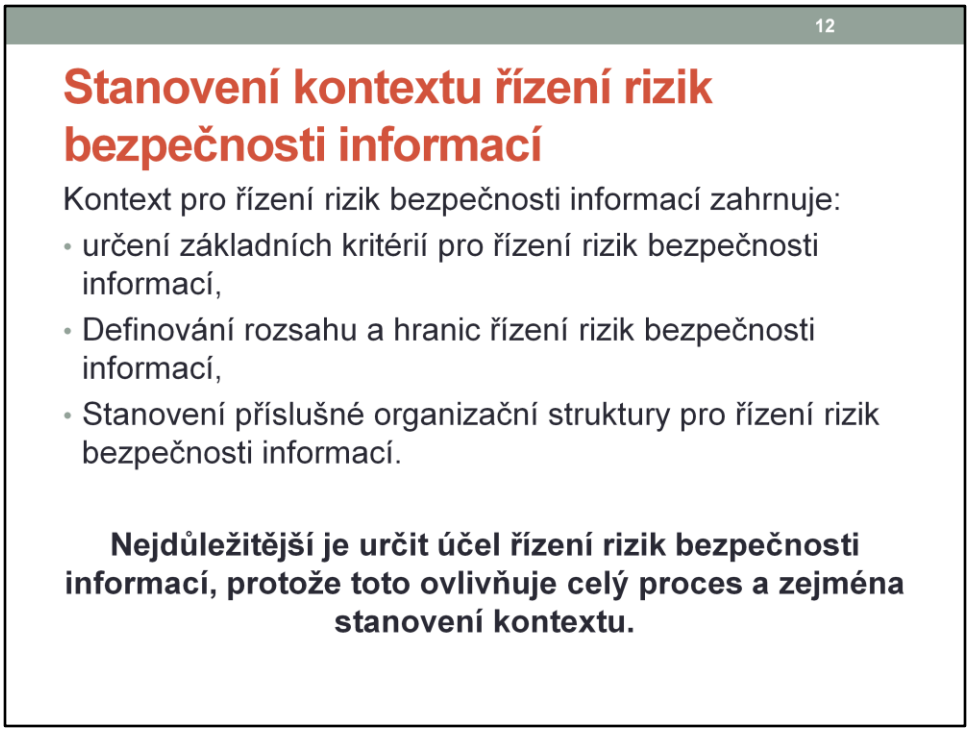
V ISMS tvoří stanovení kontextu, hodnocení rizik, vývoj plánu zvládání rizik a akceptace rizik součást fáze "plánuj".

Ve fázi "dělej" se akce a opatření potřebná k redukci rizika na přijatelnou úroveň uplatňují v souladu s plánem zvládání rizik.

Ve fázi "kontroluj" ISMS musí vedoucí pracovníci určit potřebu přezkoumání hodnocení a zvládání rizik ve světle incidentů a změn okolností.

Ve fázi "jednej" se provádějí všechny požadované akce, včetně dodatečného použití procesu řízení rizik bezpečnosti informací.

Uvedená tabulka (obrázek č. 11) shrnuje činnosti řízení rizik bezpečnosti informací k těmto čtyřem fázím procesu ISMS.



Obecná hlediska

Veškeré informace o organizaci týkající se stanovení kontextu řízení rizik bezpečnosti informací.

Činnost: Měl by být stanoven kontext pro řízení rizik bezpečnosti informací, který zahrnuje určení základních kritérií pro řízení rizik bezpečnosti informací, definuje rozsah a hranice, a stanoví příslušnou organizační strukturu pro řízení rizik bezpečnosti informací.

Doporučení k realizaci:

Nejdůležitější je určit účel řízení rizik bezpečnosti informací, protože toto ovlivňuje celý proces a zejména stanovení kontextu.

Tím účelem může být:

- Podpora ISMS

- Právní shoda a důkaz povinné péče
- Příprava plánu kontinuity činností organizace
- Příprava plánu reakce na incidenty
- Popis požadavků na bezpečnost informací u produktu, služby nebo mechanismu (bezpečnostního).

POZNÁMKA:

Norma ISO/IEC 27001 nepoužívá výraz "kontext". Avšak všechno v kapitole 7 se vztahuje k požadavkům "definovat rozsah a hraníce ISMS" [4.2.1 a)], "definovat politiku ISMS" [4.2.1 b)] a "definovat přístup k hodnocení rizik" [4.2.1 c)], jež jsou v ISO/IEC 27001 specifikovány.

Výstup: Specifikace základních kritérií, rozsahu, hranic a organizační struktury pro proces řízení rizik bezpečnosti informací.

Základní kritéria

V závislosti na rozsahu a cílech řízení rizik lze použít různé přístupy. Přístup může být také různý pro každé opakování. Měl by být vybrán a vhodně přizpůsoben přístup k řízení rizik, který řeší základní kritéria: kritéria vyhodnocení rizik, kritéria dopadu, kritéria akceptace rizik.

Kromě toho by organizace měla zhodnotit, zda jsou k dispozici potřebné zdroje pro:

- Provedení hodnocení rizik a stanovení plánu zvládání rizik
- Definování a zavedení politik a postupů, včetně implementace vybraných opatření

- Opatření pro monitorování
- Monitorování procesu řízení rizik bezpečnosti informací.

Kritéria vyhodnocení rizik

Měla by být vytvořena kritéria vyhodnocení rizik bezpečnosti informací zohledňující následující:

- Strategické hodnoty procesu informací o činnostech organizace
- Kritičnosti informačních aktiv
- Legislativní a regulatorní požadavky, smluvní povinnosti
- Důležitost dostupnosti, důvěrnosti a integrity provozu a obchodních činností
- Očekávání a představy zainteresovaných stran, negativní následky ztráty důvěryhodnosti a pověsti
- Kromě toho lze kritéria vyhodnocení rizik použít k určení priorit pro zvládání rizik.

Kritéria dopadu

Měla by být vytvořena kritéria dopadu, která by měla být specifikována na základě stupně škod nebo ztrát organizace způsobených bezpečnostní událostí, s ohledem na:

- Úroveň klasifikace ovlivněného informačního aktiva
- Narušení bezpečnosti informací (například ztráta důvěrnosti, integrity a dostupnosti) Poškozené provozy (vnitřní nebo třetích stran)
- Ztrátu činností organizace a finanční hodnoty
- Přerušení plánů a nedodržení konečných termínů

- Poškození pověsti
- Porušení právních, regulatorních nebo smluvních požadavků.

Kritéria akceptace rizik

Měla by být vytvořena a určena kritéria akceptace rizik. Tato kritéria často závisí na politikách, záměrech a cílech organizace a zájmech zainteresovaných stran.

Organizace by měla definovat své vlastní škály pro úrovně akceptace rizik. Při jejich vytváření by mělo být bráno v úvahu, že:

- Kritéria akceptace rizik mohou obsahovat četné prahové úrovně s požadovanou cílovou úrovní rizika, ale i ustanovení pro řídící pracovníky, aby za stanovených okolností akceptovali i rizika nad touto úrovní.
- Kritéria akceptace rizik lze vyjádřit jako poměr odhadnutého zisku (nebo jiného obchodního přínosu) k odhadnutému riziku.
- Pro různé třídy rizik mohou platit různá kritéria akceptace rizik, například rizika, která mohou mít za následek nesoulad s předpisy nebo zákony, nelze akceptovat, zatímco lze připustit akceptaci vysokých rizik, pokud je to specifikováno jako smluvní požadavek.
- Kritéria akceptace rizik mohou zahrnovat požadavky na budoucí dodatečné zvládání, například riziko lze akceptovat, jestliže existuje schválení a závazek přijmout opatření k jeho redukci na přijatelnou úroveň v určitém stanoveném termínu.

Kritéria akceptace rizik se mohou lišit také podle toho, jak dlouho se očekává, že riziko bude existovat, například riziko může být spojeno s dočasnou nebo krátkodobou

činností. Kritéria akceptace rizik by se měla stanovit s přihlédnutím k:

- Obchodním kritériím
- Právním a regulačním aspektům
- Provozu
- Technologiím
- Financím
- Sociálním a humanitárním faktorům.

POZNÁMKA:

Kritéria akceptace rizik odpovídají "kritériím pro akceptaci rizik a identifikaci přijatelné úrovně rizika" specifikovaným v ISO/IEC 27001 4.2.1 c) 2).

Rozsah a hranice

Organizace by měla definovat rozsah a hranice pro řízení rizik bezpečnosti informací.

Rozsah procesu řízení rizik bezpečnosti informací musí být definován, aby bylo zajištěno, že jsou při hodnocení rizik brána v úvahu všechna příslušná aktiva. Kromě toho je nutno identifikovat hranice k řešení těch rizik, která by mohla tyto hranice prolomit.

O organizaci by měly být shromážděny informace, aby bylo možno určit prostředí, v němž působí, a jeho důležitost pro proces řízení rizik bezpečnosti informací.

Při definování rozsahu a hranic by organizace měla přihlížet k těmto informacím:

- Strategické obchodní cíle, strategie a politiky organizace
- Obchodní procesy

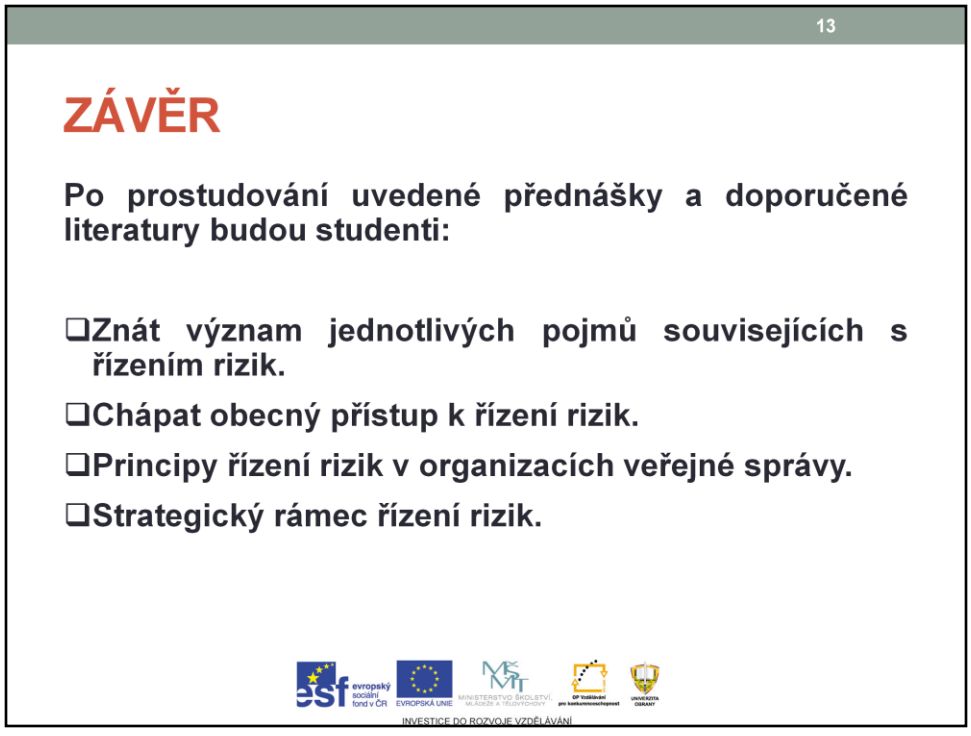
- Funkce a struktura organizace
- Právní, regulatorní a smluvní požadavky platné pro organizaci
- Politika organizace týkající se bezpečnosti informací
- Celkový přístup organizace k řízení rizik
- Informační aktiva
- Sídla organizace a jejich geografické charakteristiky
- Omezení ovlivňující organizaci
- Očekávání podílníků
- Sociálně kulturní prostředí
- Rozhraní (například výměna informaci s prostředím).

Kromě toho by organizace měla poskytnout odůvodnění pro všechna vyloučení z tohoto rozsahu.

Příkladem rozsahu řízení rizik může být aplikace, IT infrastruktura, obchodní proces nebo definovaná část organizace.

POZNÁMKA:

Rozsah a hranice řízení rizik bezpečnosti informací se vztahují k rozsahu a hranicím ISMS, které jsou požadovány v ISO/IEC 27001 4.2.1 a).



Proces řízení rizik bezpečnosti informací lze používat pro organizaci jako celek, jakoukoliv samostatnou část organizace (například oddělení, fyzické místo, službu), jakýkoliv informační systém, stávající nebo plánované nebo konkrétní aspekty opatření (například plánování kontinuity činností organizace).

Proces řízení rizik bezpečnosti informací musí být nedílnou součástí řízení organizace, musí být zakotven v kultuře a praxi organizace a musí být uzpůsoben jejím procesům.

Závěrem bych rád upozornil, že implementací strategického rámce a procesu řízení rizik mají organizace zajištěnou plnou integraci řízení rizik do stávajících procesů na všech úrovních. Tyto organizace rovněž předejdou neefektivnímu způsobu řízení rizik bezpečnosti informací , který se vyznačuje mnohými závažnými nedostatky (např. řízením rizika bez kontextu, neefektivním způsobem identifikace rizik a rizikových faktorů, příliš obecným definováním rizik, nezapojením interních a externích zainteresovaných stran či diskontinuitou celého procesu).

Dotazy?

pplk. Ing. Radek Dubec, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra celoživotního vzdělávání
E-mail.: radek.dubec@unob.cz

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Dotazy?