Úvod do řízení rizik

Řízení rizik

Jedná se o oblast řízení, která se zaměřuje na analýzu a snižování rizik. Cílem analýzy rizik je eliminace **či** snížení a vlastně ve své podstatě i odhalení všech potencionálních rizik.

Co je to riziko? Dle definice MV ČR = Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě tzv. analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit.)[1]

Slovník pojmů[1] :

Riziko – potenciální událost v budoucnosti s negativními následky. Riziko tedy může a nemusí nastat. Určitá rizika jsou spojená s každou činností, v chodu každé organizace proto rizika vždy byla, jsou a budou přítomna. Cílem proto není všechna rizika eliminovat, ale být si jich vědom a pracovat s nimi (tj. řídit je).

Řízení rizik – integrální součást každého rozhodování v organizaci. Soustavná činnost, jejímž cílem je omezit pravděpodobnost výskytu rizik nebo snížit jejich dopad. Účelem řízení rizik je předejít problémům či negativním jevům, tj. zamezit vzniku problémů a vyhnout se tím nutnosti krizového řízení.

Významnost rizika – relativní důležitost rizika pro organizaci, která je zpravidla vyjádřena součinem pravděpodobnosti rizika a dopadu rizika. (Dále jen V).

Pravděpodobnost rizika – míra pravděpodobnosti výskytu rizikové události v budoucnosti měřená dle převažující praxe na škále 1-5 (1 nejméně pravděpodobné, 5 nejvíce pravděpodobné). (Dále jen P).

Dopad rizika (účinek na organizaci) – rozsah negativního dopadu či ztráty, která organizaci vznikne v případě výskytu rizikové události. Lze do něj zahrnout jak přímé finanční ztráty či dodatečné náklady, tak i dopady nefinančního 4 charakteru, např.

[1] https://www.mvcr.cz/clanek/riziko.aspx

ztrátu dobré pověsti, snížení kvality služeb pro občany atd.). Dopad rizika se dle převažující praxe opět měří na škále 1-5 (1 nejmenší negativní dopad, 5 největší negativní dopad). (Dále jen D).

Mapa rizik – výsledek analýzy rizik; přehled identifikovaných rizik organizace, může být v programu seřazených podle jejich významnosti, který slouží jako jeden z podkladů pro sestavování – tyto mapy rizik slouží a pro účely řízení rizik organizace jejím vedením.

Vrcholové vedení organizace – 1. a 2. stupeň řízení organizace, ředitel a náměstci, vedoucí klíčových odborů, např. ekonomického či finančního odboru, odboru informatiky, odboru právního

Vedoucích pracovníci na ostatních úrovních řízení – ostatní vedoucí pracovníci na nižších stupních řízení organizace.

Řízení rizik je soustavná, opakující se sada navzájem provázaných činností, jejichž cílem je řídit potenciální rizika, tedy omezit pravděpodobnost jejich výskytu nebo snížit jejich dopad na organizaci a její cíle. **Účelem řízení rizik** je předejít problémům či negativním jevům, vyhnout se krizovému řízení a zamezit vzniku problémů. Řízení rizik se skládá se z několika vzájemně provázaných fází - podle různých metodik se jich rozlišuje 4, 5, 6 nebo 8. Nejčastěji se využívá 6 základních fází a to:

- **identifikace rizik** (risk identification)
- **analýza rizik** (risk analysis)
- **zhodnocení rizik** (risk evaluation)
- **ošetření rizik** (risk mitigation)
- **zvládnutí rizik** (respektive jejich zmírnění)
- **monitoringu rizik** (risk monitoring and review)

Existuje celá řada oblastí, kde jsou rizika identifikována, ale v souhrnu lze rizika dělit do těchto základních druhů:

- ekonomická a finanční rizika
- projektová rizika
- tržní rizika
- technická rizika

- sociální rizika
- provozní rizika
- bezpečnostní rizika

Zásadní pro řízení rizik je jejich analýza. Pomocí **analýzy rizik** se zjišťuje míra nebezpečí (hrozba), kterým je organizace vystavena, jak moc jsou její aktiva vůči těmto hrozbám zranitelná, jak vysoká je pravděpodobnost, že hrozba nastane (zranitelnost) a jaký dopad to na organizaci může mít. Základní principy řízení rizik lze shrnout do následujících tvrzení:

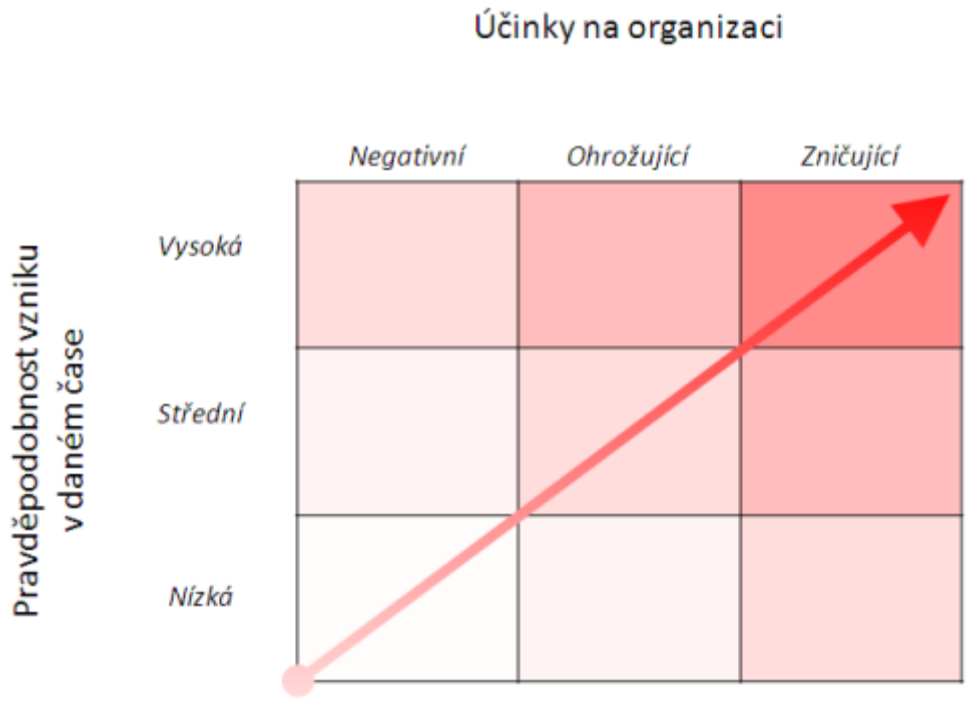
- Každá lidská činnost přináší určitá rizika
- Nulové riziko neexistuje

Odpovědnost za **řízení rizik** je v organizacích rozložena v rámci celého managementu. Nejvyšší odpovědnost má přirozeně vlastník, statutární orgán a nejvyšší management (top management) společnosti. V **malých organizacích** je odpovědnost za řízení rizik koncentrována na úrovni statutárního orgánu, protože není efektivní zaměstnávat specializovaného manažera rizik na plný úvazek. Ve středních a velkých organizacích je odpovědnost rozložena na jednotlivé manažery. Velké organizace nebo organizace podnikající v rizikovém prostředí (například banky, pojišťovny, petrochemický a energetický průmysl, letecký průmysl, doprava) mají určeného specialistu (manažera rizik). Téměř vždy je řízení rizik spojeno s rolí finančního ředitele, neboť dopady rizik (škody) i protiopatření lze finančně vyjádřit a mají dopad na finanční plánování.

Winterlingova matice[2] – grafické znázornění používané pro interpretaci mapy rizik, vychází ze vztahu

V=PxD (významnost= pravděpodobnost x dopad)

Matice se graficky znázorňuje takto:



Obecné předpoklady funkčního řízení rizik[1,3]

Úspěšnost zavedení kteréhokoliv z výše uvedených modelů řízení rizik v praxi má několik obecně platných předpokladů, mezi které patří v rámci každé organizace.

Zejména:

1. Jednoznačná organizační struktura a funkční organizační řád, ve kterém jsou vymezeny přesně, srozumitelně a v souladu se skutečností odpovědnosti jednotlivých organizačních útvarů tak, aby se vzájemně nepřekrývaly a aby naopak nedocházelo k existenci agend či činností, ke kterým nemá odpovědnost stanovenu žádný z organizačních útvarů.

2. Vhodně definované pracovní náplně jednotlivých zaměstnanců, které jsou v souladu s organizačním řádem a zároveň odpovídají skutečně vykonávaným agendám a činnostem.

3. Jasně, srozumitelně a konkrétně formulovaný etický kodex organizace schválený a podporovaný jejím vrcholným vedením, nejlépe doplněný o proškolení zaměstnanců v této oblasti.

4. Jasně stanovená pravidla v klíčových oblastech vnitřního chodu organizace, která jsou ve vzájemném souladu (zejména směrnice o oběhu účetních dokladů; schvalovací postupy a oprávnění; jednací řády).

Jedná se o základní stavební kameny každé organizace, o které se následně může opřít jakýkoliv řídící a kontrolní mechanismus včetně řízení rizik.

Rozhodování o rizicích[1,3] :

Při rozhodování o riziku je potřeba mít na paměti zejména relativní význam daného rizika pro organizaci. Tomuto ukazateli se obecně říká významnost rizika a stanovuje se jako součin pravděpodobnosti rizika a dopadu rizika, jež se v praxi nejčastěji měří na škále 1-5 (blíže viz Slovník). Při rozhodování o dalším postupu při řízení daného rizika je však nutné zohlednit5 rovněž další dva faktory, kterými jsou:

- Schopnost dané riziko řídit (tj. ovlivnit jeho další vývoj), a to nikoliv pouze já osobně jako jedinec, ale já jako součást dané organizace prostřednictvím všech kroků a nástrojů, které mám jako součást této organizace k dispozici (mohu např. požádat někoho dalšího o součinnost, informovat nadřízené atd.)

- Náklady spojené s řízením rizika – cílem jednoznačně je, aby náklady na řízení rizika nepřevyšovaly úspory plynoucí z jeho eliminace . Tyto faktory není nutné nijak přehnaně formalizovaně vyčíslovat či škálovat, stačí je pouze přiměřeně zohlednit v úvaze o dalším postupu při řízení daného rizika.

K řízení rizika lze následně zvolit některý z následujících přístupů:

- Vyvarování se rizika (např. neschválení dané operace, zákaz vykonání rizikové aktivity nebo procesu; organizace si však musí dát pozor, zda takovým opatřením nevznikají rizika jiná, která mohou být ještě významnější).

- Udržování rizika na stávající míře významnosti (akceptace rizika a sledování jeho vývoje bez dalších opatření k jeho eliminaci; k těm by případně došlo, až pokud by se kriticky zvýšila významnost rizika).

- Redukce rizika – přijetí nápravných opatření vedoucích ke snížení pravděpodobnosti výskytu rizika nebo jeho dopadu na přijatelnou mez.

• Přenos / sdílení rizika s někým dalším – snížení případného negativního dopadu tím, že je částečně přenesen na další osoby (např. na dodavatele v rámci smluvního vztahu, pojištěním rizika apod.; za takovou službu se však zpravidla vždy platí a organizace by si měla dobře spočítat, zda se jí takový postup skutečně vyplatí nebo nikoliv) Organizace by se měla prostřednictvím svých vedoucích pracovníků soustředit primárně na řízení rizik s vysokou, příp. střední mírou významnosti. U rizik s nízkou mírou významnosti lze doporučit taktiku udržování rizika. Každé riziko by mělo být řízeno subsidiárně na té úrovni řízení, která je k tomu vybavena potřebnými znalostmi a kompetencemi. V opačném případě je potřeba riziko dobře popsat, pokusit se definovat vhodná nápravná opatření a včas jej předat na vyšší úroveň řízení. Optimálním a přirozeným nosičem takových informací v organizaci je materiál, podklady pro poradu vedení organizace, podklady připravované ke schválení veřejné zakázky, studie proveditelnosti, investiční záměr atd. Pro účely řízení rizik rozhodně není nutné vytvářet nové samostatné dokumenty, stačí úplné a v maximální možné míře objektivní informace o rizicích v přehledné podobě (nejlépe včetně návrhu souvisejících opatření k řízení rizik) zahrnout do podkladů, na základě kterých příslušná osoba či orgán o té které operaci rozhoduje.

Modely řízení rizik uplatňované v praxi[1,3]

Centralizovaný model řízení rizik

Stručný popis: Řízení rizik organizace má na starosti Výbor pro řízení rizik složený z vrcholového vedení organizace. Ke koordinaci činností v oblasti řízení rizik napříč organizací a přípravě podkladů pro jednání a rozhodování Výboru pro řízení rizik je pověřen jeden ze zaměstnanců organizace (manažer rizik). Předpoklady Pracovník, který má v organizaci na starosti koordinaci řízení rizik musí mít dostatek znalostí, zkušeností, kompetencí a důvěry ze strany vrcholového vedení organizace i vedoucích pracovníků na ostatních úrovních řízení, aby byl schopen zajistit:

• Aktivní a otevřenou komunikaci s členy Výboru pro řízení rizik

• Přípravu úplných a pravdivých podkladů (ve spolupráci s vedoucími pracovníky na všech úrovních řízení a odbornými útvary) včetně zahrnutí negativních informací a možných dopadů souvisejících s danou operací, které jsou pro rozhodování o dalším postupu relevantní

• Předkládání těchto podkladů Výboru pro řízení rizik a aktivní účast při jejich projednávání Členové Výboru pro řízení rizik musí být ochotni a schopni existenci rizik u operací ve své gesci akceptovat, nesnažit se je marginalizovat a dále s nimi pracovat, a to nikoliv pouze individuálně, ale i před ostatními členy vrcholového vedení organizace.

Výhody:

Umožňuje organizaci klást důraz na řízení rizik v podobě samostatných aktivit zaměřených na zjišťování, vyhodnocování, monitorování a vykazování významných rizik v organizaci. Při správném provádění dává vrcholovému vedení organizace přiměřenou jistotu, že klíčová rizika jsou vedoucími pracovníky na příslušných úrovních organizace opravdu důsledně řízena.

Nevýhody:

Mezi nejčastěji identifikované nedostatky řízení rizik patří sklon k formalismu, chápání mapy rizik či katalogu rizik organizace jako cíle aktivit v oblasti řízení rizik, nikoliv jako pouhého nástroje pro aktivní řízení rizik vedením organizace, a přílišný důraz na kvantifikaci významnosti rizik, nikoliv na další práci s nimi. Všechny tyto nedostatky zavedení centralizovaného modelu řízení rizik spíše přirozeně podporuje, než aby jim zamezovalo. Jedná se proto o model v prostředí neziskových organizací vhodný spíše jen pro ty organizace, které se skutečně pohybují v rizikovém prostředí a kde je proto fungování systému řízení rizik v podobě samostatných aktivit zaměřených na zjišťování, vyhodnocování, monitorování a vykazování významných rizik klíčové pro jejich úspěšné fungování. V ostatních organizacích, které se pohybují ve standardním prostředí, kde je nejhorším možným negativním dopadem špatného rozhodnutí finanční ztráta, dodatečné náklady či případné správní nebo soudní řízení, není tento model řízení rizik příliš účelný a v praxi mají tendenci se projevovat spíše jeho nevýhody.

Decentralizovaný model řízení rizik

Stručný popis: Řízení rizik je integrální součástí každého rozhodnutí, které je v rámci organizace jejími vedoucími pracovníky přijímáno. Od určité hladiny významnosti

přijímaného rozhodnutí musí mít řízení rizik svou dokumentovanou podobu, aby o něm v organizaci zůstávala auditní stopa. Hladinu významnosti si organizace určí sama ve svých vnitřních předpisech a může, resp. měla by být pro různé typy operací v různých oblastech různá (podle rizikovosti operací daného typu v dané oblasti pro organizaci obecně).

Předpoklady fungování: Vedoucí pracovníci na všech úrovních řízení musí chápat, co je to riziko a jak se s ním pracuje a vědomě tyto znalosti uplatňovat v praxi při řízení jím svěřeného útvaru, vždy přiměřeně k operaci, o které rozhodují.

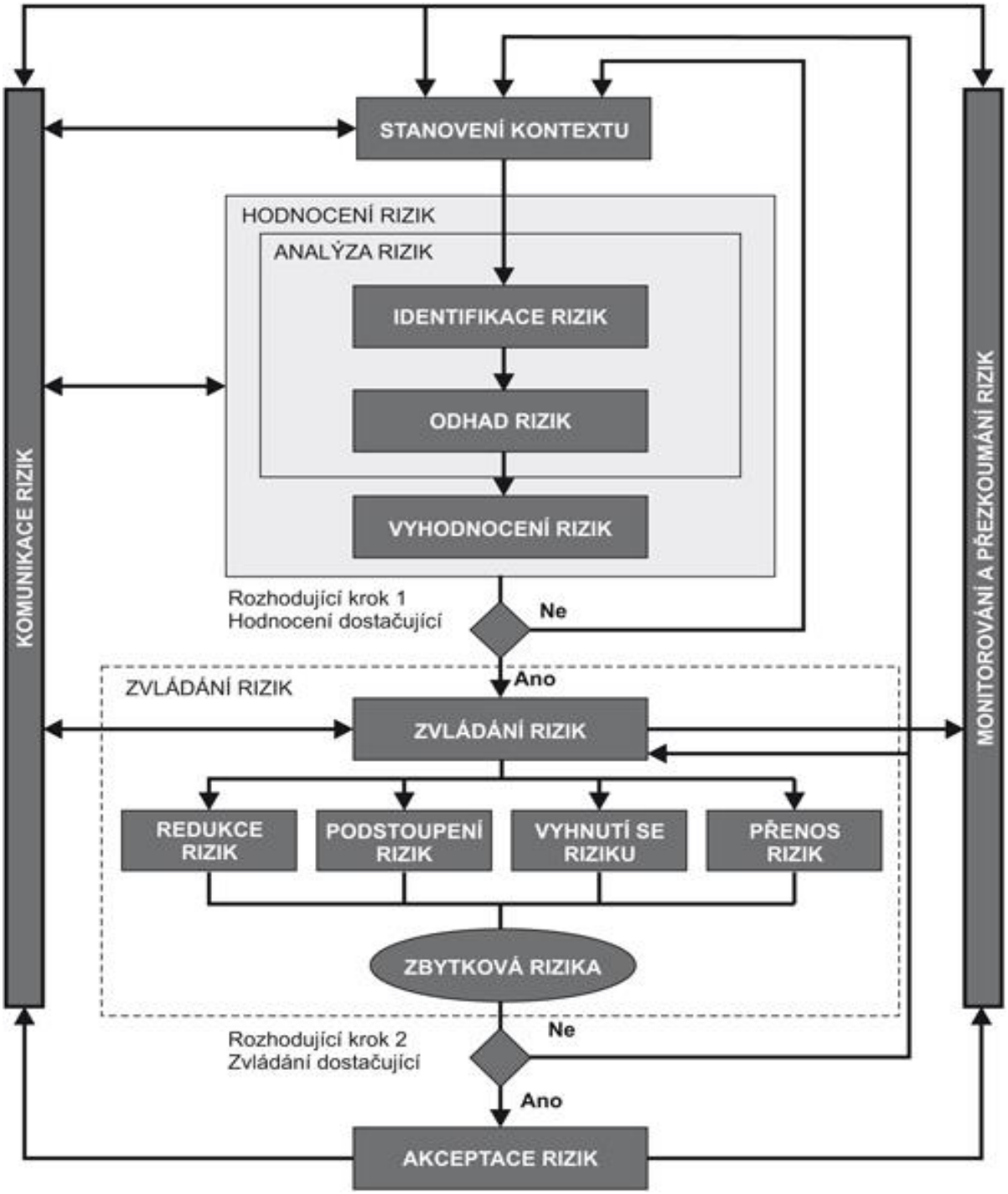
Výhody:

Eliminuje většinu nevýhod centralizovaného modelu řízení rizik. Nepředpokládá existenci centrálního koordinátora rizik, po kterém lze v prostředí veřejné správy přirozeně jen velmi obtížně požadovat takovou míru znalostí, zkušeností a kompetencí, aby byl v diskusi o řízení rizik rovnocenným partnerem vrcholovému vedení organizace.

Nevýhody:

Aby fungoval optimálně, vyžaduje aktivní účast všech vedoucích zaměstnanců na jednotlivých úrovních řízení. Podmínkou dobrého fungování decentralizovaného modelu řízení rizik však není, aby byl uplatňován hned od prvního okamžiku dokonale plošně napříč celou organizační strukturou. Někde může fungovat lépe a někde hůře, záleží na konkrétních vedoucích pracovnících. Postupně lze napříč organizací sjednocovat formou přenášení dobré praxe z útvarů, kde funguje, na ty ostatní.

Algoritmus možného řízení rizik [4]:



ISO 31000 –

Smysl standardu:

Záměrem standardu je zajištění ovlivňování rizik podnikání s ohledem na vnitřní a vnější prostředí a to vhodným zvládáním rizik tak, aby docházelo k omezování výskytu rizik s ohledem na jejich dopady na organizaci.

Použití / uplatnění standardu:

Tento standard definuje požadavky na systém managementu rizik a je aplikovatelný na všechny typy organizací, může být použit jak pro služby, tak pro výrobní sektory. Je použitelný pro jakýkoli typ a velikost organizace.

Charakteristika standardu:

Základem standardu je identifikace a hodnocení všech možných rizik podnikání a jejich vhodné zvládání (např. vyhnutí se riziku, omezení rizika nebo výcvik pracovníků) za účelem minimalizace dopadů rizikových událostí.

Hlavní přínosy standardu:

- zvýšení konkurenceschopnosti za pomocí včasného rozpoznání a zvládání možných rizik,
- lepší připravenost organizace na výskyt rizikových událostí,
- redukce nákladů spojených s následky výskytu rizikových událostí,
- předcházení nebo omezování nových rizik díky systému identifikace a hodnocení rizik (včasný varovný systém).

ISO/IEC 27001 - Management bezpečnosti informací

Historie

Prvním standardem zahrnující požadavky na bezpečnost informací byl BS 7999. Cílem této první normy bylo definovat požadavky na ochranu informací obecně, tedy uložených nejen na elektronických médiích, ale i tištěných nebo sdělovaných slovem nebo obrazem. Protože rozvoj technologií od roku 2000 přinesl IT technologiím v oblasti informací dominantní roli, vyvolalo toto nutnost vytvořit v roce 2006 normu ISO 27001 a následně v roce 2013 novelizovat.

Princip normy

Norma ISO 27001 je mezinárodně platný standard, který definuje požadavky na systém managementu bezpečnosti informací.
Norma specifikuje požadavky na řízení bezpečnosti informaci, kdy požaduje po firmě, aby s veškerými interními nebo informacemi sdílenými se svými partnery nebo zaměstnanci nakládala tak, aby nedošlo k jejich ztrátě, zneužití nebo i pouze narušení důvěry.

Přínos normy pro organizaci

· přináší díky standardizaci procesů zefektivnění činnosti při klasifikaci rizik spojených se ztrátou nebo zneužití informací

· umožní jednotlivým firmám získat důvěru při sdílení informací se svými obchodními partnery

· sníží riziko vícenákladů souvisejících možnými s neočekávanými událostmi

· redukuje náklady spojené údržbou a rozvojem informačních technologií ve firmě

· zlepší přístup státních kontrolních úřadů, včetně nově požadované legislativy se Směrnicí GDPR.

Seznam použité literatury :

1. Ministerstvo financí ČR, Metodika CHJ č.2, www.mfcr.cz
2. Ministerstvo financí ČR, Metodický pokyn CHJ č.006, www.mfcr.cz
3. Management media, https://managementmania.com/cs/winterlingova-krizova-matice
4. Management media, https://www.businessinfo.cz/metody-snizovani-rizika/
5. Https://managementmania.com/cs/rizeni-rizik)
6. ISO - International Organization for Standardization