IT a anatomie firmy

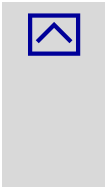
(Řízení rizik)

(pracovní dokument)

Mariia Shevchenko

VŠE Praha, 2026

Obsah



Text se věnuje základním vymezením problematiky risk managementu. ***Účelem*** je definovat ***pojem riziko a jeho základní klasifikace***. Následně charakterizovat samotný ***proces risk managementu***, jeho cíle a životní cyklus. Text představuje dále i ***koncept Enterprise Risk Managementu*** jako integrovaný přístup k řízení rizik napříč organizací, včetně jeho přínosů a praktických nástrojů využívaných v praxi a poukazuje i na limity tradičního přístupu a identifikuje ***klíčové faktory ovlivňující efektivitu*** systému řízení rizik.

1. Základní vymezení rizika

V odborné literatuře neexistuje jednotná definice rizika, ale lze identifikovat společné prvky, které se opakují v různých zdrojích. Podle normy ***ISO 31000 riziko je definováno jako***

„effect of uncertainty on objectives“

Tento účinek představuje jakoukoli ***odchylku od očekávaného stavu***, ať už negativní nebo pozitivní (ISO 31000, 2018).

Historicky pojem riziko byl chápán spíše jako nebezpečí ztráty či nezdaru. Ale v současném ekonomickém kontextu zahrnuje i ***změny výsledků a potenciál pro zisk***, například při investování (Smejkal & Rais, 2013). Riziko je neoddělitelně spojené s rozhodováním v situacích, kdy ***výsledek není jistý***, a obvykle se popisuje pomocí zdrojů rizika, potenciálních událostí, jejich následků a pravděpodobnosti, že nastanou (Majumder & Dey, 2024).

1.1 Klasifikace rizik

Klasifikace rizik představuje základní stavební kámen efektivního řízení podniku. Správná klasifikace umožňuje organizacím ***identifikovat potenciální hrozby***, lépe jim porozumět a následně přiřadit k nim ***odpovídající opatření***. Vzhledem k tomu, že neexistuje jeden univerzální seznam rizik platný pro všechny subjekty, měla by být kategorizace vždy ***přizpůsobena velikosti, složitosti a specifickému kontextu*** dané organizace. Rizika se nejčastěji dělí podle jejich povahy, vztahu k ekonomickému prostředí a oblastí podniku (Smejkal & Rais, 2013).

Podle Hopkina (Hopkin, 2018) existují čtyři ***hlavních typy rizik***:

- compliance risks,
- hazard risks,
- control risks,
- opportunity risks.

Compliance rizika souvisejí ***s dodržováním zákonů, předpisů a regulačních požadavků***. Jsou zvláště významná v regulovaných odvětvích a organizace se obvykle snaží dosáhnout dodržování těchto pravidel.

Hazardní rizika jsou taková, která mohou pouze negativně ovlivnit nebo znemožnit dosažení cílů. Typicky jde o ***pojistitelná rizika*** jako požár, krádež či jiné škody a jsou spojena s narušením běžného provozu.

Kontrolní rizika vyvolávají pochybnost o tom, zda bude organizace schopna svých cílů dosáhnout v důsledku ***selhání interních procesů, řízení nebo lidí***. Patří sem například riziko podvodu nebo nedodržení interních postupů.

Rizika příležitostí jsou na rozdíl od předchozích často vědomě podstupována, protože přinášejí možnost vyššího zisku či růstu. Například ***investice do inovací nebo expanze*** na nové trhy. Mohou sice přinést ztrátu, ale zároveň představují klíčový faktor dlouhodobého rozvoje (Hopkin, 2018).

Jedním z dalších ***členění je rozlišení na rizika čistá a spekulativní***. ***Čisté riziko*** popisuje situace, kde existuje pouze možnost ztráty nebo zachování stávajícího stavu. ***Spekulativní riziko*** v sobě zahrnuje možnost ztráty i zisku a skoro vždycky je součástí podnikání a investování.

Další významné hledisko dělí rizika na ***statická a dynamická*** podle jejich závislosti na změnách v prostředí. ***Statická rizika*** se vyskytují v stálém ekonomickém prostředí a jsou nezávislá na vývoji trhu. ***Dynamická rizika*** jsou naopak přímo spojena se změnami v ekonomice, technologiích nebo preferencích spotřebitelů (Smejkal & Rais, 2013).

1.2 Risk management a jeho význam v organizacích

Podobná situace, jako u pojmu riziko, nastává i během hledání jednotlivé definice risk managementu. Každý autor tento pojem vysvětluje jinak. Norma ***ISO 31000 definuje risk management*** následně:

„coordinated activities to direct and control an organization with regard to risk.“

Tradiční přístup k řízení rizik byl často omezen na určité funkční oblasti organizace, například finance nebo výrobu. Což pak vedlo k tomu, že jednotlivá rizika nebyla posuzována v širším kontextu celkové strategie organizace. V současné době tento pojem je mnohem širší. ***Risk management*** představuje ***systematický přístup k identifikaci, analýze a řízení rizik***, která mohou ovlivnit dosažení cílů organizace. Risk management není vnímán pouze jako ochranný mechanismus, ale jako ***podstatná součást strategického řízení***, která pomáhá vedené při rozhodování (Hampton, 2009).

1.2.1 Cíle risk managementu

Hlavním cílem risk managementu je ***omezovat negativní dopady nejistých událostí*** a současně ***podporovat stabilitu a dlouhodobou udržitelnost*** organizace. Firmy, které pravidelně řídí rizika, jsou lépe připraveny reagovat na změny v business prostředí a efektivně alokovat své zdroje. Identifikace klíčových rizik ***umožňuje*** managementu ***stanovit priority*** a zaměřit se na ***oblasti s největším dopadem*** na organizaci. Tím se snižuje pravděpodobnost nečekaných ztrát a zvyšuje se stabilita podnikových procesů (Majumder & Dey, 2024).

Risk management má významný vliv také na ***zvyšování kvality rozhodovacích procesů***. Systematické shromažďování a vyhodnocování informací o rizicích poskytuje managementu podklady pro rozhodnutí. Díky tomu mohou organizace lépe ***předvídat možné změny*** a připravovat se na různé varianty budoucího vývoje. Tento přístup zlepšuje schopnost organizace ***reagovat na krizové situace*** a minimalizovat jejich dopady (Smejkal & Rais, 2013).

Dalším významným přínosem risk managementu je ***podpora souladu s právními a regulačními požadavky***. Identifikace a řízení právních a regulačních rizik napomáhá organizacím předcházet sankcím, soudním sporům a poškození reputace (ISO 31000, 2018).

Kromě toho risk management hraje klíčovou roli v oblasti ***interní kontroly a auditu***. Poskytuje rámec pro ***hodnocení účinnosti kontrolních mechanismů*** a identifikaci slabých míst v procesech organizace. Prostřednictvím pravidelného monitorování rizik lze včas odhalit odchylky od stanovených cílů a přijmout nápravná opatření. Tento přístup podporuje neustálé zlepšování procesů a zvyšování celkové efektivity organizace (Hampton, 2009).

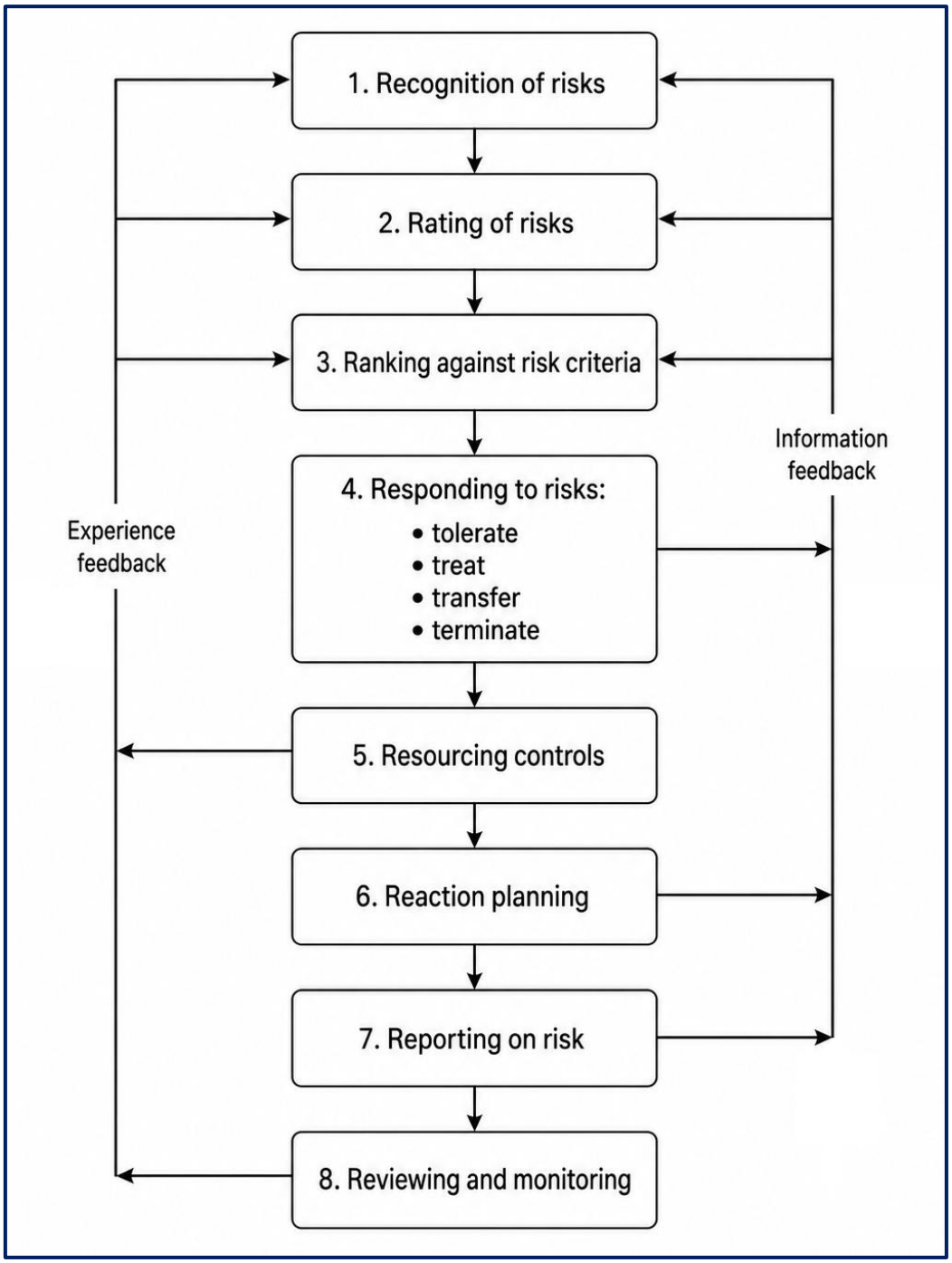
V současné době se význam risk managementu dále zvyšuje v důsledku rostoucího objemu dat, složitosti a nejistoty. ***Technologický rozvoj a regulatorní změny přinášejí nové typy rizik***. Organizace, které vnímají risk management jako integrální součást svého řízení, získávají konkurenční výhodu a zvyšují svou schopnost dlouhodobě uspět na trhu (Majumder & Dey, 2024).

1.2.2 Risk management lifecycle

Risk management lifecycle představuje ***systematický a opakující se proces řízení rizik***, který zajišťuje jejich ***identifikaci, hodnocení, řízení i průběžné sledování***. Obrázek 1-1 znázorňuje princip 8Rs and 4Ts.

8 Rs označuje ***osm klíčových kroků*** procesu: Recognition, Rating, Ranking, Responding, Resourcing controls, Reaction planning, Reporting a Reviewing.

4 Ts představují ***čtyři základní strategie reakce na riziko***: Tolerate, Treat, Transfer a Terminate.



Obrázek 1-1 Risk management lifecycle (Zdroj: Hopkin, 2018)

Proces začíná ***identifikací rizik a povahy a okolností***, za kterých rizika mohou nastat. Identifikace rizik zahrnuje jak ***interní faktory***, například organizační strukturu, lidské zdroje nebo technologické procesy, tak ***externí faktory***, mezi které patří legislativní změny, tržní vývoj nebo chování konkurence. Cílem této fáze je vytvořit co nejúplnější přehled rizik, kterým organizace čelí.

Následuje ***hodnocení***, kdy se posuzuje ***velikost dopadu a pravděpodobnost výskytu***. Toto hodnocení může mít kvalitativní, kvantitativní nebo kombinovaný charakter, přičemž volba konkrétní metody závisí na dostupnosti dat, složitosti rizika a potřebách managementu.

Poté probíhá ***porovnání s předem stanovenými kritérii organizace***, aby bylo možné určit, která rizika jsou přijatelná a která vyžadují zásah. Hodnocení rizik je ***klíčové pro efektivní alokaci zdrojů*** a zaměření pozornosti na ***rizika s největším potenciálním dopadem*** na firmu.

Další fází je reakce na rizika. V této fázi firma má na ***výběr čtyři možnosti***:

- tolerate – přijmout riziko bez dalšího zásahu,
- treat – snížit pravděpodobnost nebo dopad prostřednictvím kontrolních opatření,
- transfer – přenést riziko na jiný subjekt (outsourcing),
- terminate – ukončit činnost, která riziko způsobuje.

Pak následuje ***zajištění zdrojů pro kontrolní opatření,*** aby byla přijatá opatření skutečně implementována. Součástí cyklu je také ***plánování reakcí***, zejména pro krizové situace. Proces pokračuje ***reportingem a monitoringem***, tedy sledováním výkonnosti řízení rizik a ***komunikací výsledků***, a končí ***revizí a přezkumem systému***, což zajišťuje jeho aktualizaci a neustálé zlepšování. Celý cyklus je dynamický a opakuje se na základě zpětné vazby a nových informací.

Model 8Rs a 4Ts tak poskytuje ***přehledný rámec pro řízení rizik*** od jejich identifikace až po strategické rozhodnutí a zdůrazňuje nutnost průběžného monitoringu a zlepšování celého systému (Hopkin, 2018).

Proces řízení rizik lze tedy chápat jako ***cyklický a neustále se opakující mechanismus***, který podporuje stabilitu a rozvoj organizace. Jeho systematická aplikace umožňuje organizacím nejen předcházet negativním událostem, ale také aktivně pracovat s nejistotou a využívat příležitosti k dosažení strategických cílů (Smejkal & Rais, 2013).

1.3 Enterprise Risk Management

Enterprise Risk Management (ERM) představuje ***komplexní a integrovaný přístup k řízení rizik*** v celé organizaci. Na rozdíl od tradičního pojetí risk managementu, které se často zaměřovalo na jednotlivé oblasti nebo typy rizik, ERM usiluje o systematické ***řízení všech rizik v jejich vzájemných souvislostech (***Majumder & Dey, 2024).

Základní princip ERM spočívá v tom, že ***jednotlivá rizika nelze řídit izolovaně***, protože mezi nimi existují vzájemné vazby a závislosti. ERM proto klade důraz na koordinaci řízení rizik ***napříč všemi organizačními úrovněmi a oblastmi.*** Tím se zvyšuje schopnost organizace efektivně reagovat na komplexní a dynamické změny v podnikatelském prostředí (Hampton, 2009).

1.3.1 Přínosy ERM

Hlavním přínosem Enterprise Risk Managementu je ***tvorba a ochrana hodnoty*** organizace. Tento přístup se posouvá od tradiční defenzivní ochrany aktiv ***k aktivnímu zvyšování hodnoty firmy***. Klíčovým cílem je dosáhnout strategických cílů, vizí a misí podniku. ERM umožňuje organizacím nejen ***identifikovat a minimalizovat hrozby***, které by mohly ohrozit jejich existenci, ale také rozpoznat a využít ***příležitosti k získání konkurenční výhody*** na trhu. Pokud je například strategickým cílem přežití, systém se zaměřuje na cash flow, zatímco při strategii růstu se soustředí na řízení rizik spojených s investicemi a inovacemi.

Dalším přínosem ERM je ***zkvalitnění rozhodovacích procesů*** na všech úrovních řízení. Díky systematickému sběru a analýze dat o rizicích vedení má k dispozici lepší podklady pro kvalifikované rozhodování. Toto vede k ***efektivnější alokaci kapitálu*** a zdrojů tam, kde jsou nejvíce potřeba. To přímo ***přispívá k provozní efektivitě, optimalizaci nákladů a stabilitě výnosů***, protože firma dokáže lépe předcházet provozním narušením a minimalizovat nečekané ztráty (Majumder & Dey, 2024).

Významnou součástí ERM je také ***zajištění kontinuity podnikání*** (Business Continuity) a odolnosti organizace vůči krizím. Systém má za úkol připravit firmu na neočekávané události tak, aby byla schopna ***fungovat i v dobách potíží nebo se rychle zotavit***. V neposlední řadě ERM ***chrání reputaci společnosti***, čímž posiluje důvěru zákazníků a dalších zainteresovaných stran. Celkově tak ERM transformuje vnímání rizika z izolovaného problému na ***integrovanou součást strategického řízení,*** která prostupuje celou firemní kulturou (Hampton, 2009).

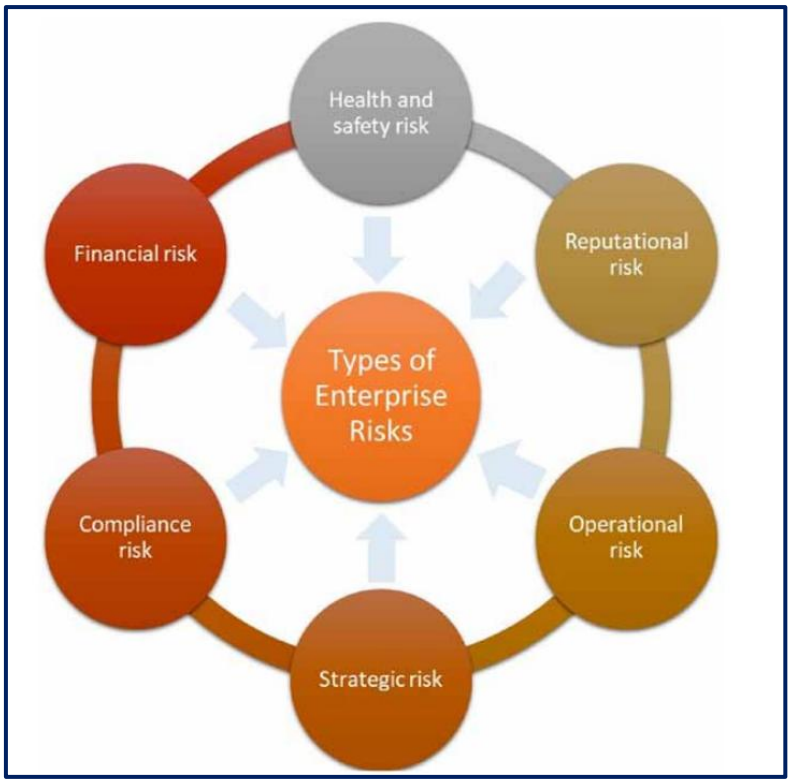
Tabulka 1-1 uvádí konkrétní přínosy ERM rozdělené podle oblastí.

Tabulka 1-1: Přínosy Enterprise Risk Managementu (Zdroj: Hopkin, 2018)

Oblast	Přínosy
Finanční	• Snížení nákladů na financování a kapitál • Lepší kontrola schvalování kapitálových výdajů • Zvýšení ziskovosti organizace • Přesné finanční reportování rizik • Posílené řízení a corporate governance
Provozní	• Efektivita a konkurenční výhoda • Dosažení stavu bez narušení provozu • Zlepšení vztahů s dodavateli a morálky zaměstnanců • Cílené snižování rizik a nákladů • Snížení provozních nákladů
Reputační	• Spokojenost regulátorů • Lepší využití značky společnosti • Zvýšení hodnoty pro akcionáře • Dobrá pověst a publicita • Zlepšení vnímání organizace
Tržní	• Maximalizace obchodních příležitostí • Lepší postavení na trhu • Zvýšení útrat (a spokojenosti) zákazníků • Vyšší míra obchodních úspěchů • Nižší míra obchodních selhání

1.3.2 Klasifikace rizik v kontextu ERM

V kontextu Enterprise Risk Management se využívá ***kategorizace podle oblastí***, které jsou ohroženy. Obrázek 1-1 dokumentuje klíčové typy rizik.



Obrázek 1-2: Kategorizace rizik (Zdroj: Majumder & Dey, 2024)

Rizika v oblasti BOZP

Bezpečnost a ochrana zdraví při práci se týká každého pracoviště, od kanceláří po stavby. Základem je ***identifikace fyzických, chemických či ergonomických rizik*** a následná implementace kontrolních mechanismů. Prioritou je fyzická i duševní pohoda zaměstnanců, které lze dosáhnout pouze skrze spolehlivou prevenci a důsledné hodnocení rizik (Majumder & Dey, 2024).

Reputační riziko

Dobré jméno firmy je ***klíčové pro vztahy s investory i zákazníky***. V éře sociálních sítí a globální komunikace se vnímání značky může změnit velmi rychle, což zvyšuje nároky na kvalitu strategického rozhodování. Jakékoli poškození reputace má přímý negativní dopad na celkovou efektivitu a stabilitu organizace (Majumder & Dey, 2024).

Operační riziko

Tato oblast se zaměřuje na ***hrozby plynoucí z vnitřních procesů***, ***selhání systémů nebo lidského faktoru, včetně kybernetických útoků či globálních krizí***. Pro minimalizaci škod musí organizace detailně znát své denní operace a mít připravený krizový plán. K efektivnímu řízení a identifikaci slabých míst v těchto funkčních doménách lze využít specializovaný software (Majumder & Dey, 2024).

Strategické riziko

Strategická rizika ***vyplývají z vnějších okolností***, které mohou vynutit ***změnu celkového směřování*** podniku. Každý obor čelí jiné míře hrozeb a příležitostí, ale včasná analýza těchto faktorů je nezbytná pro budoucí úspěch. Aktivní vyhledávání potenciálních strategických zádrhelů pomáhá zmírnit jejich dopady dříve, než nastanou (Majumder & Dey, 2024).

Compliance riziko

Tato rizika souvisejí ***s dodržováním zákonů, regulací a etických norem***, které se v globálním prostředí neustále vyvíjejí. Nedostatečná správa těchto pravidel může vést k vážným právním a finančním

postihům. Prioritizací managementu shody (např. pomocí digitálních modulů) získává firma ***jistotu v nepřehledném legislativním rámci*** (Majumder & Dey, 2024).

Finanční riziko

Finanční nestabilita hrozí ***při poklesu tržeb, neuvážených investicích nebo špatném řízení hotovosti***. Riziko zvyšuje také mezinárodní expanze, kde hrají roli ***výkyvy měnových kurzů***. Bez precizního finančního řízení je dosažení firemních cílů nereálné, přičemž tyto dopady jsou v praxi často nevyhnutelné a obtížně předvídatelné (Majumder & Dey, 2024).

1.4 Metody řízení rizik

Metody a nástroje řízení rizik představují praktické ***prostředky, pomocí nichž organizace identifikují, analyzují a hodnotí rizika a navrhují opatření k jejich ošetření***. Volba vhodných metod závisí na charakteru organizace, složitosti jejích procesů, dostupnosti informací a cílech řízení rizik. Správně zvolené nástroje umožňují systematický přístup k rizikům a ***podporují kvalitu rozhodovacích procesů*** na všech úrovních řízení.

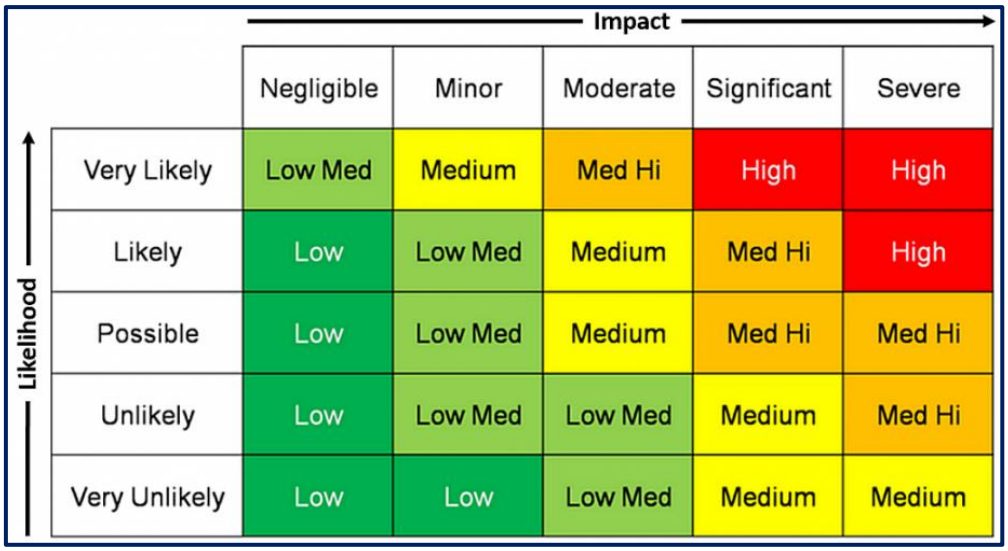
Pro řízení rizik lze využívat rovněž ***kvalitativní a kvantitativní metody***. Kvalitativní metody se opírají především o expertní odhady a slovní popis rizik, zatímco kvantitativní metody pracují s numerickými údaji a statistickými modely. Organizace proto často kombinují oba přístupy v závislosti na konkrétní situaci (Rejda et al., 2016).

Jednou ***ze základních metod identifikace rizik je brainstorming***, který spočívá ve strukturované diskusi skupiny odborníků nebo zaměstnanců s cílem odhalit potenciální rizikové faktory. Brainstorming je často využíván v počátečních fázích projektů nebo při zavádění nových procesů (Majumder & Dey, 2024).

SWOT analýza patří mezi často používané metody řízení rizik, zejména v oblasti strategického plánování. Metoda rozlišuje čtyři oblasti – silné stránky (Strengths), slabé stránky (Weaknesses), příležitosti (Opportunities) a hrozby (Threats). Z pohledu řízení rizik je klíčové zejména ***systematické posouzení slabých stránek a hrozeb,*** které představují potenciální zdroje interních a externích rizik. V rámci procesu identifikace rizik SWOT umožňuje strukturované zachycení rizikových faktorů napříč celou organizací. Výhodou této metody je její ***přehlednost a schopnost propojit interní a externí prostředí podniku do jednoho analytického rámce.*** SWOT analýza však sama o sobě neposkytuje kvantifikaci rizik ani jejich prioritizaci, a proto bývá zpravidla doplňována dalšími nástroji řízení rizik. V praxi tak SWOT často slouží jako ***vstupní fáze*** procesu řízení rizik, která vytváří základ pro následnou detailnější analýzu a návrh opatření ke snížení identifikovaných rizik (Hill & Westbrook, 1997).

Další významnou metodou je ***analýza příčin a následků (Root Cause Analysis).*** Tato metoda se zaměřuje na ***identifikaci základních příčin rizikových událostí*** a umožňuje lépe porozumět mechanismům jejich vzniku. Díky tomu lze navrhovat opatření, která neřeší pouze důsledky rizika, ale směřují ***k odstranění jeho hlavních příčin***. Root Cause Analysis je využívána zejména při řešení opakujících se problémů nebo incidentů (Majumder & Dey, 2024).

Matice rizik představuje jednu ***z nejpoužívanějších metod hodnocení rizik*** v organizacích. Jedná se o nástroj, který umožňuje systematicky posoudit ***význam rizik na základě dvou základních kritérií – pravděpodobnosti výskytu a dopadu.*** Výsledkem je grafické znázornění rizik ve formě matici podobně (Obrázek 1-3), kde jednotlivé kombinace hodnot určují míru rizika vyjádřenou barevně (např. zelená – nízké riziko, červená – vysoké riziko).



Obrázek 1-3: Matice rizik (Zdroj: Acebes et al., 2024)

Proces aplikace matice rizik navazuje na fázi identifikace rizik. Každému ***riziku je přiřazena hodnota pravděpodobnosti*** (např. velmi nízká až velmi vysoká) ***a hodnota dopadu*** (např. zanedbatelný až kritický). Následným vynásobením či kombinací těchto hodnot ***vzniká úroveň rizika***, která umožňuje ***jejich prioritizaci***. Rizika umístěná v horní části matice vyžadují okamžitá opatření, zatímco rizika s nízkým skóre mohou být pouze monitorována. Matice rizik je proto důležitým nástrojem pro rozhodování managementu o alokaci zdrojů a nastavení kontrolních mechanismů (Hopkin, 2018).

Výhodou této metody je její ***jednoduchost, přehlednost a univerzální použitelnost*** napříč různými odvětvími. Matice podporuje transparentní komunikaci rizik v rámci organizace a umožňuje vizuální prezentaci jejich závažnosti. Matice rizik je běžně ***doporučována v mezinárodních standardech*** řízení rizik, zejména v rámci ***Committee of Sponsoring Organizations of the Treadway Commission*** (COSO, 2017).

Podle normy ***ISO 31000*** metody a nástroje řízení rizik je nutné ***průběžně přizpůsobovat měnícím se podmínkám organizace a jejímu okolí***. Neexistuje univerzální nástroj vhodný pro všechny situace, a proto je důležité volit kombinaci metod, která odpovídá specifickým potřebám organizace. Efektivní využívání nástrojů řízení rizik podporuje systematičnost, transparentnost a dlouhodobou udržitelnost řízení organizace (ISO 31000, 2018).

2. Nástroje používané v praxi v řízení rizik

Risk management je v současné praxi ***podporován širokou škálou nástrojů***, které ***se liší svou komplexitou, účelem i mírou integrace do organizačních procesů.*** V praxi se nejčastěji setkáváme s kombinací tabulkových nástrojů, analytických a reportingových řešení typu Business Intelligence a specializovaných softwarových platforem pro Enterprise Risk Management.

2.1 Tabulkové nástroje

Nejrozšířenějšími nástroji používanými v praxi jsou tabulkové procesory, zejména ***Microsoft Excel a Google Sheets.*** Tyto nástroje jsou často využívány zejména ***v malých a středních organizacích*** nebo v projektech, kde není zaveden specializovaný systém řízení rizik. Excel i Google Sheets umožňují vytváření matic rizik, hodnocení pravděpodobnosti a dopadu rizik. Tabulkové nástroje jsou často využívány v raných fázích zavádění risk managementu nebo jako ***doplněk k sofistikovanějším řešením,*** například jako zdroj dat pro reporting a vizualizaci rizik.

Hlavní výhodou takových nástrojů je jejich ***dostupnost, flexibilita a nízké náklady*** na implementaci.

2.2 Analytické a reportingové nástroje

Další významnou skupinou nástrojů jsou ***analytické a reportingové platformy typu Business Intelligence.*** Mezi nejčastěji používané nástroje v této oblasti patří Microsoft Power BI, Tableau nebo Domo.

Tyto nástroje ***nejsou primárně určeny k samotnému řízení rizik***, ale slouží jako ***podpůrné nástroje*** pro analýzu, vizualizaci a reporting rizikových dat. V praxi jsou využívány zejména pro ***sledování klíčových rizikových indikátorů (KRI)***, ***identifikaci trendů*** rizik v čase a poskytování přehledných dashboardů pro management. BI nástroje umožňují ***integraci dat z různých zdrojů***, například z tabulkových nástrojů, databází nebo ERP systémů, a jejich následnou analýzu v reálném čase.

Podle metodických doporučení COSO je kvalitní reporting a komunikace rizik jedním z klíčových předpokladů efektivního systému enterprise risk managementu (COSO, 2017).

Význam BI nástrojů v risk managementu spočívá především ***v podpoře rozhodování a zvyšování transparentnosti rizik napříč organizací.*** BI nástroje ale nenahrazují procesy identifikace, hodnocení a řízení rizik, které musí být zajištěny organizačně a metodicky.

2.3 Specializované nástroje Enterprise Risk Managementu

Ve středních a velkých organizacích se stále častěji uplatňují ***specializované Governance, Risk and Compliance (GRC) systémy***. Tyto systémy představují integrovaná softwarová řešení určená k podpoře správy a řízení organizace, řízení rizik a zajištění souladu s právními a interními předpisy.

Obrázek 2-1 znázorňuje Magic Quadrant for Governance, Risk and Compliance (GRC) Tools, Assurance Leaders publikovaný společností Gartner k září 2025. Obrázek zachycuje ***jednotlivé dodavatelé softwarových řešení,*** mezi které patří AuditBoard, LogicManager, ServiceNow GRC nebo SAP GRC.

Obrázek 2-1: Magic Quadrant for Governance, Risk and Compliance (GRC) Tools, Assurance Leaders (Zdroj: Gartner, 2025)

V praktickém fungování GRC systémy umožňují ***centralizovanou evidenci rizik, řízení interních kontrol, sledování regulatorních požadavků a automatizaci schvalovacích a kontrolních procesů***. Organizace prostřednictvím těchto nástrojů vytvářejí registry rizik, přiřazují odpovědnosti jednotlivým vlastníkům rizik, nastavují kontrolní mechanismy a sledují klíčové rizikové ukazatele (KRI).

Na druhou stranu implementace GRC systému představuje ***náročný proces vyžadující organizační změny, úpravu interních procesů a investice*** do technologií i školení zaměstnanců. Efektivita systému proto závisí nejen na technologii samotné, ale také na nastavení firemní kultury řízení rizik.

Z výše uvedeného přehledu vyplývá, že v praxi ***neexistuje univerzální nástroj pro řízení rizik***. Organizace obvykle využívají kombinaci více nástrojů, které se vzájemně doplňují. Tabulkové nástroje slouží k základní evidenci rizik, BI nástroje k analýze a reportingu a specializované GRC systémy k systematickému řízení rizik na úrovni celé organizace. Efektivita risk managementu tak ***nezávisí pouze na použitém softwaru, ale především na správném nastavení procesů a metodiky řízení rizik*** v souladu s mezinárodními standardy.

2.4 Limity tradičního přístupu

Jedním ***z největších problémů zůstává rozdělení řízení***. V mnoha organizacích jsou rizika stále ***spravována izolovaně*** v rámci jednotlivých oddělení, kdy například IT řeší kybernetickou bezpečnost a finanční oddělení zajištění investice, aniž by docházelo k vzájemné komunikaci a koordinaci. Tento nedostatek vede k tomu, že vedení nevidí souvislosti mezi jednotlivými hrozbami, což způsobuje neefektivitu a může vést ***k duplicitním procesům či přehlédnutí kaskádových dopadů rizik*** napříč firmou (Majumder & Dey, 2024).

Kritickým faktorem, na kterém řízení rizik často selhává, je ***lidský faktor***. I při existenci správných procesů může dojít k selhání, pokud vedení špatně nastaví priority. Problémem je také ***odpor zaměst-***

nanců ke změnám a rozšířený názor, že řízení rizik je odpovědností pouze úzké skupiny specialistů, a ***ne součástí práce každého pracovníka***.

V rámci každodenní praxe je ***risk manažer*** nucen pracovat s poměrně vysokým počtem reportů a dashboardů. Ve finančním sektoru i o více než 15 specializovaných dashboardů zaměřených na různé typy rizik. Každý z těchto reportů vyžaduje alespoň ***základní kontrolu klíčových ukazatelů, identifikaci odchylek a případné vyhodnocení jejich dopadu***. Tento proces je časově náročný a může vést k přetížení manažera a zvýšenému riziku přehlédnutí významných odchylek.

3. AI v oblasti risk managementu

Umělá inteligence se v posledních letech stává ***významným nástrojem pro podporu procesů řízení rizik.*** Díky schopnosti analyzovat velké objemy dat a identifikovat komplexní vzorce umožňuje firmám efektivněji identifikovat, hodnotit a monitorovat rizika. Zatímco tradiční přístupy k řízení rizik často vycházejí především z historických dat a expertního posouzení, moderní ***AI technologie dokážou pracovat s rozsáhlými datovými soubory v reálném čase a generovat přesnější predikce*** potenciálních rizikových událostí (Yazdi et al., 2024).

Implementace AI tak přispívá k transformaci risk managementu ***z převážně reaktivního přístupu na přístup více prediktivní a proaktivní.*** Organizace mohou díky pokročilým analytickým nástrojům identifikovat potenciální hrozby dříve, než se projeví, a přijímat preventivní opatření, která minimalizují dopad rizik. (Wai, 2026).

3.1 Přínosy využití AI v risk managementu

Jedním z hlavních přínosů využití umělé inteligence v risk managementu je schopnost zpracovávat a ***analyzovat velké objemy dat v krátkém čase***. AI algoritmy mohou analyzovat historická data, identifikovat vzorce a na jejich základě vytvářet modely pro predikci budoucích rizikových událostí. (Farmer, 2025).

Dalším významným přínosem je ***zvýšení přesnosti rozhodovacích procesů.*** Umělá inteligence dokáže analyzovat velké množství strukturovaných i nestrukturovaných dat, což umožňuje získat ***komplexnější pohled na rizika.*** (Wai, 2026).

AI rovněž přispívá ***k automatizaci procesů*** v oblasti risk managementu. Automatizované systémy mohou průběžně monitorovat klíčové rizikové indikátory, analyzovat transakční data nebo generovat reporty. Tím dochází ke snížení administrativní zátěže a zaměstnanci se mohou více soustředit na interpretaci analytických výsledků. Další důležitou výhodou je ***schopnost AI identifikovat anomálie a potenciální podvody*** v datech. Algoritmy strojového učení mohou analyzovat chování a odhalit hodnoty, které mohou ukazovat rizikové aktivity. Tato schopnost je využívána například ve finančním sektoru při detekci podvodů (Farmer, 2025).

3.2 Aplikace AI v risk managementu

Umělá inteligence nachází uplatnění v celé řadě oblastí risk managementu napříč různými sektory. Jednou ***z nejrozšířenějších aplikací je oblast finančních rizik***, kde jsou AI modely využívány například pro hodnocení ***kreditního rizika***. Algoritmy analyzují historická finanční data a další relevantní informace, aby identifikovaly podezřelé transakce. AI je taky široce využívána ***v oblasti kybernetické bezpečnosti.*** Moderní systémy založené na strojovém učení dokážou analyzovat síťový provoz, chování uživatelů nebo systémové logy a identifikovat neobvyklé vzorce, které mohou signalizovat potenciální kybernetický útok. Díky tomu mohou organizace reagovat na bezpečnostní incidenty rychleji a efektivněji. (Farmer, 2025).

Další možností je ***řízení operačních rizik***. AI systémy mohou monitorovat interní procesy, ***výkon systémů nebo chování zaměstnanců*** a identifikovat potenciální problémy dříve, než přerostou v závažné problémy. (Wai, 2026).

Pokročilé AI technologie mohou být využívány také ***pro analýzu obrazových dat.*** Například v oblasti bezpečnosti nebo průmyslových provozů mohou algoritmy hlubokého učení analyzovat kamerové záznamy nebo satelitní snímky a identifikovat potenciální bezpečnostní hrozby nebo provozní anomálie (Yazdi et al., 2024).

3.3 Omezení využití AI v risk managementu

Implementace AI v risk managementu také má několik ***omezení***. Jedním z nejvýznamnějších problémů je ***kvalita a dostupnost dat***. AI modely jsou silně závislé na datech, na kterých jsou trénovány, a pokud jsou tato data neúplná nebo zkreslená, mohou vést k nepřesným nebo zavádějícím výsledkům (Gurung, 2024). Problémem může být také ***integrace AI do existujících systémů řízení rizik***. Implementace AI technologií často vyžaduje významné investice do technologické infrastruktury, dato-

vého managementu a rozvoje potřebných kompetencí zaměstnanců. Organizace proto musí plánovat implementaci AI a postupně ji integrovat do svých procesů.

V neposlední řadě je důležité zdůraznit, že AI by ***neměla nahrazovat lidské rozhodování***, ale spíše jej doplňovat. Efektivní risk management vyžaduje kombinaci analytických schopností AI a odborných znalostí člověka. Tento přístup, často označovaný jako ***„human-in-the-loop***“, umožňuje využít výhody AI při současném zachování kritického lidského posouzení v rozhodovacích procesech (KPMG, 2026).

4. Závěr

- Z provedené analýzy vyplývá, že ř***ízení rizik představuje nedílnou součást současného managementu*** a jeho význam pořád roste.
- Efektivní řízení rizik vyžaduje ***systematický a cyklický proces***, který propojuje identifikaci, hodnocení, reakci a průběžný monitoring rizik.
- Samotné ***využívání nástrojů či metod však není dostačující, rozhodující je jejich začlenění do strategického řízení a každodenního fungování organizace***.
- ***Enterprise Risk Management*** přináší vyšší úroveň koordinace a umožňuje lépe reflektovat vzájemné vazby mezi jednotlivými riziky.
- Současně se ukazuje, že ***tradiční přístupy k řízení rizik narážejí na významná omezení.***
- Rostoucí ***datová náročnost a regulatorní tlak*** navíc zvyšují ***administrativní zátěž,*** což může snižovat efektivitu rozhodovacích procesů.

5. Zdroje

Acebes, F., González-Varona, J.M., López-Paredes, A. et al. (2024). Beyond probability-impact matrices in project risk management: A quantitative methodology for risk prioritisation. Humanit Soc Sci Commun 11. Dostupné z: https://doi.org/10.1057/s41599-024-03180-5

COSO (2004). Enterprise Risk Management – Integrated Framework. Application Techniques. Committee of Sponsoring Organizations of the Treadway Commission. Dostupné z: https://www.macs.hw.ac.uk/~andrewc/erm2/reading/ERM%20-%20COSO%20Application%20Techniques.pdf

COSO (2017). Enterprise Risk Management – Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission. Dostupné z: https://static.poder360.com.br/2023/09/Diretriz-Enterprise-Risk-Management-Coso-2017.pdf

Farmer, D. (2025). AI in risk management: Top benefits and challenges explained. TreeHive Strategy. Dostupné z: https://www.techtarget.com/searchsecurity/tip/The-benefits-of-using-AI-in-risk-management

Gartner, (2025). Magic Quadrant for Governance, Risk and Compliance (GRC) Tools, Assurance Leaders. Dostupné z: https://www.logicgate.com/resources/reports/gartner-magic-quadrant-for-grc-tools-assurance-leaders/

Hampton, J. (2009). Fundamentals of Enterprise Risk Management : How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity. AMACOM. Dostupné z: http://ebookcentral.proquest.com/lib/vsep/detail.action?docID=452609

Hill, T. & Westbrook, R. (1997). SWOT Analysis: It's Time for a Product Recall. Long Range Planning, 46–52. Dostupné z: https://ftms.edu.my/images/Document/MOD001074%20-%20Strategic%20Management%20Analysis/WK6_SR_MOD001074_Hill_Westbrook_1997.pdf

Hopkin, P. (2018). Fundamentals of Risk Management. New York: Kogan Page. SBN 978-0-7494-8307-4

ISO (2018). ISO 31000. International standard. Risk management — Guidelines. Dostupné z: https://www.ler.uam.mx/Calidad-UAML/wp-content/uploads/2025/02/ISO-31000-2018.pdf

KPMG. (2026). AI is revolutionizing risk management. Dostupné z: https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/ai-revolutionizing-risk-management.pdf

Majumder, S. & Dey, J. (2024). A Notion of Enterprise Risk Management: Enhancing Strategies and Wellbeing Programs Available. Emerald Publishing. ISBN: 978-1-83797-736-9. Dostupné z: https://doi.org/10.1108/9781837977352

Rejda, G. et al. (2016). Principles of Risk Management and Insurance. Pearson Education. Boston. ISBN 978-0-321-41493-9, Dostupné z: https://fab.upt.edu.vn/wp-content/uploads/2020/04/Principles-of-risk-management-and-insurance_2016.pdf

Smejkal, V. & Rais, K. (2013). Řízení rizik ve firmách a jiných organizacích. Praha: Grada Publishing a.s. ISBN 978-80-247-4644-9