FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

Název:	Návrh systému pro identifikaci vzájemných závislostí rizik
Student:	Bc. Vilém Hujňák
Vedoucí:	Ing. Petra Pavlíčková, Ph.D.
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce zimního semestru 2021/22

Pokyny pro vypracování

Cílem práce je navrhnout systém pro identifikaci vzájemných závislostí rizik, tzv. domino efektu.

1) Prostudujte a popište stěžejní metodické přístupy k řízení rizik.
2) Analyzujte duality rizika, agregaci rizik a vzájemné závislosti rizik (vznik domino efektu).
3) Charakterizujte dostupné systémy pro řízení rizik, zejména se zaměřením na závislá rizika.
4) Navrhněte způsob posuzování rizik v kontextu rizikových scénářů, identifikujte vzájemné závislosti rizik a navrhněte přístup k posuzování možností vzniku domino efektu.
5) Navrhněte demonstrační program umožňující identifikovat domino efekt a jeho příčinná závislá rizika a vytvořte prototyp.
6) Zhodnoťte a doporučte další rozvoj.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 27. února 2020

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Diplomová práce

Návrh systému pro identifikaci vzájemných závislostí rizik

Bc. Vilém Hujňák

Katedra softwarového inženýrství
Vedoucí práce: Ing. Petra Pavlíčková, Ph.D.

20. května 2020

Poděkování

Děkuji vedoucí práce Ing. Petře Pavlíčkové, Ph.D. za konstruktivní připomínky a podněty k vypracování práce, společnosti Per Partes Consulting, s.r.o. za konzultace možných rizik na projektech a v neposlední řadě rodině a blízkým za podporu během psaní této práce i během celého studia.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, avšak pouze k nevýdělečným účelům. Toto oprávnění je časově, teritoriálně i množstevně neomezené.

V Praze dne 20. května 2020 .....

Odkaz na tuto práci

Hujňák, Vilém. *Návrh systému pro identifikaci vzájemných závislostí rizik.* Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2020.

Abstrakt

Tato práce se zabývá problematikou identifikace vzájemných závislostí rizik. Představuje současné stěžejní metodické přístupy řízení rizik a shrnuje současné poznatky o závislostech mezi riziky. V práci je navržen nový způsob strukturovaného popisu rizik – rizikový scénář – který umožňuje identifikaci několika typů vzájemných závislostí. Tyto závislosti byly nalezeny a byl vymyšlen způsob, jak je identifikovat a posoudit. Jedním specifickým typem je závislost v práci nazvaná kauzální nebo-li domino efekt. Dále je v práci navržen systém, který implementuje identifikaci vzájemných závislostí rizik a pomocí experimentů vyvinutým prototypem a s testovací množinou rizik jsou vyhodnoceny některá důležitá zjištění.

Klíčová slova riziko, rizikový scénář, agregace rizik, vzájemně závislá rizika, domino efekt

Abstract

This thesis deals with the issue of identifying risk interdependencies. It presents the current key methodological approaches to risk management and summarizes current knowledge about the dependencies between risks. The work proposes a new way of structured description of risks - risk scenario -

which allows the identification of several types of interdependencies. These dependencies have been found and a way has been devised to identify and assess them. One specific type is a dependency called a causal dependence or domino effect. Furthermore, an information system is proposed in the work, which implements the proposed method of identifying the interdependencies of risks. With the help of experiments with a developed prototype of the system and a set of test risks, some important findings are evaluated.

Keywords risk, risk scenario, risk aggregation, interdependent risks, domino effect

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Riziko je historický výraz, pocházející údajně ze 17. století, kdy se objevil v souvislosti s lodní plavbou. Výraz *risico* pochází z italštiny a označoval úskalí, kterému se museli plavci vyhnout. [1] Stejně tak se i dnes objevují v organizacích nebo na projektech různá úskalí, která je nutné řídit. Existuje mnoho metodických přístupů, které se zabývají řízením rizik, ale každý si tuto problematiku vykládá po svém a jednotný standard neexistuje. Už jen definice samotného pojmu *riziko* je nejednotná až rozdílná, detailněji rozebírám v kapitole 2.

Co je ovšem problematičtější, žádný ze současných stěžejních metodických přístupů k řízení rizik se podrobně nevěnuje problematice vzájemných závislostí rizik. Podcenění interakcí a možného propojení rizik je hlavním nedostatkem současného řízení rizik, které má za následek těžce zvládnutelné krizové situace. Přitom izolovaným pohledem na jednotlivá rizika se každé riziko samostatně považuje za zvládnutelné, čímž dochází ke zkreslení významu vzájemně závislých rizik.

V této práci se proto věnuji přehlížené problematice vzájemných závislostí rizik a navrhuji ucelený způsob, jak závislosti mezi riziky identifikovat a takto závislá rizika posoudit. K tomuto účelu navrhuji strukturovaný popis rizika, tzv. rizikový scénář a dále navrhuji informační systém, který implementuje pravidla pro odhalení vzájemných závislostí rizik a přehlednou formou je prezentuje rizikovým manažerům.

Kapitola 1

Cíle práce

Hlavním cílem této práce je navrhnout systém pro identifikaci vzájemných závislostí rizik. Pro dosažení hlavního cíle práce jsem si stanovil následující postupové cíle.

1.1 Postupové cíle

1. Prostudování odborné literatury ke stěžejním metodickým přístupům řízení rizik.
2. Analýza duality rizika, tj. negativních a pozitivních vlivů rizikových událostí (ztráta, zisk).
3. Analýza agregace rizik a vzniku vzájemných závislostí rizik (domino efektu).
4. Charakteristika systémů pro řízení rizik dostupných na trhu se zaměřením na závislá rizika.
5. Návrh způsobu posuzování rizik v kontextu rizikových scénářů.
6. Návrh způsobu identifikace vzájemných závislostí rizik vyvolávajících domino efekt.
7. Návrh vhodného přístupu k posuzování možnosti vzniku domino efektu analýzou vzájemné závislosti rizik.
8. Návrh demonstračního programu umožňujícího identifikovat domino efekt a jeho příčinná závislá rizika a vytvoření prototypu.
9. Demonstrace navrženého přístupu užitím programu na testovacím vzorku dat.
10. Zhodnocení a doporučení dalšího rozvoje.

Kapitola 2

Metodické přístupy k řízení rizik

Ohledně řízení rizik bylo vymyšleno a napsáno mnoho metodických přístupů, ale v mnohém se rozcházejí. Cílem této kapitoly je popsat základní myšlenky stěžejních metodických přístupů, poukázat na jejich silné a slabé stránky a mezi sebou je porovnat. Abych obsáhl co nejvíce odlišné a zároveň v praxi užívané přístupy, vybral jsem následující:

- Přístup IPMA [2]
- Přístup PMI [3]
- Standardy ISO [4] [5] [6] [7] [8]
- Metodický rámec ISACA COBIT5 [9]
- Přístup SEI MOSAIC [10] [11] [12]

Tato kapitola začíná vysvětlením pojmů, které se pojí s řízením rizik. Tyto obecné pojmy budou v dalších podkapitolách předefinovány dle různých metodických přístupů, jejichž popis následuje. A na závěr jsou popsány procesy řízení rizik podle jednotlivých přístupů.

2.1 Základní nastínění pojmů k řízení rizik

Vysvětlení následujících pojmů je převážně laické a cílem je nastínění do problematiky této práce – řízení rizik.

Riziko (risk) – obecně nějaká událost, která může uškodit. Nastává s určitou pravděpodobností a ohrožuje zejména aktiva a cíle. Riziko nemusí být pouze negativní, viz příležitost. Konkrétní definice pojmu riziko podle jednotlivých metodických přístupů jsou v podkapitole 2.2.

Likelihood	Consequence: Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Obrázek 2.1: Příklad rizikové matice [14]

Příležitost (opportunity) – pozitivní analogie rizika, nejistá událost, která může přilepšit. Hranice mezi rizikem a příležitostí může být velice tenká, viz kapitola 3 o dualitě rizik.

Rizikový apetit (risk apetite) – nebo také „chuť riskovat“ vyjadřuje, na kolik je organizace ochotný riskovat za účelem uskutečnění svých cílů. Vždy jej vědomě určuje vedení organizace. [13]

Riziková kapacita (risk capacity) – vyjadřuje maximální riziko, kterému je organizace schopný čelit, nebo také jakých ztrát se může dopustit, aniž by to ohrozilo jeho existenci. Riziková kapacita nesmí být zpravidla menší, než rizikový apetit.

Riziková matice (risk matrix) – dvourozměrná matice, která slouží jako nástroj pro zobrazení rizik a stanovení priorit rizik. Jedna osa vyjadřuje pravděpodobnost vzniku rizika a druhá osa velikost jeho dopadu.

Inherentní a reziduální riziko (inherent and residual risk) – inherentní riziko (vlastní riziko) nebere v úvahu již zavedená opatření snižující možnost působení hrozby, zranitelnost nebo dopad rizika a naproti tomu riziko reziduální je riziko, které zbude po implementaci opatření. [15]

Mitigace rizika (risk mitigation) – aplikování vhodných opatření, kterými se riziko snižuje na akceptovatelnou úrove, tj. pod úroveň rizikového apetitu. Obecně dochází ke snížení pravděpodobnosti či velikosti dopadu rizika. [16]

Akceptace rizika (risk acceptance) – vědomé přijetí rizika. Žádná akce proti působení rizika není provedena a ztráta z propuknutého rizika, pokud nastane, bude akceptována. Přitom nejde o ignorování rizika, protože riziko je známo a vedením je rozhodnuto jej jako takové přijmout. Místo akceptace je také možné ještě riziko sdílet nebo přenést na někoho jiného. [17]

Aktiva (assets) – vše, co má pro určitou organizaci hodnotu a je proto organizací řízeno pro dosahování cílů. Hodnota aktiv může být snížena působením rizik. [1]

2.2 Metodické pojetí rizik

V této části jsou popsány základní myšlenky jednotlivých metodických přístupů a definovány základní pojmy podle těchto přístupů.

2.2.1 Rizika podle IPMA

Společnost pro projektové řízení (SPR), která je rovněž zástupcem IPMA v České republice, naznačuje přístup a požadavky na kompetence k řízení rizik v publikaci Národní standard kompetencí projektového řízení [2]. Na rozdíl od jiných standardů však IPMA nejde do hloubky potřebné pro praktické řízení rizik. Následují definice klíčových pojmů.

Riziko – nejistá událost nebo podmínka, která pokud nastane, má negativní vliv na dosažení cíle projektu.

Rizikový faktor – možnost vzniku měřitelné situace či měřitelné události, která záporným způsobem ovlivní naplnění trojimperativu projektu.

Hrozba – konkrétní událost, jejíž výskyt nastartuje děj s negativním dopadem na cíl projektu. Nazývá se také riziková událost.

Příležitost – pozitivní ovlivnění projektu a jeho projektových cílů. [2]

I když jsou v definicích IPMA uvedeny pojmy riziko, rizikový faktor, hrozba, příležitost a riziková událost, standard podle IPMA s těmito pojmy blíže nepracuje. Řízení rizik a příležitostí je podle IPMA chápáno jako proces probíhající během celého projektu od jeho iniciace až po ukončení. Riziko je vztaženo k projektovým cílům, což znamená, že pro úspěšní řízení rizik je nezbytné nejdříve dobře pochopit a definovat projektové cíle.

2.2.2 Rizika podle PMI

Practice standard for project risk management [3] je rozšiřující nadstavbou řízení rizik uvedeného v PMBok Guide [18] a jde o postup řízení rizik specializovaný na oblast projektů. Definuje projektové riziko a to následovně.

"Project risk is an uncertain event or condition that, if it occurs, has a positive or a negative effect on a project's objectives."[3]

Definice rizika zde obsahuje dva klíčové aspekty: *nejistotu* (incertainty) a *efekt na cíle projektu* (effect on a project's objectives). Nejistota je popsána pravděpodobností rizika (probability) a efekt na cíle projektu je popsán dopadem rizika (impact). Důležité je si všimnout, že na rozdíl od definice IPMA, riziko může mít jak negativní tak i pozitivní efekt na projektové cíle.

Pro rozlišení negativního a pozitivního efektu, PMI používá pojmy hrozba (threat) a příležitost (opportunity):

"Threat is a condition or situation unfavorable to the project, a risk that will have a negative impact on a project objective if it occurs, or a possibility for negative changes."[3]

"Opportunity is a condition or situation favorable to the project, a risk that will have a positive impact on project objectives, or a possibility for positive changes."[3]

Metodický přístup PMI vztahuje všechna rizika na některý z projektových cílů a proto je nezbytné dobře pochopit, k čemu jsou projektové cíle vztaženy a jak je definovat a řídit. Důvodem pro řízení projektových rizik je pak zvýšení pravděpodobnosti a dopadu pozitivních událostí a snížení pravděpodobnosti a dopadu událostí nepříznivých na projektové cíle. [18]

2.2.3 Rizika podle standardů ISO

ISO norem zmiňujících rizika je více, ale popíši zde chápání rizik normou ISO 27001 [4] a ISO 27005 [5], které jsou z řady ISO 27000 [8], zaměřené na systémy managementu bezpečnosti informací (ISMS). Některé informace jsou také čerpány z normy ISO 31000 [7]. Tyto ISO normy jsou široce rozšířené a jsou v podstatě standardem pro řízení rizik na projektech a mnoho organizací má na tyto normy akreditovanou certifikaci. Přístup k řízení rizik je postavený na aktivech, hrozbách a zranitelnostech. Pojem riziko je definován napříč normami shodně.

"Risk is an effect of uncertainty on objectives."

Čili jedná se o účinek nejistoty na dosažení cílů. Dále je u definice rizika v [5] poznámka, která říká, že riziko bezpečnosti informací je spojeno s potenciálem, kterým hrozba využije zranitelnosti aktiva a tím zapříčiní škodu organizaci.

Zde je důležité si všimnou výskytu nových pojmů – zranitelnost (vulnerability) a aktivum (asset). Ty vnáší do řízení rizik větší míru detailu a nové možnosti při definicí rizik, které tyto definice zpřesňují.

Standard pracuje pouze s pojmem hrozba, příležitosti jsou opomíjeny. Dále ale definuje zranitelnosti, jako slabiny aktiv.

"Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization."

"Vulnerability weakness of an asset or control that can be exploited by one or more threats."[8]

Riziko je podle ISO 27005 [5] vztaženo k dosažení cílů, které mohou mít různá hlediska (finanční, zdravotní, bezpečnostní nebo environmentální) a mohou být uplatňovány na různých úrovních (strategická úroveň, úroveň týkající se celé organizace, projektu, produktu nebo procesu). Cíle jsou podle ISO 27005 vázány na aktiva.

Aktivum (asset) je cokoli, co má pro organizaci nějakou hodnotu. A proto musí být řízeno a chráněno na působení nežádoucích rizik. Aktivum je nezbytné a podstatné pro dosažení cílů organizace. Splnění cílů má poté dopad do podnikání dané organizace. Aktiva můžou být **hmotná** (např. infrastruktura, servery, budovy, stroje atp.) i **nehmotná** (např. obchodní tajemství, znalosti, schopnosti atp.).

Důvodem proč rizika řídit je pak podle normy ISO 27001 [4] nastavování a udržování přiměřené ochrany aktiv organizace. Podle normy ISO 10006 se rizika řídí z důvodu minimalizace vlivu možných negativních událostí a využití všech příležitostí ke zlepšení. [6]

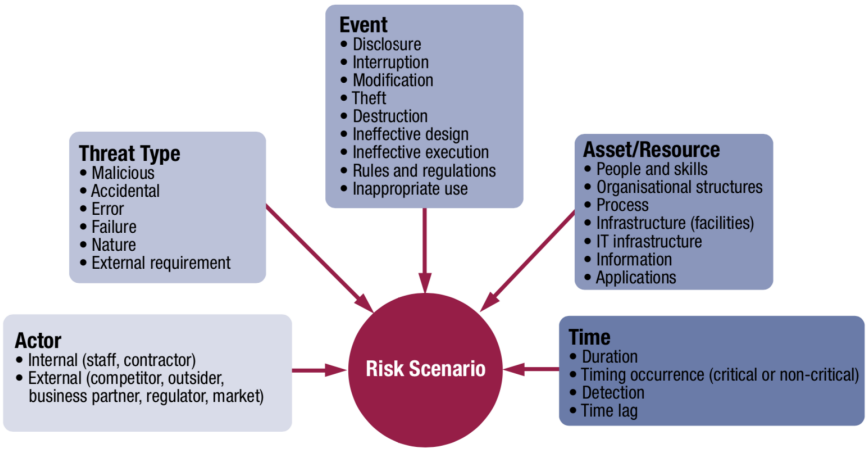
2.2.4 Rizika podle ISACA COBIT 5

Nezisková organizace ISACA popisuje řízení rizik v rámci svého frameworku COBIT, konkrétně publikace COBIT 5 for Risk [9], a také publikace The Risk IT Framework [19]. Definici rizika jako takového neuvádí a místo toho zavádí pojem rizikový scénář.

2.2.4.1 Rizikový scénář

Rizikový scénář je popis možné události, která pokud nastane, tak bude mít neurčitý dopad na dosažení cílů organizace. Dopad může být pozitivní i negativní. Rizikový scénář vzniká spolupůsobením více komponent, které jsou znázorněný na obrázku 2.2.

Aktér generuje hrozbu která využije zranitelnosti. Může být interní (např. zaměstnanci, dodavatelé) nebo externí (např. konkurence, legislativa, trh) a mohou být lidské nebo nelidské povahy.



Obrázek 2.2: Rizikový scénář podle COBIT 5, ISACA [9]

Typ hrozby – povaha hrozby, např. náhoda, zlý úmysl, selhání nebo dílo přírody.

Událost je něco, co se stane na specifickém místě a/nebo čase. Může to být např. zničení či krádež, pád systému nebo přerušení projektu.

Aktivum/zdroj je jakýkoli objekt, který má pro organizaci hodnotu a může být ovlivněn událostí, a vede k business dopadu. Zdrojem se rozumí jakákoli věc, která pomáhá dosáhnout IT cíle. Aktivum a zdroj mohou být identické, např. IT hardware je zdrojem protože jej využívají všechny IT aplikace, a zároveň je aktivem, protože má určitou hodnotu pro organizaci. Aktiva mohou být kritická či nikoli, např. webová stránka internetového bankovnictví v porovnání s intranetem pro vývojářské oddělení. Kritická aktiva/zdroje přitahují více útoků a vyžadují větší důraz na správné fungování.

Čas obsahuje dobu výskytu události, dobu trvání, dobu detekce a zpoždění mezi událostí a dopadem. [9]

2.2.4.2 Typy možných událostí

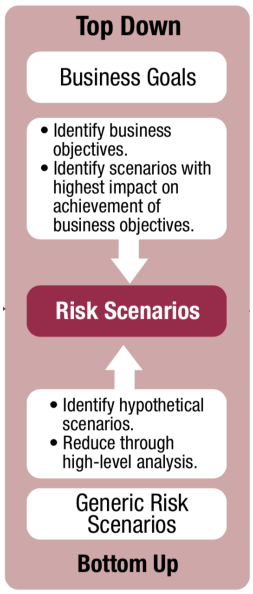
Dále ISACA uvádí tři nadřazené kategorie událostí, které mohou nastat a mezi kterými je třeba rozlišovat:

- **Hrozbové události** (Threat events) – tyto události jsou spouštěčem rizikových scénářů (spojení hrozby a události z obrázku 2.2).
- **Ztrátové události** (Loss events) – nastanou naplněním či zhmotněním rizikového scénáře.

- **Zranitelnostní události** (Vulnerability events) – četnost hrozbové události, která navodí ztrátovou událost, je ovlivněna rizikovými faktory nebo zranitelností. Zranitelnost může být snížena, nebo také zvýšena právě zranitelnostními událostmi.

2.2.4.3 Přístupy k tvorbě rizikových scénářů

Pro tvorbu konkrétních rizikových scénářů doporučuje ISACA dva způsoby:



Obrázek 2.3: Způsob tvorby rizikových scénářů, ISACA [9]

Přístup shora-dolů (top-down) – počáteční identifikace business cílů organizace a následná analýza nejdůležitějších a nejpravděpodobnějších hrozbových událostí s dopadem na identifikované cíle.

Přístup zdola-nahoru (bottom-up) – analýza seznamu generických scénářů, vzniklých ze zkušenosti, které se při identifikaci konkretizují a přizpůsobují na specifické podmínky v dané organizaci.

ISACA dále radí, že je vhodné tyto přístupy kombinovat, neboť se navzájem doplňují. Generické scénáře, zmíněné v definici přístupu zdola-nahoru, jsou v rámci publikace COBIT 5 [9] vypsány a je jich obsaženo celkem 111. Scénáře jsou sdružovány do kategorií, kde každá kategorie obsahuje několik scénářů s negativním výsledkem a několik s výsledkem pozitivním, viz obrázek 2.4.

Pro shrnutí, přístup k identifikaci rizik podle ISACA vychází ze situace, při které se obecně působící hrozba spojí se specifickými podmínkami umožňujícími zranitelnost zdroje/aktiva v rámci rizikové události.

Ref.	Risk Scenario Category	Risk Type: IT Benefit/Value Enablement	Risk Type: IT Programme and Project Delivery	Risk Type: IT Operations and Service Delivery	Example Scenarios: Negative Example Scenarios	Example Scenarios: Positive Example Scenarios
0601	Information (data breach: damage, leakage and access)	S		P	Hardware components are damaged, leading to (partial) destruction of data by internal staff.	Backup procedures, aligned to the business criticality of the data, are established, ensuring key business data is always retained at a second location.
0602		S	S	P	The database is corrupted, leading to inaccessible data.	
0603		S	S	P	Portable media containing sensitive data (CD, USB drives, portable disks, etc.) is lost/ disclosed.	Portable media are appropriately secured and encrypted to ensure protection of data.

Obrázek 2.4: Generické rizikové scénáře, ISACA [9]

2.2.4.4 Rizikové faktory

V definici zranitelnostní události byl zmíněn pojem **rizikový faktor**. Ten ISACA definuje jako podmínku, která ovlivňuje frekvenci a/nebo magnitudu a, v konečném důsledku, business dopad události/scénáře spojeného s IT. [9]

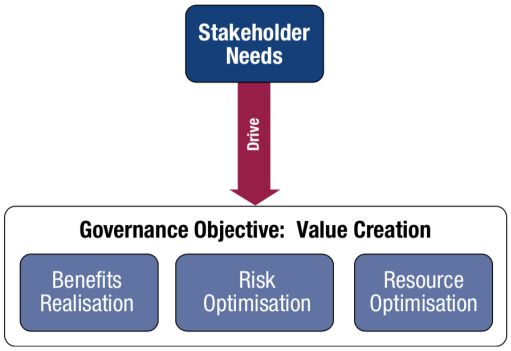
Obrázek 2.5: Vztah mezi inherentním, současným a reziduálním rizikem, ISACA [9]

2.2.4.5 Inherentní, současné a reziduální riziko

Na základě řízení rizik můžeme jedno a to samé riziko v průběhu času definovat jako tzv. inherentní, současné a reziduální, viz obrázek 2.5. Inherentní riziko nebere v úvahu již zavedená opatření snižující pravděpodobnost nebo dopad. Současné riziko pak tyto opatření v potaz bere a odpovídá riziku, které organizace v současnosti čelí. A Reziduálním rizikem se rozumí současné riziko s dalšími aplikovanými opatřeními, které jsou identifikovány na základě prováděné analýzy rizik. ISACA uvádí, že kdykoli užívá pojem riziko, myslí tím riziko současné.

2.2.4.6 Důvod pro řízení rizik dle ISACA

A jaký je důvod pro řízení rizik dle ISACA? Rámec COBIT5 je postaven na pěti principech, kde prvním z nich je *Vytváření hodnot pro zainteresované strany* (stakeholders). Podle ISACA, organizace existují k vytváření hodnot pro jejich zainteresované strany (stakeholders), tudíž každá organizace musí mít vytváření hodnoty jako vrcholový cíl. A vytváření hodnoty znamená: "realizování přínosů za optimálních nákladů na zdroje"2.6 a zároveň optimalizování rizik, viz obrázek.



Obrázek 2.6: Začlenění řízení rizik, ISACA [9]

2.3 Procesy řízení rizik

V předešlé části bylo popsáno chápání rizik jednotlivými metodickými přístupy a v této části jsou popsány procesy řízení rizik. Každý přístup si proces řízení rizik definuje po svém, a i když vychází ze stejného základu, v mnohém se rozcházejí.

2.3.1 Proces řízení rizik podle IPMA

Řízení rizik podle IPMA [2] je pojato jako jeden element technických kompetencí projektového manažera. Tento element se jmenuje *Rizika a příležitosti* a obsahuje možné procesní kroky řízení rizik a příležitostí. Tyto kroky jsou:

1. Identifikujte a kvantifikujte rizika a příležitosti.
2. Vytvořte plán odezvy, nechte jej odsouhlasit a komunikujte jej.
3. Aktualizujte všechny projektové plány, na které má schválený plán odezvy vliv.
4. Vyhodnoťte pravděpodobnosti dosažení časových a nákladových cílů a v průběhu projektu tento odhad provádějte opakovaně.

5. Neustále identifikujte nová rizika a znovu rizika vyhodnocujte. Plánujte jejich eliminaci a modifikujte tím plán projektu.
6. Řiďte a kontrolujte plán odezvy.
7. Dokumentujte získané poznatky a tyto poznatky užijte v budoucích projektech. [2]

IPMA dále do větších detailů nezachází.

2.3.2 Proces řízení rizik podle PMI

Podle PMI [3] je proces řízení rizik rozdělen do šesti navazujících a různě propojených činností, viz obrázek 2.7. Šipky znázorňují tok informací mezi procesními činnostmi, které jsou:

1. plánování řízení rizik;
2. identifikace rizik;
3. kvalitativní analýza rizik;
4. kvantitativní analýza rizik;
5. plánování reakce na rizika;
6. monitorování a kontrola rizik.

Tento proces je detailně popsán (na rozdíl od procesu IPMA) a dává volnost v použití vhodných technik při kvalitativní a zejména kvantitativní analýze rizik. Jednotlivé kroky jsou rozebrány v následujících podkapitolách.

2.3.2.1 Plánování řízení rizik

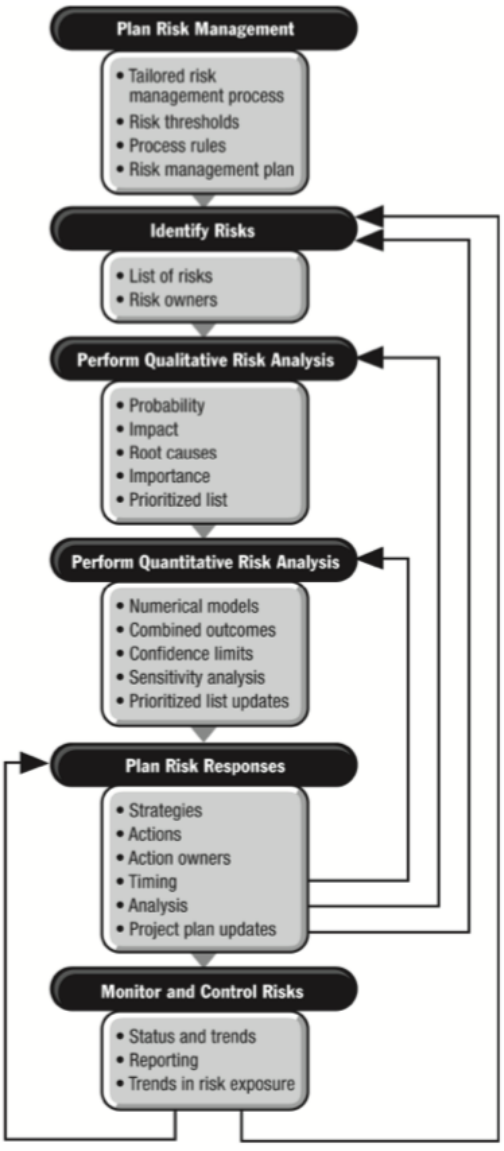
Plánování a řízení rizik stanovuje účel a cíle procesu řízení rizik, kritické faktory úspěchu a bariéry úspěšného řízení rizik. Dále jsou definováni hlavní aktéři řízení rizik, soulad řízení rizik s cíli a strategií organizace, zvyklosti organizace, použití nástrojů a technik a dokumentace, která bude při řízení rizik vytvářena.

2.3.2.2 Identifikace rizik

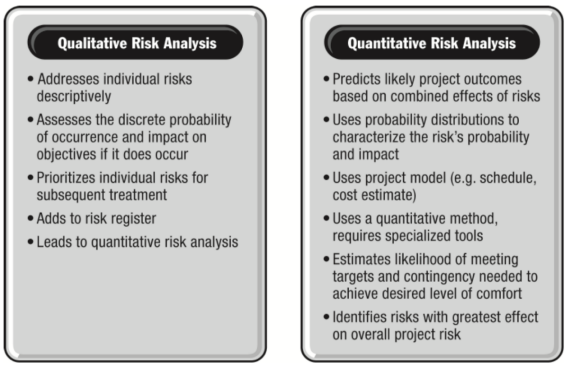
Rizika jsou identifikována ve vazbě na cíle projektu, viz kapitola 2.2.2.

2.3.2.3 Kvalitativní analýza rizik

Kvalitativní analýza rizik slouží k prioritizaci rizik podle jejich pravděpodobnosti a velikosti jejich dopadu na specifické cíle projektu a tím i na celý projekt. Pro rizika jsou stanoveny příčiny vedoucí k riziku nebo množině rizik.



Obrázek 2.7: Proces řízení rizik PMI [3]



Obrázek 2.8: Srovnání kvalitativní a kvantitativní analýzy [3]

2.3.2.4 Kvantitativní analýza rizik

Kvantitativní analýza poskytuje číselný odhad celkového dopadu rizik na projektové cíle. Vstupem kvantitativní analýzy jsou prioritizovaná rizika z kvalitativní analýzy. PMI uvádí, že tato analýza není povinným krokem, ale jeho provedení vnese realističtější pohled na celkový projekt, ale vyžaduje mnohem detailnější analýzu. Dále je kladen důraz na posuzování současně působících rizik, které bude dále rozebráno v kapitole 4. Výsledky z kvantitativní analýzy slouží ke stanovení pravděpodobnosti úspěšného dosažení cílů projektu a odhadu rezerv (v času a ceně) na projektu. Vysokoúrovňové srovnání kvalitativní a kvantitativní analýzy je popsáno na obrázku 2.8.

2.3.2.5 Plánování reakce na rizika

Reakce na rizika udává vhodnou odezvu jak na individuální rizika, tak i na celková rizika projektu. Reakce závisí na rizikovém apetitu zainteresovaných stran a na nastaveném plánu řízení rizik.

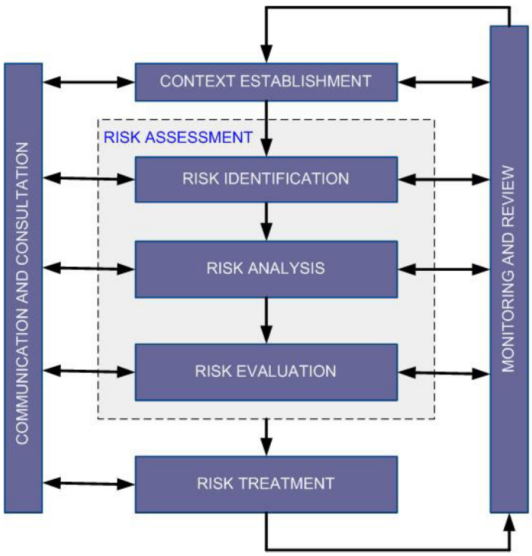
2.3.2.6 Monitorování a kontrola rizik

Monitorování rizik zahrnuje přezkoumávání rizik a audity stavu rizik. Kontrola rizik sestává z uplatňování plánů reakce z předešlé procesní činnosti na působení rizik, provádění další identifikace rizik, jejich analýzy a následné plánování reakce na rizika.

2.3.3 Proces řízení rizik podle ISO

Standardy ISO 27005 [5] a ISO 31010 [7] popisují proces řízení rizik stejně. Jak je znázorněno na obrázku 2.9, proces se skládá ze:

1. stanovení souvislostí;



Obrázek 2.9: Proces řízení risik dle standardů ISO [7]

2. hodnocení rizik;
    a) identifikace rizik;
    b) analýza rizik;
    c) vyhodnocení rizik;
3. ošetření rizik;
4. monitorování a kontrola rizik.

Výše uvedené kroky musí být průběžně komunikovány a konzultovány se všemi zainteresovanými stranami. Nevýhodou těchto standardů je nezahrnutí kvantitativní analýzy jako povinného kroku při analýze rizik a tím i nejasný přístup k agregaci rizik. Následuje popis jednolivých procesních činností.

2.3.3.1 Stanovení souvislostí

Souvislosti řízení rizik určují, jak jsou rizika identifikována, kdo je zodpovědný za vlastnictví rizik, jak rizika ovlivňují bezpečnost informací a jak se vypočítávají pravděpodobnosti a dopady rizik.

2.3.3.2 Hodnocení rizik

Hodnocení rizik je pojato jako samostatný proces sestávající z tří kroků:

1. Identifikace rizik – pro identifikaci rizik je nezbytné identifikovat aktiva, hrozby, zranitelnosti a současná opatření na rizika.

2. Analýza rizik – přiřazení hodnot pravděpodobnosti a dopadu každému identifikovanému riziku.

3. Vyhodnocení rizik – vyhodnocení každého rizika na základě předem stanovených úrovní přijatelnosti a jejich prioritizace.

2.3.3.3 Ošetření rizik

Ošetření rizik je chápáno jako proces výběru a přijímání opatření ke změně rizik, který se skládá z následujících kroků:

1. posouzení zvládání rizik;

2. rozhodnutí, zda jsou zbytkové úrovně rizik v tolerancích (pokud nejsou v tolerancích, vytvoření nového přístupu k jejich zvládání);

3. vyhodnocení účinnosti (efektivnosti) zvládání rizik.

Samotné opatření ke změně rizik jsou následující:

- Vyhnutí se riziku ukončením jakékoli činnosti, která toto riziko vytváří.

- Modifikace (mitigace) rizika implementací kontroly, která sníží pravděpodobnost, že k riziku dojde nebo sníží jeho dopad.

- Sdílení rizika s třetí stranou. Může jít o outsourcing bezpečnosti na jinou společnost, nebo placení pojištění.

- Přijmutí rizika, kdy organizace věří, že náklady na ošetření rizika jsou vyšší, než škody, které by způsobilo.

2.3.3.4 Monitorování a kontrola rizik

Monitorování a kontrola rizik slouží k včasné detekci chyb ve zpracování procesu řízení rizik a pro včasnou identifikaci nezvládání rizik.

2.3.4 Proces řízení rizik podle ISACA

V publikaci COBIT 5 for Risk [9] jde uvedené srovnání procesu řízení rizik s procesy ISO 27005 a ISO 31010 a závěrem je, že COBIT pokrývá oba standardy a navíc je rozšiřuje a v některých oblastech jde do větších detailů.

V publikaci The Risk IT Framework ISACA definuje tři procesní domény, které se týkají řízení rizik a jsou znázorněny na obrázku 2.10:

1. Risk Governance (vrcholové směrování rizik),

Obrázek 2.10: Proces řízení risik dle ISACA [19]

2. Risk Evaluation (hodnocení rizik),
3. Risk Response (odpověď na rizika).

V každé z procesních domén je provedena dekompozice na tři procesy, které se v rámci dané domény zapojují do řízení rizik v organizaci.

2.3.4.1 Risk Governance

Snaha o zajištění, aby praktiky řízení IT rizik byly začleněny do organizace jako takového, což umožní zajistit optimální návratnost přizpůsobenou rizikům. [19] Procesy součástí této domény jsou:

1. vytvoření a udržení společného pohledu na rizika;
2. integrace s Enterprise Risk Management (ERM);
3. dělání obchodních rozhodnutí s vědomím rizik.

2.3.4.2 Risk Evaluation

Snaha o zajištění, aby rizika a příležitosti související s IT byly identifikovány, analyzovány a prezentovány z obchodního hlediska.

Procesy součástí této domény jsou:

1. sběr dat;
2. analýza rizik;
3. udržování rizikového profilu.

2.3.4.3 Risk Response

Snaha o zajištění, aby rizika, příležitosti a události spojené s IT byly řešeny nákladově efektivním způsobem a v souladu s obchodními prioritami.

Procesy součástí této domény jsou:

1. vyjádření (artikulace) rizik;
2. řízení rizik;
3. reakce na události.

Kapitola 3

Analýza duality rizika

V předešlé kapitole byly definovány hlavní myšlenky jednotlivých metodických přístupů k řízení rizik. V této kapitole je analyzováno téma duality rizik – tedy nahlížení na riziko jako na možnou ztrátu, ale také jako na příležitost zisku. Tento koncept je stěžejní pro pochopení výsledků rizikových událostí. Jak je viditelné z již zmíněných generických rizikových scénářů v kapitole 2.2.4.3, rizika mohou pro organizace představovat i příležitost k zisku.

V kapitole je nejprve popsán přístup organizace ISACA a následně více propracovaný pohled výzkumného a vývojového centra Software Engineering Institute.

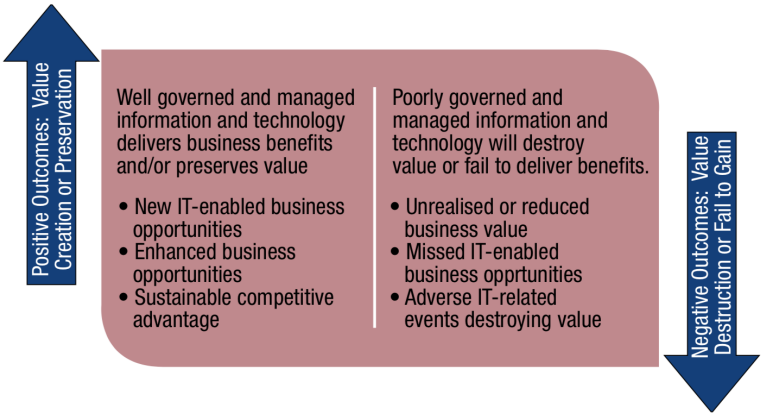
3.1 Dualita rizika podle ISACA

V publikaci COBIT 5 [9] je uvedeno, že by se organizace neměly snažit rizikům pouze vyhýbat. K dosažení vytyčených cílů je mnohdy naopak zapotřebí rizika podstupovat, ale jen taková, která jsou konzistentní s rizikovým apetitem. Přijmutí IT rizik bývá nezbytné pro realizaci podnikových záměrů a cílů, a taková rizika by měla být řízena a ne aby se jim organizace snažily nezbytně vyhnout.

Dále ISACA uvádí, že je důležité mít při všech rozhodnutích souvisejících s riziky tuto dualitu na paměti. Rozhodnutí by měla zvažovat: [9]

- Dopad, který vznikne, pokud není riziko zmírněno, versus výhoda, která může vzniknout, pokud je dopad snížen na přijatelnou úroveň.
- Potenciální přínos, který může nastat, pokud jsou příležitosti využity, versus ztracené výhody při nevyužití příležitostí.

ISACA tedy popisuje dualitu rizika tak, že jako negativní dopad je potřeba uvažovat i nevyužití příležitostí. Když bude organizace příležitosti ignorovat, k žádnému viditelnému negativnímu dopadu nedojde, ale přijde se o možný zisk. Tyto myšlenky znázorňuje ISACA na obrázku 3.1.



Obrázek 3.1: Dualita rizika, ISACA [9]

Dále ISACA v publikaci Risk IT [19] klade důraz na informační technologie jako na zprostředkovatele přidané hodnoty. Nové obchodní iniciativy téměř vždy závisí na zapojení IT. Naproti tomu je ale IT častým zdrojem nedodání přidané hodnoty, kvůli novým, neočekávaným událostem.

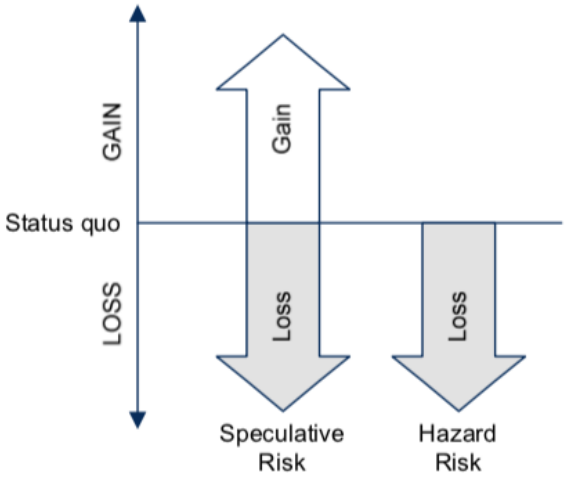
3.2 Dualita rizika podle Software Engineering Institute

Výzkumné a vývojové centrum Software Engineering Institute se dotýká problematiky duality rizik v příloze publikace Mission Diagnostic Protocol [10] z roku 2008. Popisují zde obecný koncept řízení rizik a uvádí dvě perspektivy rizik.

Jde o rozdělení rizik na dvě velké skupiny – spekulativní a hazardní. Důležitým pojmem společným pro obě perspektivy je tzv. stávající stav (status quo), který označuje stav před vypuknutím rizika. Následuje popis obou perspektiv a srovnání je vidět na obrázku 3.2.

Spekulativní perspektiva Riziko podle této perspektivy neposkytuje pouze potenciál ztráty vůči stávajícímu stavu, ale i potenciál zisku, kterým se zlepší stav vzhledem ke stávající situaci. Jako příklad je uvedena hra pokeru – při vsázení je třeba vybalancovat potenciál zisku vůči potenciálu ztráty a cílem je zvětšit vsazené peníze vůči stávajícímu stavu.

Jako další příklad poslouží obecné podnikatelské riziko. Investice do aktiv organizace musí být balancovány potenciálním ziskem z provedené investice. [10]



Obrázek 3.2: Dualita rizika, SEI [10]

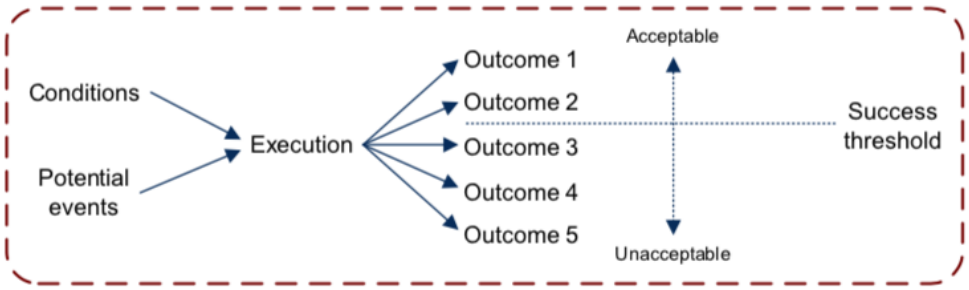
Hazardní perspektiva Podle této perspektivy riziko poskytuje pouze potenciál ztráty, tj. zhoršení oproti stávající situaci. Není zde možnost ji zlepšit.

Příkladem je bezpečnost – představte si, že máte obavy o ochranu cenností uložených ve své domácnosti. Vaším hlavním cílem v tomto příkladu je zajistit, aby žádný z cenností ve vašem bydlišti nebyl odstraněn bez vašeho vědomí a svolení. Po vyhodnocení toho, jak jsou vaše cennosti chráněny, se můžete rozhodnout nainstalovat bezpečnostní systém, aby bylo pro zloděje obtížnější proniknout a ukrást vaše cennosti. Všimněte si, že cíl v tomto příkladu omezuje zaměření rizika jen na potenciál ztráty. Za nejvýhodnějších okolností si ponecháte pouze to, co již máte. Neexistuje žádný potenciál pro zisk. [10]

3.2.1 Kontext rizika

Nyní uvažme stejný příklad, ale z jiného úhlu pohledu (perspektivy). V tomto případě byste chtěli získat klid mysli tím, že zabráníte zlodějům získat vstup do svého domu. Váš cíl být bezpečnější definuje kontext, ve kterém vidíte riziko. Po analýze situace se můžete rozhodnout nainstalovat bezpečnostní systém, aby pro někoho bylo obtížnější proniknout dovnitř. V tomto případě jste ochotni investovat peníze do bezpečnostního systému, abyste se mohli cítit bezpečněji. Bezpečnostní riziko v tomto příkladu je tedy spekulativní, protože vyvažuje vaši toleranci vůči riziku (tj. množství peněz, které jste ochotni investovat do bezpečnostního systému) s vaší touhou realizovat příležitost (tj. získat klid mysli). [10]

Dva předchozí příklady bezpečnosti ilustrují, jak lze stejnou situaci považovat za hazardní riziko v jednom kontextu a za spekulativní riziko v jiném.



Obrázek 3.3: Rozsah potenciálních výsledků, SEI [11]

Riziko je proto klasifikováno jako spekulativní nebo hazardní na základě kontextu, ve kterém je vnímáno. Explicitní určení kontextu, ve kterém se analyzují a řídí rizika, je tedy nezbytné.

3.2.2 Rozsah potenciálních výsledků

Jak je již patrné z obrázku 3.2 a detailněji zobrazeno na obrázku 3.3, rizika mohou mít různý rozsah potenciálních výsledků (range of potential outcome). Jednotlivé výsledky mohou být různě závažné a to pozitivně i negativně.

Jako příklad poslouží riziko zpoždění vývoje softwaru. Jestliže je projekt vývoje řízen agilní metodikou, není přesně definováno, kolik cyklů bude pro úspěšné dokončení projektu zapotřebí. Projektovým managementem ale bude pravděpodobně stanoveno, že projekt by měl být ukončen například ve čtyřech cyklech. Tento počet budeme brát jako chtěný stav. Jestliže je tento počet překročen, naplněné riziko má negativní dopad. Jestliže se podaří projekt dokončit již po třetím cyklu, dopad je naopak pozitivní. Důležité je si ještě povšimnout, že dopad nemá jen jednu negativní/pozitivní úroveň – je zde celý rozsah potenciálních výsledků, čili čím více je počet cyklů překročen, tím větší je dopad.

3.3 Zhodnocení duality rizik

Dualita rizika představuje další oblast, která není vnímána jednotně. ISACA prosazuje názor, že nevyužitá příležitost představuje jistou formou rizika. Naproti tomu Software Engineering Institute je toho názoru, že je třeba u každého rizika stanovit tzv. stávající stav a rozsah potenciálních výsledků, které mohou být pozitivního i negativního charakteru.

Kapitola 4

Analýza agregace a vzájemných závislostí rizik

Doposud bylo popsáno, jakým způsobem řeší stěžejní metodické přístupy řízení rizik a dále byla rozebrána problematika duality rizik. Tato kapitola má za cíl analyzovat další problematiku týkající se řízení rizik – agregaci rizik a vzájemné závislosti.

Posuzování rizik izolovaně se sice jeví jako praktické, ale dochází tak ke zjednodušení skutečností, které neodpovídají realitě. Vhodnější je přistupovat k rizikům jako k celku, který odpovídá širšímu záběru příslušného projektu, programu, divize, celé organizace, nebo i více propojených organizací. V této kapitole je analyzováno, jakým způsobem nahlíží současné metodické přístupy k řízení rizik jako k celku. Nejdál je v tomto směru organizace ISACA, která popisuje tzv. agregaci rizik. Dále je zajímavý pohled centra SEI, které již bylo uvedeno v kapitole 3.2 o dualitě rizik, a které mluví o kumulované návaznosti rizik, což odpovídá tzv. domino efektu.

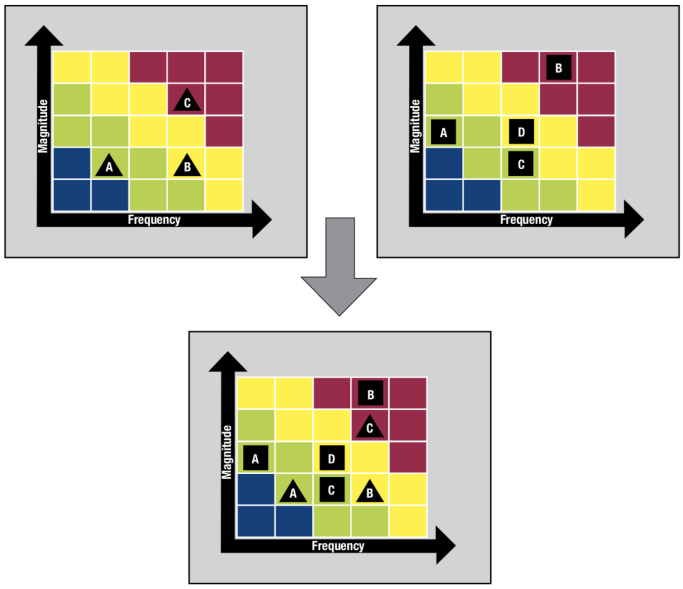
Obrázek 4.1: Ilustrace domino efektu [20]

První zmínka o teorii domino efektu byla v americké zahraniční politice po druhé světové válce a říká, že převrat nekomunistického státu na komunistický, urychlí pád okolních nekomunistických států. [21] Domino efekt tedy označuje situace, kdy se něco, obvykle špatného, stane, což způsobí další podobné události. [22] Podle jiné definice se jedná o řadu podobných nebo souvisejících událostí, které se vyskytují jako přímý a nevyhnutelný výsledek jedné počáteční události. [23] Dá se tedy zobecnit, že se jedná o řetězovou reakci vzájemně se ovlivňujících příčin a následků. Laické znázornění domino efektu je na obrázku 4.1. Následuje popis, jak stěžejní přístupy nahlíží na agregaci a vzájemné závislosti rizik.

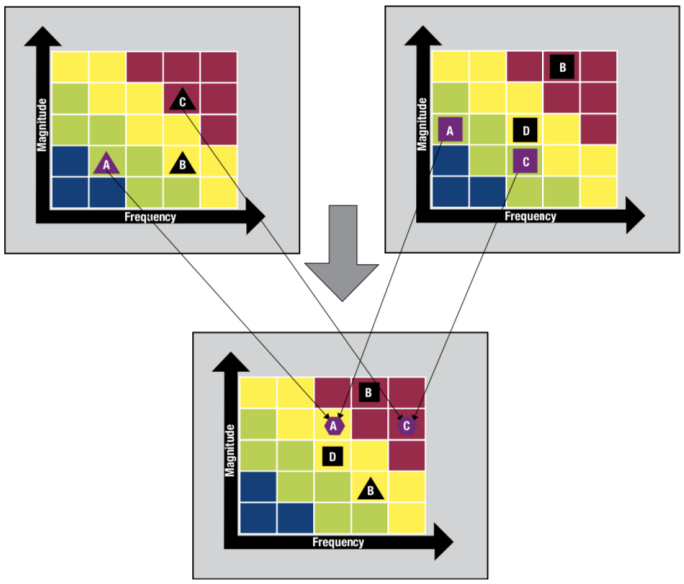
4.1 Agregace rizik podle ISACA COBIT

ISACA [9] [19] razí pojem tzv. agregace rizik a myslí tím společné posouzení rizik, které byly identifikovány odděleně. Např. může jít o posouzení rizik získaných z jednotlivých oddělení organizace, na celofiremní úrovni, nebo posouzení rizik z dílčích projektů. Jestliže se rizika neagregují, jejich posouzení je pouze částečné a to ve významu, že je posouzena pouze část rizik a/nebo jsou posouzena rizika pouze části celkové organizace. Navíc agregovaný pohled na rizika umožňuje řádné přezkoumání rizikového apetitu.

Agregace rizik Agregace je proces integrace posouzení rizik na celofiremní úrovni k získání úplného pohledu na celkové riziko pro organizaci. [9]



Obrázek 4.2: Agregace nezávislých rizik podle ISACA [9]



Obrázek 4.3: Agregace závislých rizik podle ISACA [9]

ISACA uvádí seznam devíti možných nežádoucích vlivů, které znesnadňují agregaci rizik z nichž nejzásadnější jsou:

- Nepřítomnost jasné a jednotné terminologie napříč organizací.
- Neznámé závislosti mezi stejnými riziky, která byla identifikovaná na každém oddělení samostatně.
- Přítomnost kvalitativních údajů a absence kvantitativních údajů.
- Různé zainteresované strany používají různé metodiky/rámce k řízení rizik.

Přístup k agregaci rizik je rozdělen na dva přístupy, a to na agregaci nezávislých rizik a agregaci závislých rizik, která je komplikovanější a ne zcela podrobně popsána.

4.1.1 Nezávislá rizika

Nezávislá rizika mezi sebou nemají žádná propojení a navzájem se neovlivňují. Je nutné, aby rizika nebyla nijak sdílena mezi odděleními, projekty atp. Agregace takových rizik je značně jednodušší než kdyby byla rizika závislá. Agregovaný rizikový profil pak vzniká přenesením rizik do jednoho sumarizovaného profilu pomocí sjednocení jednotlivých rizik, jak je znázorněno na obrázku 4.2. Je zde využito tzv. rizikových map, které jsou obdobou rizikových matic definovaných v kapitole 2.1.

4.1.2 Závislá rizika

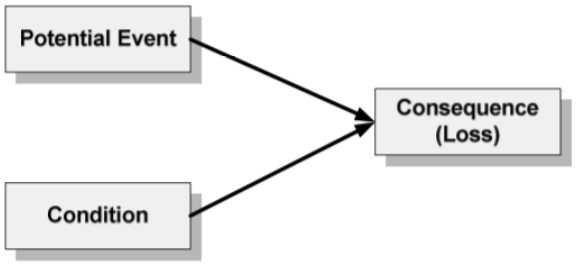
Posuzování závislých rizik již není tak triviální. ISACA zdůrazňuje, že je tento přístup validní jen pokud všechny entity používají stejné metriky a měřítka ve svých rizikových mapách. Dále je zmíněno, že závislá rizika mají obecně závažnější dopad, ale menší pravděpodobnost výskytu (pravděpodobnost selhání dvou nebo více prvků současně je zpravidla menší než pravděpodobnost selhání jednoho z nich).

Na obrázku 4.3 je vidět příklad možné agregace závislých rizik. ISACA neuvádí přesný popis, jakým byla závislá rizika identifikována a agregována a obrázek slouží pouze jako ilustrace možné agregované rizikové mapy.

4.2 Software Engineering Institute a domino efekt

SEI definuje riziko pomocí tří komponent, které jsou vidět na obrázku 4.4:

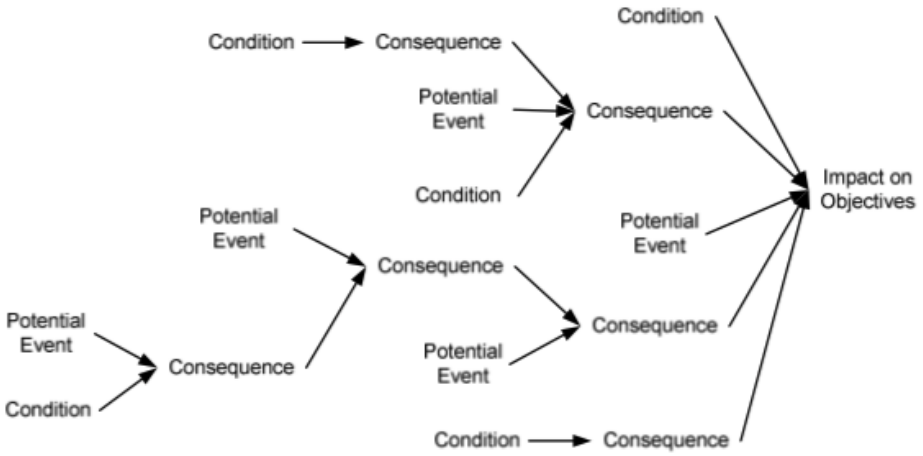
- **potenciální událost** – čin, událost nebo událost, která mění současné podmínky a vede ke ztrátě;
- **podmínka** – současný soubor okolností, které vedou k rizikům nebo je umožňují;
- **následek** - ztráta, ke které dojde, když dojde k potenciální události, ztráta se měří ve vztahu ke stávajícímu stavu [12], viz 3.2.



Obrázek 4.4: Tři komponenty rizika [12]

Podmínka je zde chápána jako zranitelnost, která vystavuje nějakou entitu ztrátě, způsobenou výskytem potenciální události. SEI nepoužívá pojem aktivum a místo toho vztahuje rizika k entitám. Entitami se rozumí objekty, které jsou riziky ovlivněny a jako možné příklady SEI uvádí projekty, programy, obchodní procesy a síťové technologie. Když riziko nastane, dojde k nepříznivému následku (tj. ke ztrátě). Konečným účinkem tohoto následku je změna aktuální sady podmínek, kterým musí entita čelit. Zde se dostáváme ke stěžejní myšlence domino efektu a tedy do bodu, kdy jsou připraveny

nové podmínky, které mohou umožnit vznik jiné události. Takové řetězení SEI nazývá příčinný řetězec podmínek, událostí a následků.



Obrázek 4.5: Příčinný řetězec podmínek, událostí a následků [12]

Na obrázku 4.5 je vidět, že spojením podmínek a potenciální události dojde k následku a tento následek je považován za podmínku, která je výsledkem jiných podmínek a událostí. Zároveň je taky možné, aby pouze podmínka (bez navazující události) dala za vznik nové podmínce. Na konci řetězce je souboru cílů, jejichž splnění řetězec ovlivňuje. Znázorněný řetězec odpovídá definovanému domino efektu, tedy řetězové reakci vzájemně se ovlivňujících příčin a následků.

4.3 PMI a vzájemné závislosti

Jak již bylo zmíněno při popisu procesu řízení rizik, PMI zmiňuje vzájemnou závislost mezi riziky v procesním kroku *kvantitativní analýza rizik*. Snahou je vyhodnotit dosažení splnění projektových cílů a odhadnout časové a peněžní rezervy. Nicméně hned v úvodu kvantitativní analýzy dle PMI je upozorněno, že je tento krok volitelný a není nutno jej provádět a naopak může být u některých projektů i nevhodný [3].

Jediná identifikovaná závislost mezi riziky dle PMI je vztah, kdy má více rizik stejnou příčinu a tudíž je pravděpodobné, že vypuknou ve stejný čas. Bližší informace, jak s takovými riziky naložit, uvedeny nejsou.

4.4 ISO 31010 a vzájemné závislosti

Standard ISO 31010 [7] se dotýká problematiky vzájemných závislostí rizik v definici dopadu rizika, kterým se rozumí výsledek rizikové události ovlivňující cíle. Poznámka u této definice říká, že jakýkoli dopad může eskalovat kaskádovými a kumulativními účinky. Tím ale standard ISO končí a dále se této problematice nevěnuje.

4.5 Zhodnocení současných přístupů

Zmíněné metodické přístupy přistupují ke vzájemným závislostem mezi riziky okrajově a zcela nekonkrétně a hlavní náplní analýzy rizik je zaměření se na rizika jednotlivě, tj. principiálně izolovaně bez vzájemných souvislostí a vazeb, která mezi riziky obecně vždy v praxi existují.

I přesto jsou ale některé důležité myšlenky v metodických přístupech popsány. ISACA razí pojem agregace rizik a odlišně přistupuje k nezávislým a závislým rizikům. Pouze ale jen naznačuje postupy k posuzování vzájemně závislých rizik a do detailů se nepouští. Navíc úplně opomíjí samotnou identifikaci závislostí mezi riziky. SEI předkládá dobře zpracovanou teorii o řetězení příčin a následků, ale praktická ukázka uvedená není. PMI pouze poukazuje na možnost propuknutí více rizik ve stejný čas a ISO zmiňuje, že dopady rizik mohou kaskádovitě eskalovat.

Kapitola 5

Současné systémy na analýzu rizik

Běžnou praktikou mnoha projektů a organizací je řídit rizika bez podpůrného informačního systému. Hojně využívaným nástrojem je MS Excel nebo podobný tabulkový procesor. Existuje ale i mnoho informačních systémů, které se dotýkají řízení rizik. Mnoho obecných podnikových informačních systému (např. pro projektové řízení) obsahuje modul/funkcionalitu pro řízení rizik. Liší se buďto dle odvětví, na které se zaměřují, nebo úrovní detailu, jakou jsou rizika popisována. Některé systémy popisují riziko nestrukturovaně jen jednou větou a některé zacházejí do úrovně aktiv, zranitelností a hrozeb. Dále některé systémy ohodnocují rizika kvalitativně a některé kvantitativně. Většina systémů zobrazuje rizikovou mapu.

Cílem této kapitoly není vypsat všechny dostupné systémy, ale popsat pár vybraných systémů, které dostatečně nastíní současnou situaci na trhu. U systémů jsou nastíněny silné a slabé stránky a vhodnost použití pro konkrétní účely. Dále je snaha o popsání, jestli lze daný systém použít pro účely identifikace vzájemných závislostí rizik.

5.1 MS Exel

Jak již bylo zmíněno, MS Excel je hojně využívaný nástroj pro řízení rizik. Existují různé předdefinované šablony, které jsou uzpůsobené pro řízení rizik. Jak může taková šablona vypadat je znázorněné na obrázku 5.1. Pro spoustu organizací se takové řešení jeví jako ideální především pro svou jednoduchost nasazení.

Jednotlivá rizika jsou triviálně popsána jedním řádkem a každé riziko má přiřazenou hodnotu pravděpodobnosti výskytu a hodnotu dopadu. Jedná se o klasické ohodnocení rizik a na základě těchto dvou hodnot je vypočítána celková závažnost rizika, která je automaticky znázorněna barevně. Chybí zde

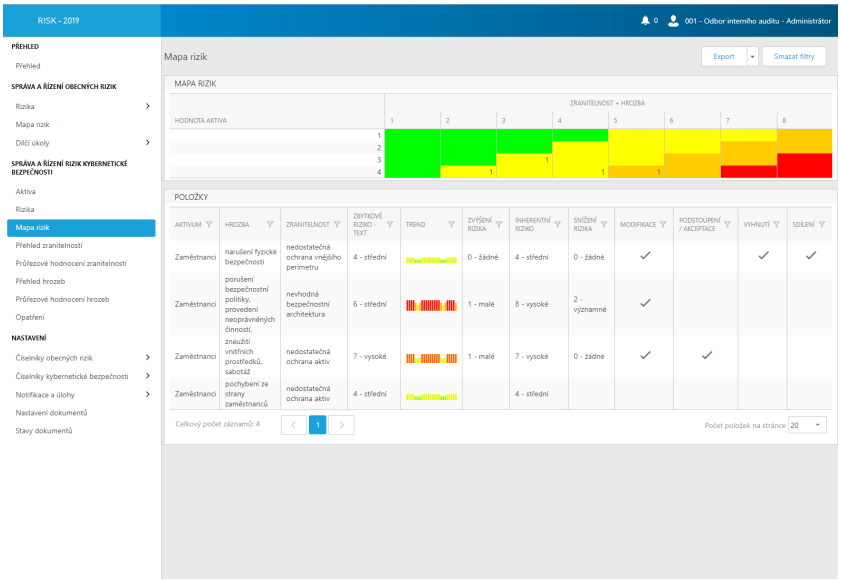
Obrázek 5.1: Řízení rizik pomocí MS Excel [24]

pohled na celkovou rizikovou mapu. Identifikovat vzájemné závislosti mezi riziky je s použitím takové šablony téměř nemožné.

MS Excel jako nástroj pro řízení rizik má velké plus v jednoduchosti nasazení a použití. Také cena takové šablony je mnohdy nižší, než sofistikovanější softwarový nástroj. Nevýhodou je omezená funkcionalita dána do jisté míry zručností vývojáře, který šablonu vytváří.

5.2 Software24

Česká společnost Software24 vyvíjí informační systémy na míru a jejich posledním vyvinutým nástrojem je aplikace na řízení rizik. Tato aplikace již umožňuje strukturovanou definici rizik a rizika jsou rozdělena na dvě kategorie: obecná rizika a rizika kybernetické bezpečnosti. S obecnými riziky je nakládáno obdobně jako v předešlé excelové šabloně, navíc je možné zobrazit



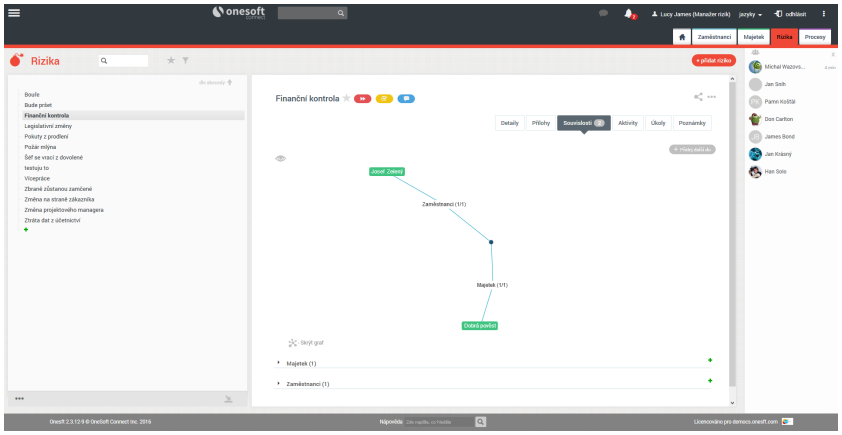
Obrázek 5.2: Řízení rizik pomocí Software24 [25]

rizikovou mapu, kde jsou rizika přehledněji zobrazena. Rizika kybernetické bezpečnosti jsou popsána těmito údaji:

- aktivum,
- hrozba,
- zranitelnost,
- hodnota rizika.

Hodnota každého rizika je pak spočítána na základě hodnoty zranitelnosti, hodnoty hrozby a hodnoty aktiva. Rizika jsou zanesena do rizikové mapy, která ovšem není tradičně rozdělena na osy podle pravděpodobnosti a dopadu (jako to je u obecných rizik, ale jedna osa vyjadřuje již zmíněnou hodnotu aktiva a druhá spojuje hodnotu zranitelnosti a hodnotu hrozby. Riziková mapa i jednotlivá rizika jsou vidět na obrázku 5.2. Dále je možné specifikovat, jakým způsobem se bude s rizikem nakládat (modifikae, akceptace, vyhnutí, sdílení) a definovat opatření, která sníží hodnoty rizik.

Tato aplikace je již sofistikovanějším nástrojem na řízení rizik, ale stále působí jako nedodělaný prototyp a práce s ní je nepřehledná. Grafické uživatelské rozhraní postrádá UX design a z uživatelského hlediska se prakticky jedná o práci s tabulkami. Zajímavé je vyčlenění rizik kybernetické bezpečnosti a odlišná evaluace hodnot těchto rizik. Vzájemné závislosti mezi riziky nejsou nijak řešeny.



Obrázek 5.3: Řízení rizik pomocí systému Onesoft [26]

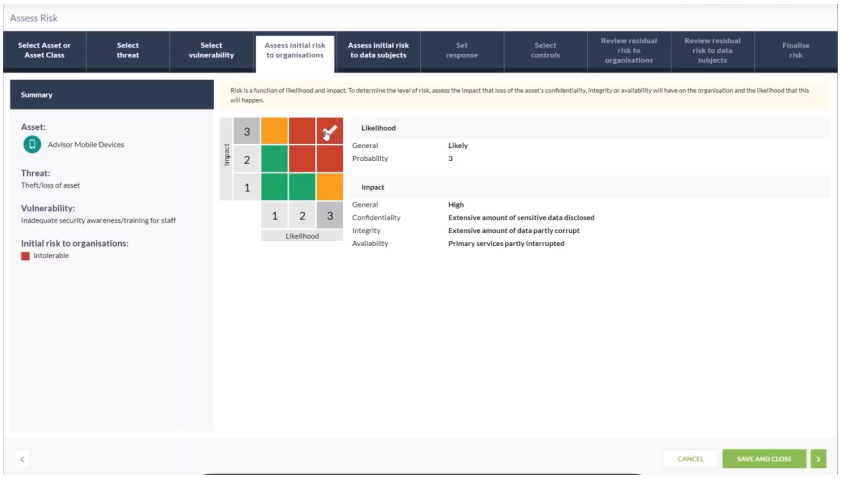
5.3 Onesoft

Další česká společnost Onesoft vytvořila ucelený software pro každodenní řízení firmy, který sdružuje funkcionality jako např. řízení projektů, správa a údržba majetku, záznam obchodních aktivit a zákazníků, provozní evidence firmy atd. Další přídavnou funkcionalitou je řízení rizik, která umožňuje definici jednotlivých rizik a zobrazení rizikové mapy. Rizika jsou definovány jednotně a to pomocí:

- aktiva,
- zranitelnosti,
- odpovědného člověka,
- hodnoty pravděpodobnosti,
- hodnoty dopadu a
- plánu prevence (textový popis).

Tento popis rizik je obdobný popisu obecných rizik u předchozí aplikace, ale je veden mnohem přívětivější a čistší formou z uživatelského hlediska. Každé riziko má svou kartu, kde je formulář pro zadání jednotlivých částí rizika. Každé riziko je kategorizovatelné do předem definovaných oblastí, jako např. provozní rizika, finanční rizika, bezpečnostní rizika atp. Kvantitativní stupnice pro hodnoty pravděpodobnosti a dopadu jsou uživatelsky definovatelné. Dalším výhodou aplikace je možnost generovat řízenou dokumentaci v souladu s požadavky ISO 9001:2015.

Co je důležité nepřehlédnout, je přiřazení odpovědného člověka a aktiva, ke kterému se riziko vztahuje (zobrazeno na obrázku 5.3). Díky těmto vazbám



Obrázek 5.4: Řízení rizik pomocí systému vsRisk [27]

je program schopen zobrazit graf těchto vazeb. Jedná se o jakýsi první pokus rozklíčovat vzájemné závislosti mezi riziky. Vazby jsou ale vedeny jen na související entity ke konkrétnímu riziku, nikoli mezi riziky samotnými. Je tedy nutné konstatovat, že vzájemné závislosti mezi riziky nejsou ani tímto programem řešeny.

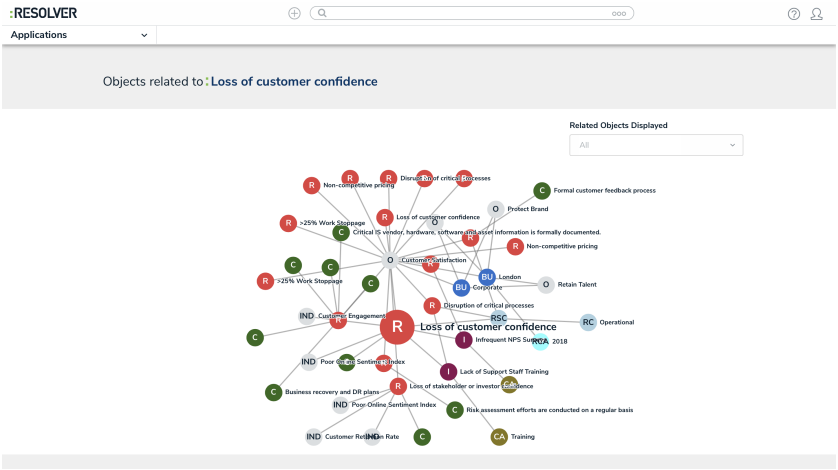
5.4 vsRisk

Systém vsRisk, vyvinutý britskou společností Vigilant Software, je zaměřený na řízení rizik dle normy ISO 27001. Obdobně jako předchozí systémy, umožňuje definice rizik pomocí aktiv, zranitelností a hrozeb, a dále definici opatření a s tím spojené inherentní riziko. Velkým plusem této aplikace je rozsáhlá knihovna hrozeb a zranitelností, které uživateli usnadňují definice rizik. Aplikace má moderní a jednoduché uživatelské rozhraní. K ohodnocení pravděpodobnosti a dopadu používá přehledné posuvníky a interaktivní matici, která je vidět na obrázku 5.4.

Co se vzájemných závislostí týče, systém umožňuje zobrazit rizika, která se dotýkají stejného aktiva. Tím ale funkcionalita končí a další možné vztahy mezi riziky nejsou řešeny.

5.5 Resolver

Kanadská společnost Resolver vyvinula stejnojmenný nástroj pro řízení rizik v roce 2015. Systém je zaměřený speciálně na rizika z oblasti IT a bezpečnosti. Díky přídavnému modulu pro řízení hrozeb a zranitelností pomáhá agregovat informace o aktivech organizace, tj. jejich zranitelnosti a možné hrozby.



Obrázek 5.5: Řízení rizik pomocí systému Resolver [28]

Dalším přídavným modulem je řízení rizik dodavatelů, který má za cíl sledování dodržování dohod o úrovni služeb (SLA).

Systém umožňuje vykreslení grafu vztahů konkrétního rizika, jak je zobrazeno na obrázku 5.5. Toto znázornění je obdobné tomu od společnosti Onesoft, ale nezůstává jen u vztahů jednoho rizika na související entity. Vykresluje i navazující rizika na daném aktivu, a tím zobrazuje závislosti mezi riziky samotnými. Více než zobrazit tento graf ale program neumožňuje, takže se uživatel nedozví, jak závažné je toto propojení a jestli je opravdu dané jen společným aktivem.

Systém klade důraz na definici opatření na rizika a hlídání reziduálního rizika v čase. Dále také obsahuje knihovnu předdefinovaných rizik. Většina uživatelských akcí má přehlednou a přívětivou formu. Funkcionalita týkající se vzájemných závislostí rizik se jen okrajově dotýká rozsáhlé problematiky, viz následující kapitole 6.

5.6 Zhodnocení současných systémů

V této kapitole byly popsány vybrané současné systémy pro řízení rizik. Většina systémů umožňuje definici z řízení rizik zejména podle standardu ISO 270001 a výsledkem je zobrazení mapy všech definovaných rizik. Velkým společným nedostatkem všech výše popsaných systémů je, že žádný nepřistupuje k řízení rizik přes rizikové scénáře a tato skutečnost znemožňuje sofistikovanější identifikaci vzájemných závislostí mezi riziky. Závislosti, které některé systémy odhalit umí, jsou přes sdílené aktivum, ale jedná se jen o část rozsáhlé problematiky vzájemných závislostí rizik.

V popisu jednotlivých systémů nebylo uvedeno, na jaké platformě jsou provozovány. Společným znakem všech výše popsaných systémů je, že se jedná

o webové aplikace, které jsou cloudově dostupné jako SaaS (Software as a service). Tento způsob nasazení je v současné době hojně používaný. Nemuset instalovat nativní aplikace a zaručený běhu napříč platformami ve webovém prohlížeči je velkou výhodou.

Kapitola 6

Identifikace vzájemných závislostí rizik

V kapitole 4 bylo zanalyzováno, jak na vzájemné závislosti nahlíží současné stěžejní metodické přístupy a následně kapitola 5 popsala vybrané systémy řízení rizik. Z těchto dvou kapitol je patrné, že současné stěžejní metodické přístupy a systémy na řízení rizik se problematiky vzájemných závislostí rizik dotýkají jen okrajově. V metodických přístupech je většinou uvedeno, že vztahově provázaná rizika mohou mít závažný dopad a je třeba takové možné vazby mezi riziky brát v potaz, ale způsob, jak tyto závislosti identifikovat a jak s nimi naložit, již uveden není. Některé systémy na řízení rizik umožňují zobrazit okolní vazby jednoho rizika na aktivum a pokročilejší systémy umí zobrazit i navazující rizika přes sdílené aktivum. Jak je ale popsáno v následující kapitole, závislostí mezi riziky může nastat mnohem více, než jen přes sdílené aktivum.

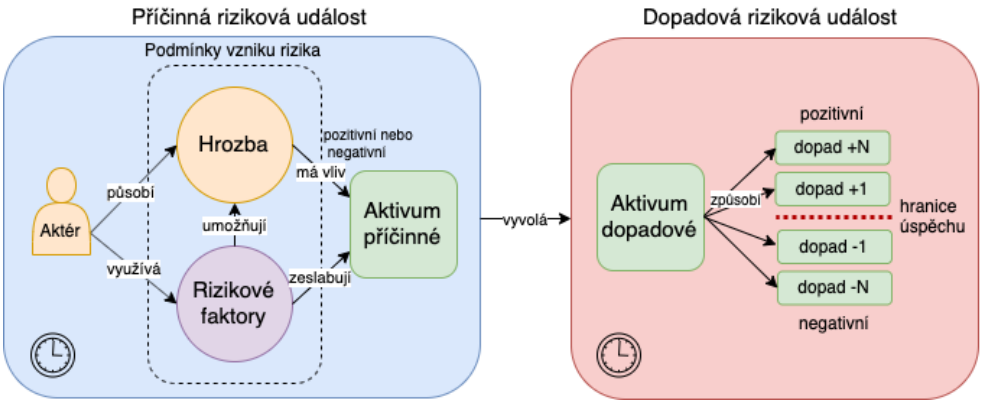
V této kapitole nejprve navrhuji vlastní rizikový scénář, který umožní identifikaci vzájemných závislostí mezi riziky. Následně analyzuji, jaké možné závislosti mohou mezi riziky vznikat s pomocí testovací množiny rizikových scénářů. A na závěr této kapitoly popisuji, jak posoudit rizika, která jsou identifikována jako závislá.

6.1 Návrh rizikového scénáře pro identifikaci vzájemné závislosti rizik

Hlavním nedostatkem většiny existujících systémů na řízení rizik je, že riziko nepopisují strukturovaně. Pouhá jedna věta, která riziko označuje, je velkou abstrakcí od skutečné reality a znemožňuje identifikaci vzájemných závislostí mezi takto vyjádřenými riziky. Proto zde nově definuji rizikový scénář, který vychází z rizikového scénáře ISACA (viz kapitole 2.2.4) a zpřesňuje jej o významné prvky nezbytné pro posuzování vzájemných závislostí rizik.

Základní myšlenkou popisování rizik pomocí scénáře je, že rizikový scénář vytváří jakousi kontextovou šablonu, která popisuje všechna možná rizika na scénáři. Pro účely zkoumání vzájemných závislostí rizik definuji pojem rizika v rizikovém scénáři následovně.

Riziko představuje v rizikovém scénáři konkrétní výskyt potenciálních událostí (příčinné a dopadové), prvků scénáře a podmínek, za kterých mohou tyto události nastat, přičemž tento konkrétní výskyt je vázán na jeden konkrétní dopad z rozsahu potenciálních výsledků (dopadů). Jde tedy o konkrétní instanci v rámci rizikového scénáře, ve kterém je obecně více takových možností.



Obrázek 6.1: Návrh rizikového scénáře pro identifikaci vzájemných závislostí rizik

Rizikový scénář se tedy skládá ze dvou hlavních entit – příčinné události a dopadové události. Tyto hlavní entity obsahují prvky a vlastnosti, viz obrázek 6.1 a následující seznam.

- Příčinná událost:
  - aktér,
  - hrozba (nebo příležitost),
  - příčinná aktiva,
  - rizikové faktory,
  - vlastnosti (čas vzniku a doména).
- Dopadová událost:
  - dopadová aktiva,t

  - dopady,
  - vlastnosti (čas vzniku a doména).

V následujícím textu jsou jednotlivé prvky scénáře vysvětleny a popsány.

6.1.1 Příčinná riziková událost

Příčinná riziková událost se ve scénáři objevuje vždy jen jedna a odpovídá nejběžnější definici rizika, tedy se jedná o možnou událost, nebo podmínku, která pokud nastane, vyvolá dopadovou událost.

Příčinná riziková událost seskupuje prvky, které se podílí na propuknutí rizika a popisují jej. Spouštěčem příčinné rizikové události je buď propuknutí hrozby (událost), nebo uplatnění nějakého rizikového faktoru (podmínka).

Pro shrnutí, v příčinné rizikové události figurují následující prvky:

- aktér,
- hrozba (nebo příležitost),
- aktiva,
- rizikové faktory,
- vlastnosti (čas vzniku a doména).

6.1.1.1 Aktér

Aktérem se rozumí kdokoli (nebo cokoli), kdo může působit nějakou hrozbou. Základní rozdělení je možné na interní a externí aktéry a také je možné aktéry dělit na živé a neživé.

Interní aktéři působí uvnitř organizace a mohou to být například zaměstnanci nebo řídicí výbor. Externími aktéry se rozumí např. konkurence, hackeři, ale i legislativa či trh. Speciálním aktérem může být i čas, jestliže budeme chtít např. namodelovat opotřebení hardwaru, nebo příroda, když budeme chtít modelovat přírodní katastrofu.

6.1.1.2 Hrozba (příležitost)

Hrozba je úzce spjatá s aktérem, který je jejím nositelem, a jedná se o potenciální událost nebo také možný spouštěč (trigger) příčinné rizikové události. Hrozba je umožněna na základě projevených rizikových faktorů, které jsou popsány níže. Hrozby mohou být záměrné, ale také zcela neúmyslné. V tabulce 6.1 jsou uvedeny příklady aktérů a hrozeb.

Tabulka 6.1: Příklady aktérů a jejich hrozeb

Aktér	Hrozba
řídicí výbor	neukončení projektu
konkurence	přeplacení zaměstnance
analytik	nedostatečná analýza
dodavatel internetu	výpadek
hacker	phishingový útok
počasí	je pod nulou a mrzne
...	

Pozitivní analogie hrozby je **příležitost**. Jedná se o událost, která představuje možnost zisku, např. důkladně provedená analýza vedoucí k urychlenému zpracování všech požadavků bez potřeb jejich dalších změn při iterativním vývoji softwaru a ušetření zdrojů na původně předpokládanou další iteraci.

6.1.1.3 Aktiva

Jako **aktivum** může figurovat cokoli, co má pro organizaci hodnotu (hmotné i nehmotné věci, zdroje atd.), a proto musí docházet k řízení aktiva tak, aby došlo k naplnění cíle, k jehož realizaci je aktivum předmětem zájmu v systému řízení (např. v organizaci nebo na projektu). Dále je nutné, aby při působení hrozby na toto aktivum byl identifikován také dopad, který je možno předpokládat a tedy i řídit. Jako konkrétní příklady aktiv mohou být např.:

- funkcionalita vyvíjeného softwaru,
- HW infrastruktura,
- poskytování služby klientům,
- citlivá data,
- zálohovací disk,
- lidé,
- finance, atd.

6.1.1.4 Rizikové faktory

Rizikové faktory jsou možné podmínky, které mohou umožnit působení hrozby, anebo samy vyvolat vznik příčinné rizikové události nabytím platnosti. Spouštěčem příčinné rizikové události tedy může být buďto vzniklá hrozba (potenciální událost), nebo uplatněný rizikový faktor, avšak ne všechny uplatněné rizikové faktory jsou automaticky spouštěčem události.

Rizikové faktory jsou dvojího typu. Může se jednat buďto o *zranitelnosti příčinného aktiva* nebo *slabiny aktivující hrozbu*. V rizikovém scénáři může být zpravidla definováno více rizikových faktorů, přičemž ne všechny se musí uplatnit.

Rizikové faktory mohou být i pozitivního charakteru a ty nazývám v práci jako *šance*, tedy faktor, který umožňuje potenciální zisk. Jako příklad může být uvedeno pojištění. Jestliže je nějaké aktivum pojištěné a dojde k jeho krádeži/zničení, představuje to možný zisk vyplývající z pojistných podmínek. Dalším příkladem je teplota jako faktor, který může vést k negativní události nebo naopak k pozitivní, tedy působí jako šance, která umožní potenciální zisk.

6.1.1.5 Vlastnosti příčinné rizikové události

U příčinné rizikové události je ještě nutné sledovat tyto vlastnosti:

Čas vzniku události, který je významným atributem pro scénáře zasazené do toku času, čili dá se určit zpravidla nějaký časový okamžik (milník), kdy příčinná událost může nastat (např. zahájení integračního testování, konec fiskálního roku).

Doména, která slouží ke kategorizaci příčinné události podle jednotlivých útvarů organizace, projektů, atp.

6.1.2 Dopadová riziková událost

Dopadová riziková událost je událost, která je vyvolána příčinnou rizikovou událostí a jedná se o negativní nebo pozitivní působení na nějaké aktivum.

V jednom scénáři může být definováno více dopadových událostí, přičemž vždy alespoň jedna nastane při konkrétním projevu rizikového scénáře (riziku). Každá dopadová událost se zpravidla týká jiných aktiv. Dále je možné v rámci jedné dopadové události definovat celou množinu dopadů, která odpovídá rozsahu potenciálních výsledků z kapitoly 3.2.2 o dualitě rizika.

Pro shrnutí, v dopadové rizikové události figurují následující prvky:

- dopadová aktiva,
- dopady,
- vlastnosti (čas vzniku a doména).

Dopadová aktiva jsou aktiva, na které dopad negativně (nebo pozitivně) působí. Tato aktiva můžou být shodná s příčinnými aktivy, ale není to pravidlem. Dopad v dopadové události může představovat nově vzniklé podmínky

po propuknutí jiného navazujícího rizika, které zapříčiní. Toto je důležitá myšlenka pro identifikaci domino efektu mezi riziky, který je popsán v kapitole 6.2.5.

Vlastnosti má dopadová událost dvě a to následující:

Čas vzniku dopadové události , který určuje, za jak dlouho po příčinné události se dopad projeví. Vyjadřuje tedy časový odstup od příčinné události. Běžnou hodnotou této vlastnosti bývá "bezprostředně po vzniku", ale může to být i časový údaj (den, týden, 14 dní atp.) nebo milník jako je tomu u času příčinné události.

Doména , která slouží ke kategorizaci příčinné události podle jednotlivých útvarů organizace, projektů, atp.

6.1.3 Kategorizační vlastnosti scénáře

Na rizikovém scénáři je možné sledovat ještě dvě vlastnosti. Jedná se o kategorizační vlastnosti, které pomáhají scénář zařadit do určitých logických celků.

Typ rizika určuje, jestli se jedná o riziko čistě hazardního charakteru (pouze potenciál ztráty), nebo jestli jde o riziko spekulativní – může dojít ke ztrátě, ale také k zisku.

Kategorie určuje, jaké oblasti v rámci domény se scénář týká.

6.1.4 Metrické vlastnosti rizik

Poslední dvě vlastnosti, které je vhodné sledovat zejména pro vizualizaci rizik do rizikové mapy, jsou pravděpodobnost a závažnost rizika. Pravděpodobnost se z důvodu existence rozsahu potenciálních dopadů nevztahuje k celému scénáři, ale je třeba ji vztáhnout k riziku chápanému jako konkrétní projev událostí, podmínek a prvků ve scénáři.

Pravděpodobnost rizika určuje, jak moc je očekáváno, že příčinná riziková událost nastane a povede ke konkrétnímu dopadu jedné dopadové události rizikového scénáře. Pro měření se používá různě definovaná škála.

Závažnost dopadu odhaduje, jak silný může konkrétní dopad být. Pro měření se používá různě definovaná škála nebo převod na finanční vyjádření dopadu.

6.1.5 Opatření vůči hrozbám a zranitelnostem

Vedle rizikového scénáře se při řízení rizik stanovují opatření proti rizikům, která mají za cíl snížit pravděpodobnost výskytu rizika, nebo snížit závažnost dopadu konkrétního rizika. Opatření, která jsou definována v návaznosti na příčinnou událost, působí buď na nějaký rizikový faktor, nebo na hrozbu. Zde mají za cíl snížit pravděpodobnost výskytu dané příčinné události. Opatření definovaná v návaznosti na dopadovou událost mají za cíl snížit závažnost konkrétní dopadové události. Způsob stanovování opatření proti působení rizik není předmětem této práce a je rozpracován ve většině metodických přístupů týkajících se rizik (viz kapitol 2).

6.2 Identifikace vzájemných závislostí rizik

Tato část se věnuje analýze možných závislostí, které mohou mezi riziky vznikat. Cílem je naleznout a popsat všechny možné typové závislosti, které mohou mezi riziky vzájemně nastat. Ze současné teorie popsané v kapitole 2, vyplývá, že rizika mohou být závislá na základě sdíleného aktiva, také může více rizik propuknout ve stejný čas a také na sebe mohou rizika kaskádovitě navazovat, tyto závislosti ale nejsou v žádné z uvedených stěžejních metodik popsány. Pro upřesnění těchto závislostí a nalezení závislostí dalších, jsem analyzoval několik konkrétních příkladů rizik, které jsou uvedeny v příloze C a popsány níže. Dále pak následuje popis a charakterizace jednotlivých typů závislostí.

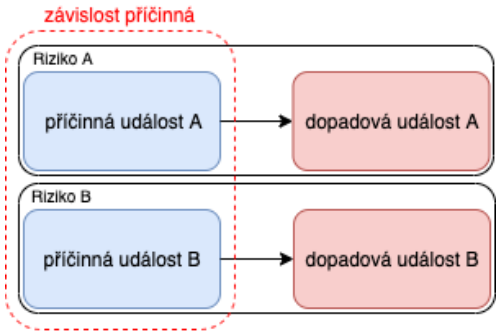
6.2.1 Testovací množina rizik

Pro účely analýzy možných vzájemných závistí mezi riziky jsem vyšel z generických rizikových scénářů definovaných organizací ISACA, viz kapitola 2.2.4.3. Použil jsem však vybrané scénáře, se kterými jsem se setkal v praxi při práci ve společnosti Per Partes Consulting, s.r.o. (www.perpartes.cz), ve které jsem zaměstnán po celou dobu vysokoškolského studia jako analytik v oblasti podpory projektů realizovaných společností. Dále jsem tyto generické scénáře zúžil a upravil v souladu s doporučeným přístupem ISACA na ty scénáře, které obsahují aplikovatelná rizika, se kterými jsem se setkal v praxi při zaměstnání. Generické rizikové scénáře a rizika na nich bylo nezbytné více konkretizovat a doplnit o další prvky a vlastnosti v souladu s navrženým rizikovým scénářem (viz kapitola 6.1). Tím bylo umožněno posuzovat vzájemnou závislost rizik. Množina testovacích rizik je součástí přílohy C.

6.2.2 Závislost příčinná

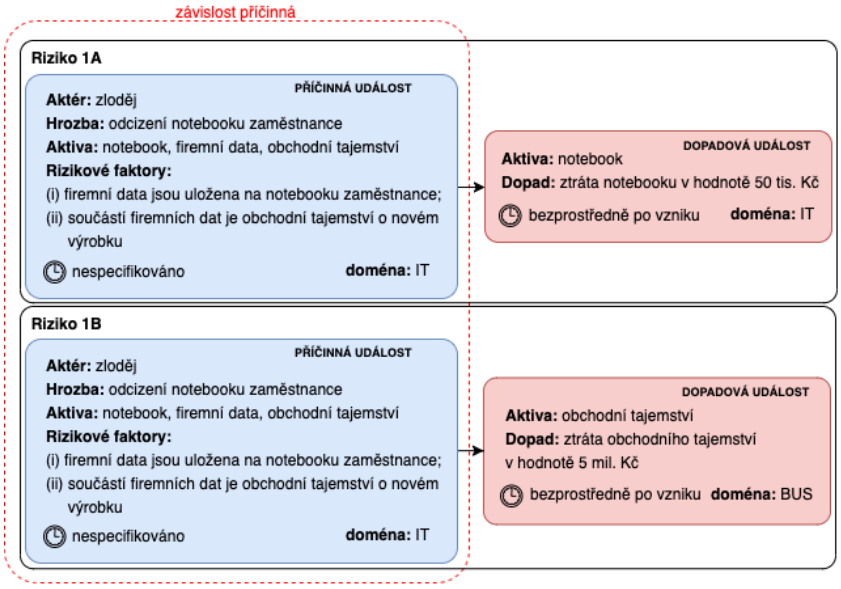
První identifikovaná závislost je na základě shodujících se prvků v příčinných rizikových událostech. Nejčastějším případem je shodující se příčinné aktivum napříč riziky. Závislost ale může být dána také pouze shodným aktérem, hroz-

bou, shodným rizikovým faktorem, časem nebo jakoukoli kombinací předešlého. Může také jít o naprosto totožné události, viz příklad níže, a takto závislá rizika pak spadají do stejného scénáře. Obecně čím více shodujících se prvků se v událostech vyskytuje, tím silnější závislost vzniká. Schématické znázornění takových rizik je na obrázku 6.2.



Obrázek 6.2: Schématické znázornění rizik s příčinnou závislostí

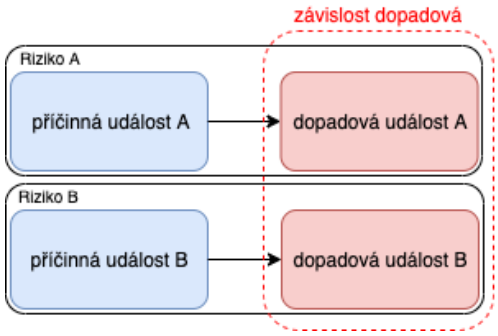
Jako příklad příčinné závislosti na úrovni stejné příčinné události mohou sloužit rizika na obrázku 6.3. Příčinné události jsou stejné, ale v jednom riziku je dopadem ztráta notebooku v hodnotě 50 tis. Kč a v druhém ztráta obchodního tajemství v hodnotě 5 mil. Kč. Je tedy patrné, že tato dvě rizika jsou silně závislá a to právě přes závislost na stejné příčinné události.



Obrázek 6.3: Rizika demonstrující příčinnou závislost

6.2.3 Závislost dopadová

Druhá identifikovaná závislost je na základě shodujících se prvků v dopadových rizikových událostech. Může tedy jít o stejné aktivum nebo dopady v různých rizicích. Opět, jako v příčinné události, čím více se identifikuje shodných prvků, tím silnější dopadová závislost vzniká. Nejsilnější závislost nastane v případě, že dopadové události jsou totožné. Schématické znázornění takových rizik je na obrázku 6.4.



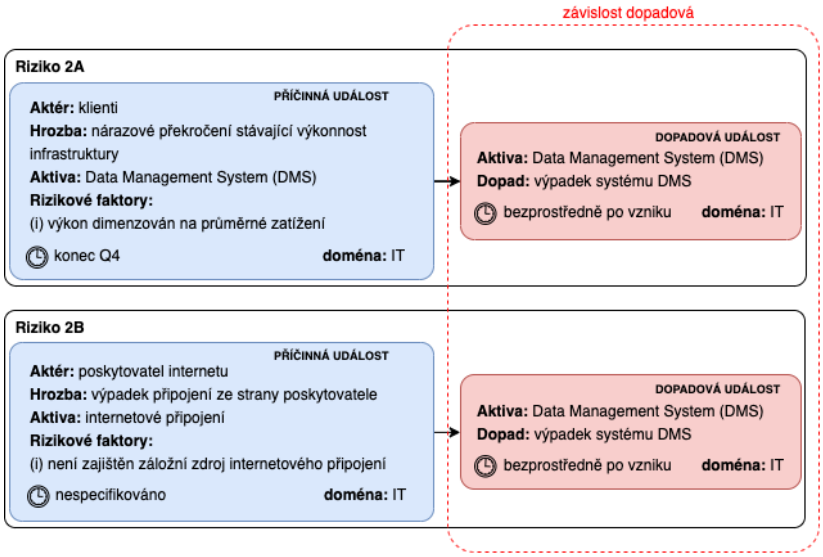
Obrázek 6.4: Schématické znázornění rizik s dopadovou závislostí

Jako příklad mohou sloužit rizika na obrázku 6.5. První riziko zachycuje možné přetížení webového systému na správu dokumentů (DMS) klienty, což má za následek výpadek tohoto systému. Druhý scénář zachycuje možný výpadek u poskytovatele připojení k internetu, který má také za následek výpadek DMS. Taková rizika mají nesouvisející příčinné události, ale mohou ohrozit stejné dopadové aktivum, tudíž jsou závislá.

6.2.4 Závislost časová

Speciálním případem závislosti je závislost časová, která vzniká mezi riziky, pokud mají stejný čas propuknutí dopadových událostí. Jejich dopad nastane ve stejném čase a ačkoliv spolu jinak nemusí souviset, je třeba jim v případě jejich propuknutí čelit společně. Časová závislost tak dává do souvislosti rizika, která se shodují v čase projevení dopadu, ale jinak spolu obecně nesouvisí. Když se sejde více rizik v jeden časový okamžik (např. nějaký milník na projektu) a i když spolu tato rizika jinak nesouvisí, může nastat vlivem jejich závislosti v čase kritická situace.

Na obrázku 6.6 jsou dvě rizika, která spolu souvisí přes čas dopadu, tj. milník GO LIVE na projektu vývoje ekonomického informačního systému (EIS). První riziko vyjadřuje možnost chybné provedené analýzy požadavků uživatelů při analytických pracích na začátku projektu (v rámci zpracování detailního návrhu systému) s dopadem takovým, že v systému chybí kritická funkcionalita. Druhé riziko vyjadřuje možnou chybu v nastavení parametrů



Obrázek 6.5: Rizika demonstrující dopadovou závislost

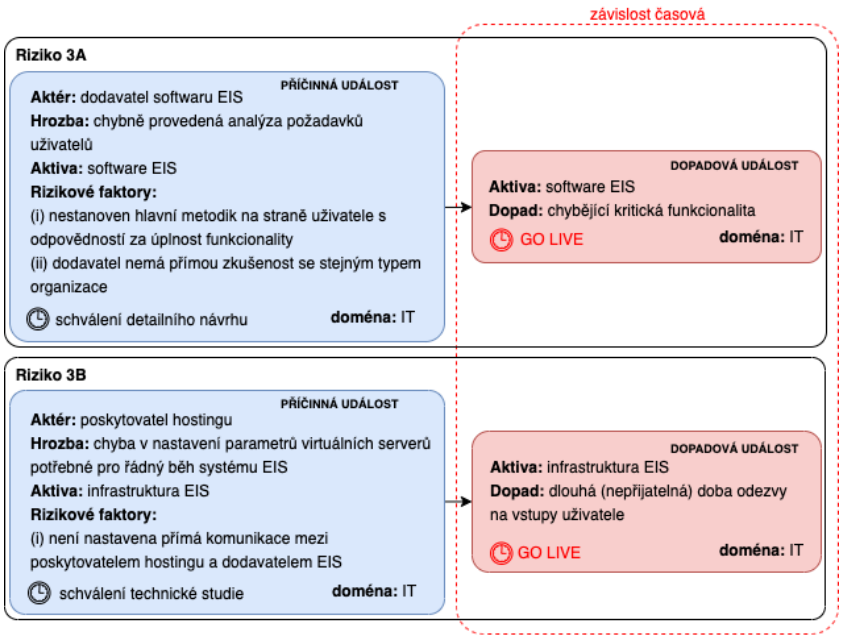
virtuálních serverů (v době zpracování technické studie) potřebných pro řádný běh EIS s dopadem na infrastrukturu, konkrétně v podobě nepřijatelně dlouhé doby odezvy na vstupy uživatele. Dopady obou těchto rizik se mohou projevit v momentě nasazení systému do ostrého provozu a tudíž spolu souvisí pouze přes čas dopadu.

6.2.5 Závislost kauzální (domino efekt)

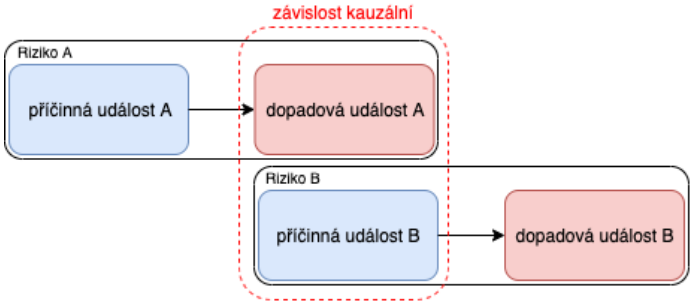
Poslední identifikovanou závislostí je závislost tzv. kauzální. Tato závislost odpovídá domino efektu, definovanému v kapitole 4.2, a je ze všech závislostí nejnáročnější na odhalení. Dává do vztahu rizika, kdy následek (dopad) jednoho rizika může být příčinnou rizika jiného.

Domino efekt vzniká, když dopad dopadové události v jednom riziku se stane hrozbou nebo rizikovým faktorem v příčinné události jiného rizika. Vysvětlení vychází z definice prvků příčinné a dopadové rizikové události v podkapitole 6.1. Dále se dopadová a příčinná událost může shodovat v aktivech, což posílí tuto závislost. Obrázek 6.7 schématicky znázorňuje kauzální závislost.

Příklad na obrázku 6.8 zobrazuje tři rizika, která jsou kauzálně závislá. První riziko (4A) zachycuje zpoždění zadávacího řízení na dodávku infrastruktury produkčního prostředí, kde je nutná součinnost s dodavatelem softwaru. Dopad tohoto rizika je zpoždění kritické cesty v harmonogramu implementačního projektu. Druhé riziko (4B) zachycuje nutnost zrychlit integrační a zátěžové testy v produkčním prostředí, kvůli zpoždění kritické cesty. Zde je vidět kauzální závislost mezi těmito riziky – dopad prvního rizika se stává rizikovým fakto-



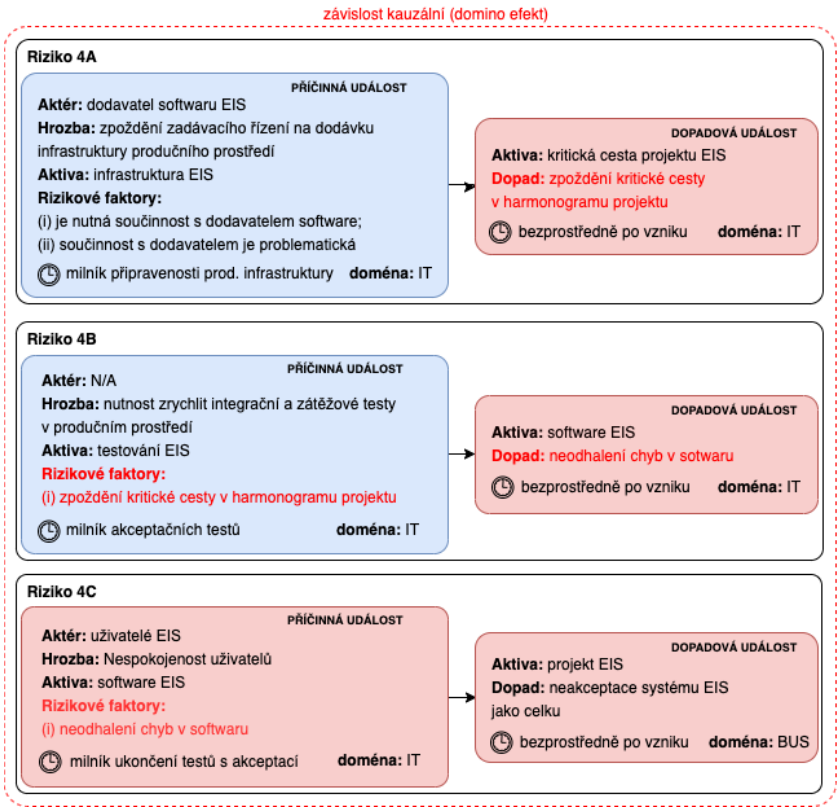
Obrázek 6.6: Rizika demonstrující závislost časovou



Obrázek 6.7: Schématické znázornění rizik s kauzální závislostí

rem rizika druhého. Dopad rizika 4B jsou chyby v uživatelském nastavení neobjevené testy. Třetí riziko (4C) zachycuje nespokojenost koncových uživatelů s implementací systému kvůli neodhaleným chybám, což má za následek neakceptaci díla jako celku. Mezi rizikem 4B a 4C je také kauzální závislost daná dopadem rizika 4B a shodujícím se rizikovým faktorem rizika 4C.

Tento příklad je vcelku triviální a slouží pro demonstraci typu kauzální závislosti. V kapitole 7.5 uvádím nalezený domino efekt na množině všech testovacích rizik, který je rozsáhlejší.



Obrázek 6.8: Rizika demonstrující kauzální závislost (domino efekt)

6.2.6 Souhrn identifikovaných závislostí

Následující seznam zachycuje všechny identifikované typy závislostí:

1. závislost příčinná,
2. závislost dopadová,
3. závislost časová,
4. závislost kauzální (domino efekt).

6.3 Posuzování síly vzájemných závislostí rizik

V předchozí části jsem popsal na konkrétních rizicích, jak identifikovat vzájemné závislosti mezi těmito riziky. Jakmile jsou nějaká rizika identifikována jako závislá, je nutné posoudit sílu jejich vzájemné závislosti. Pro tyto účely navrhuji tzv. test síly závislosti, který je popsán v závěru této podkapitoly. Nyní uvádím některé důležité poznatky, které jsem během analýzy vzájemných závislostí rizik objevil a z nichž vychází zmíněný test síly závislosti.

6.3.0.1 Kombinace vzájemných závislostí

Všechny výše identifikované závislosti se mohou navzájem kombinovat a tím zesilovat sílu vzájemné závislosti mezi danými riziky.

Například nebezpečnou kombinací je kombinace závislosti dopadové a časové, kdy se v rizicích shoduje dopadové aktivum a čas dopadu. Taková rizika ohrožují totéž aktivum ve stejný čas a to může být kritické. Naopak, když je čas různý, závislost není tak nebezpečná a obě rizika, pokud nastanou, se jednotlivě mohou dát zvládnout snáze.

6.3.0.2 Test síly závislosti

Test síly závislosti mezi riziky slouží k určení stupně síly závislosti, jaká mezi riziky vzniká. Test spočívá v nalezení společných prvků (nebo vlastností) mezi dvěma riziky a počet těchto shodujících se prvků určí sílu závislosti. Čím více společných prvků mají posuzovaná rizika ve scénářích, tím větší je síla závislosti těchto rizik. Tato síla společně s danými závislými riziky a typem závislostí je stěžejní informací pro rizikové manažery. Prvky, které jsou v rámci jednotlivých typů závislostí testovány na shodu, jsou:

1. Příčinná závislost:
   - aktér,
   - hrozba,
   - příčinná aktiva,
   - rizikové faktory,
2. Dopadová závislost:
   - dopadová aktiva,
   - dopad,
3. Časová závislost:
   - čas dopadové události,
4. Kauzální závislost (domino efekt):
   - shoda dopadu s hrozbou,
   - shoda dopadu s rizikovými faktory,
   - shoda příčinného a dopadového aktiva.

Dále je nutné testovat kauzální závislost, zda se shoduje dopad jednoho rizika s hrozbou či rizikovým faktorem druhého rizika (domino efekt).

U testování shody prvků, kterých může být v příčinné či dopadové události rizika více (aktiva a rizikové faktory), je nutné otestovat každý prvek s každým

v těchto množinách. Jestliže se najde shoda alespoň v jedné dvojici prvků na scénářích posuzovaných rizik, je identifikována závislost rizik daného typu. Pokud je nalezena další závislost na rozdílných prvcích, je inkrementována síla závislosti rizik. S dalšími identifikovanými závislostmi se tedy síla závislosti zvyšuje. Pokud je však nalezena další shoda na typově shodných prvcích (nejčastěji na více rizikových faktorech či aktivech), na nichž již byla závislost dříve identifikována, síla závislosti se již z pragmatických důvodů nezvětšuje a k inkrementaci hodnoty síly závislosti v takovém případě již nedochází. Pro příklad: shodují-li se v příčinných událostech dvě aktiva (tj. dva shodné páry), síla závislosti je zvětšena pouze o jeden stupeň.

Kapitola 7

Systém DOMINO na identifikaci vzájemných závislostí rizik

Po identifikaci a popsání možných vzájemných závislosti mezi riziky v předchozí kapitole, navrhuji nový informační systém, který bude schopen takové závislosti identifikovat a usnadní manažerské posouzení vzájemně závislých rizik. Návrh systému vychází ze zkušeností se současnými systémy řízení rizik popsanými v kapitole 5, ale protože žádný ze systémů problematiku závislostí neřeší, funkcionalitu navrhuji od základu. Hlavním přínosem navrhovaného systému je schopnost identifikovat vzájemné závislosti mezi riziky, což je umožněno díky vyjádření rizik v rámci nově v práci navržených rizikových scénářů. Z čeho se scénář skládá a jak je sestaven bylo popsáno v kapitole 6.1.

Celá tato kapitola se řídí kroky a praktiky popsanými v knize Software Engineering [29], která popisuje celý životní cyklus analýzy, návrhu, implementace a testování softwarových produktů.

Na závěr kapitoly je popsána implementace prototypu tohoto systému, na kterém jsem úspěšně otestoval a ověřil stěžejní funkcionalitu navrženého systému a samotný způsob identifikace vzájemných závislostí rizik.

7.1 Analýza

První část – analýza – pokrývá sepsání funkčních a nefunkčních požadavků a jejich podrobnou specifikaci. Také jsou zde sepsány případy užití (use-cases) systému.

7.1.1 Funkční požadavky

Níže jsou vypsány všechny funkční požadavky na systém, které jsou rozdělené do 4 oblastí: Dashboard Management, Rizika, Vzájemné závislosti a Integrace.

7.1.1.1 Oblast Dashboard & Management

F 1.1 Registrace uživatelského účtu – na základě zakoupené licence je uživateli umožněno založení uživatelského účtu (individuální nebo firemní licence). U firemní licence je možno zřídit 5 uživatelských podúčtů. V případě potřeby více uživatelů je možné dokoupit další uživatle po jednotkách.

F 1.2 Správa uživatelského účtu – editace uživatelských údajů právě přihlášeného uživatele (celé jméno, přihlašovací jméno, e-mail, profilová fotka). V případě firemní licence existují uživatelé s právy `admin`, kteří mohou editovat i ostatní účty spojené s touto firemní licencí.

F 1.3 Logování změn – u každého uživatele jsou zaznamenávány veškeré změny, které provádí týkající se definice a úprav rizik. Tyto změny se dají zobrazit na úrovni uživatele nebo na úrovni konkrétního rizika.

7.1.1.2 Oblast Rizikové scénáře

F 2.1 Vytvoření domény pro rizika – uživatel může vytvořit domény, do kterých bude přiřazovat příčinné a dopadové události rizik.

F 2.2 Vytvoření rizika – uživatel může vytvářet rizika podle definované struktury v kapitole 6.1. *Tento požadavek je detailně specifikován v části 7.1.3.1.*

F 2.3 Duplikování rizika – vytvoření nového rizika je možné duplikováním již existujícího rizika.

F 2.4 Náhled na existující rizika při definici scénáře – během definice nového rizika je možné zobrazit již existující rizika pro účely porovnání.

F 2.5 Smazání (archivace) rizika – smazání rizika jej pouze přesune do archivu, ze kterého jde dále vymazat úplně. Při archivaci je také nutné automaticky odstranit vzájemné závislosti tohoto rizika.

F 2.6 Zobrazení seznamu rizik – seznam rizik zobrazuje základní údaje o rizicích a možnost zobrazení detailu.

F 2.7 Zobrazení detailu rizika – rozkliknutí rizika ze seznamu zobrazí detailní informace rizika a také seznamu závislostí na ostatní rizika a rizikovou mapu těchto závislých rizik.

F 2.8 Aktualizace rizika – editace již vytvořeného rizika. Po potvrzení změn musí znovu proběhnout nalezení závislostí vůči tomuto změněnému riziku. Změny jsou logovány pod rizikem i uživatelem.

F 2.9 Přidání komentáře k riziku – uživatelé mohou přidávat komentáře k rizikům s poznámkami.

F 2.10 Zobrazení rizikové mapy – vedle zobrazení seznamu rizik je zobrazená i interaktivní riziková mapa. *Tento požadavek je detailně specifikován v části 7.1.3.2.*

F 2.11 Filtrace rizik – seznam rizik je možné filtrovat podle aktéra, příčinných a dopadových aktiv, kategorií, domén, uživatele (tvůrce rizika) a zvolené odpovědi na riziko.

F 2.12 Řazení rizik – seznam rizik je možné seřadit podle pravděpodobnosti, závažnosti a času příčinné a dopadové události.

F 2.13 Vytvoření opatření – opatření je možné vytvořit s návazností na příčinnou událost nebo dopadovou událost. U příčinné události se opatření váže na rizikové faktory nebo hrozby a snižuje se tím pravděpodobnost výskytu rizika. U dopadové události se opatření snižuje závažnost rizika.

F 2.14 Zvolení odpovědi na riziko – u rizik je možné zvolit, jak bude riziko řízeno – mitigace, vyhnutí, sdílení, akceptace. Jestliže je definováno nějaké opatření vůči riziku, odpovědí je automaticky mitigace.

F 2.15 Správa aktiv a aktérů – aktiva a aktéry je možné spravovat odděleně mimo rizika.

7.1.1.3 Oblast Vzájemné závislosti

F 3.1 Nalezení závislostí pro dané riziko – při přidání nového rizika bude proveden test na závislost se všemi již existujícími riziky. Hledat se budou všechny typy závislostí definovaných v kapitole 6.2.

F 3.2 Výpočet síly identifikované závislosti – nalezené závislosti budou ohodnoceny na základě toho, jak moc silná závislost mezi nimi je. Tuto funkcionalitu bude zařizovat tzv. test síly závislosti. *Tento požadavek je detailně specifikován v části 7.1.3.3.*

F 3.3 Zobrazení závislostí pro dané riziko – u detailu rizika je zobrazen seznam závislostí s ostatními riziky a riziková mapa zobrazující tyto závislosti.

F 3.4 Zobrazení detailu závislosti – závislosti ze seznamu je možné rozkliknout a zobrazit detailní informace. *Tento požadavek je detailně specifikován v části 7.1.3.4.*

F 3.5 Vytvoření či zrušení závislosti manuálně – závislosti je možné vytvářet i manuálně, dle uvážení uživatele. Rušit lze pouze manuálně vytvořené závislosti. Automaticky vytvořené závislosti lze pouze skrýt.

7.1.1.4 Oblast Integrace

F 4.1 REST API – integrace mezi backendem a frontendem je realizována pomocí REST API.

F 4.1 Import a export scénářů – je možné hromadně importovat a exportovat scénáře ve formátu JSON. Export je možné omezit filtrováním scénářů.

7.1.2 Nefunkční požadavky

Nefunkční požadavky se týkají převážně použitých technologií pro vývoj a nasazení do provozu.

N 1.1 Backend systému vyvinut v Pythonu – backend systému bude realizován v programovacím jazyku Python.

N 1.2 Využití technologie ORM pro ukládání dat – Obejct Relation Mapping umožňuje ukládat data do databáze jako objekty a také s nimi tak pracovat.

N 1.3 Frontend systému vyvinut jako SPA (single-page application) – použití moderního frameworku pro vytvoření frontendu systému, který bude podporovaný v nejnovějších prohlížečích Chrome, Firefox a Safari.

N 1.4 REST API definováno pomocí Swagger – definice REST API s pomocí nástroje Swagger zajistí automaticky generovanou dokumentaci a testovací prostředí.

N 1.5 Nasazení pomocí technologie Docker v cloudu – doporučeno je nasazení aplikace přes platformu Docker v cloudovém prostředí Amazon Web Services (AWS).

7.1.3 Specifikace vybraných požadavků

Některé funkční požadavky vyžadují podrobnější specifikace, které jsou uvedeny v následujících částech.

7.1.3.1 Specifikace F 2.2 Vytvoření rizika

Softwarová reprezentace rizika musí odpovídat definici rizika z kapitoly 6.1. Pravděpodobnosti rizik budou uváděny kvalitativně a to pomocí 5 hodnotové škály zobrazené v tabulce 7.1. Závažnost rizik bude uváděna obdobně na stupnici od 1 do 5, která je zobrazená v tabulce 7.2.

Tabulka 7.1: Hodnoty pravděpodobnosti výskytu rizika

Číslo	**Hodnota**	**Popis**
1	Ojedinělé	Riziko se vyskytne pouze ve výjimečných případech a za specifických podmínek.
2	Nepravděpodobné	Riziko se někdy může vyskytnout, ale je to nepravděpodobné.
3	Možné	Riziko se někdy může vyskytnout (např. za specifických podmínek).
4	Pravděpodobné	Riziko se pravděpodobně vyskytne.
5	Téměř jisté	Riziko se téměř vždy vyskytne.

Tabulka 7.2: Hodnoty závažností rizik

Číslo	**Hodnota**	**Popis**
1	Zanedbatelné	Situace sice negativně omezuje chod firmy, ale nezpůsobuje ztráty.
2	Nevýznamné	Situace omezuje vnitřní chod firmy (např. dojde k časovým zpožděním).
3	Střední	Situace nebezpečně ovlivní vnitřní i vnější chod společnosti (např. ztráty vzniknou, ale firma je schopna dále fungovat).
4	Významné	Situace velmi nebezpečně ovlivňuje vnitřní i vnější chod společnosti (např. vznik významných ztrát finančních, časových, vznik soudních sporů, apod.).
5	Kritické	Situace zásadně omezí nebo ukončí provoz společnosti (např. bankrot, ztráty na životech apod.).

7.1.3.2 Specifikace F 2.10 Zobrazení rizikové mapy

Interaktivní riziková mapa je hlavním bodem pro zobrazení rizik. Vychází z matice rizik definované v kapitole 2.1, tedy se jedná o 2D pole, které na vodorovné ose znázorňuje pravděpodobnost a na svislé ose závažnost rizik.

Na souhrnné stránce se seznamem rizik bude zobrazena riziková mapa, která zobrazuje všechny rizika jako tečky. Riziková mapa bude směrem dolů rozšířená o pozitivní kvadrant, protože rizika mohou být duálního charakteru, viz kapitola 3. Jestliže uživatel označí jedno z rizik, toto riziko se zvýrazní a spolu s ním i všechna závislá rizika vůči označenému. Zároveň se v seznamu pod rizikovou mapou vyfiltrují pouze závislá rizika.

7.1.3.3 Specifikace F 3.2 Výpočet síly identifikované závislosti

Pro stanovení síly identifikované závislosti je nutné provést test síly, který jsem definoval v podkapitole 6.3.0.2. Pro výpočet velikosti síly je nutné projít po prvcích obě rizika a testovat prvky na shodu (v příčinné i dopadové události, protože závislosti se mohou kombinovat). Dále je nutné odhalit domino efekt, který vzniká na základě shody dopadu jednoho rizika s hrozbou či rizikovým faktorem rizika druhého.

Určení prvků, které se testují na shodu, musí být konfigurovatelné a také musí být možné dodefinovat další dodatečná pravidla, která ovlivní sílu závislosti.

7.1.3.4 F 3.4 Zobrazení detailu závislosti

Při zobrazení detailu závislosti bude vidět o jaký z pěti typů závislostí se jedná, popřípadě jestli jde o kombinaci více závislostí. Podle typu závislosti budou generovány varovné hlášky pro rizikového manažera, které jsou specifikované v tabulce 7.3.

Tabulka 7.3: Varovné hlášky podle typu závislostí

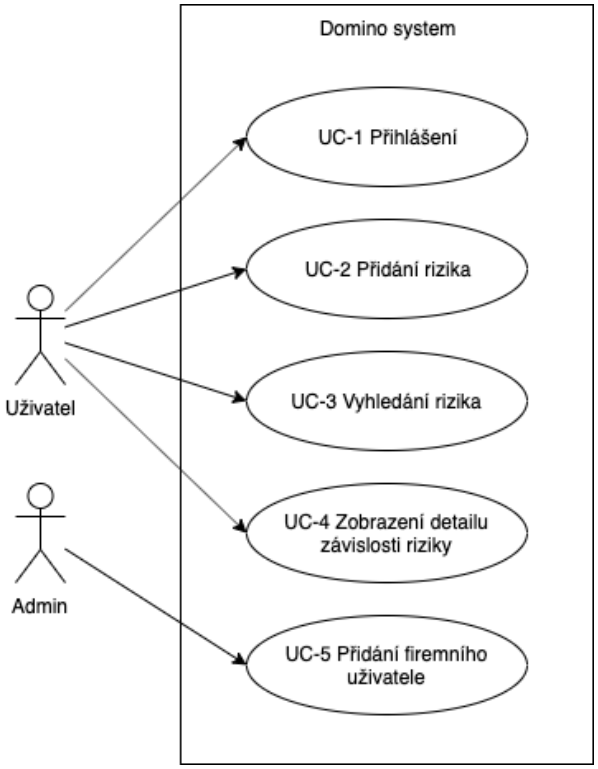
Typ závislosti	**Varovná hláška**
Příčinná	Pozor, shodující se prvky v příčinné události! [výčet prvků] Pozor, stejná příčinná událost!
Dopadová	Pozor, shodující se prvky v dopadové události! Pozor, stejná dopadová událost!
Časová	Pozor, rizika se mohou projevit ve stejný čas!
Kauzální	Pozor, riziko XY může vyvolat domino efekt! Pozor, domino efekt může vyvolat riziko XY!

7.1.4 Případy užití

V rámci analýzy jsem detailně popsal případy užití navrhovaného systému. Celkový pohled na případy užití zobrazuje obrázek 7.1. Jsou zde dva aktéři:

- Uživatel – běžný uživatel, který se systémem pracuje. Jedná se o uživatele s individuální licencí, nebo uživatele firemní licence, kteří nejsou administrátoři.

- Administrátor – uživatel, který má všechna práva jako běžný uživatel, ale navíc může upravovat uživatele pod jednou firemní licencí.



Obrázek 7.1: Diagram případů užití (use-case diagram)

7.1.4.1 UC-1 Přihlášení

Aktér: Uživatel

Vstupní data: Přihlašovací údaje

Spouštěč: Tlačítko ”Přihlásit se”

Předpoklady:

- Uživatel je registrován e-mailem a má platné heslo.
- Backend systému je dostupný.

Hlavní scénář:

1. Uživatel klikne na tlačítko ”Přihlásit se”ve webovém frontendu aplikace.
2. Frontend zobrazí přihlašovací okénko.
3. Uživatel zadá e-mail a heslo.
4. Frontend pošlě požadavek přes API na autentifikaci uživatele (heslo je hashováno).

5. Backend ověří zadaný e-mail a hash hesla vůči databázi registrovaných uživatelů.

6. Backend zašle zpět odpověď, že přihlášení proběhlo úspěšně.

7. Frontend přihlásí uživatele a zobrazí stránku Dashboard.

Alternativní scénář:

- Zadaný e-mail a heslo není validní. Backend zašle zpět odpověď, že přihlášení není úspěšné a uživatel zůstává v přihlašovacím okně s varovnou hláškou.

Akceptační kritéria:

- Uživatel je úspěšně přihlášen do systému.

7.1.4.2 UC-2 Přidání rizika

Aktér: Uživatel

Vstupní data: Prvky a vlastnosti rizika

Spouštěč: Tlačítko "Přidat riziko"

Předpoklady:

- Uživatel je přihlášený.
- Backend systému je dostupný.

Hlavní scénář:

1. Uživatel klikne na tlačítko "Přidat riziko"ve webovém frontendu aplikace.

2. Frontend zobrazí stránku s formulářem pro přidání rizika.

3. Uživatel vyplní všechny údaje tvořící riziko. (Systém poskytuje nápovědy, jak daná pole vyplnit.)

4. Uživatel klikne na tlačítko "Uložit riziko".

5. Frontend pošle požadavek přes API na uložení zadaných dat.

6. Backend uloží data do databáze a vyhledá závislosti vůči nově přidanému scénáři, u kterých spočítá jejich sílu a uloží je do databáze.

7. Backend zašle zpět potvrzení frontendu o úspěšném přidání rizika.

8. Frontend zobrazí hlášku úspěšného uložení rizika a zobrazí uživateli hlavní stránku se souhrnem všech rizik.

Alternativní scénář:

- Ne všechny povinné údaje jsou vyplněny a tlačítko "Uložit riziko"zůstává neaktivní.
- Backendu se nepodaří uložit nové riziko do databáze a vrátí chybu frontenedu. Uživatel nepřijde o již zadané vstupy ve formuláři a pokračuje v editaci.

Akceptační kritéria:

- Nově zadané riziko je uložen do databáze.
- Vzájemné závislosti nově zadaného rizika a všech již existujících jsou nalezeny a je spočítána jejich síla.

7.1.4.3 UC-3 Vyhledání rizika

Aktér: Uživatel

Vstupní data: Vyhledávací kritéria

Spouštěč: Tlačítko "Filtr"na hlavní stránce se souhrnem rizik

Předpoklady:

- Uživatel je přihlášen.
- Backend systému je dostupný.
- Uživatelem má uložený alespoň jedno riziko.

Hlavní scénář:

1. Uživatel klikne na tlačítko "Filtr"na hlavní stránce se souhrnem rizik ve webovém frontendu aplikace.
2. Frontend zobrazí filtrovací formulář s položkami: id, kategorie, doména, odpověď, aktér, hrozba, aktivum (příčinné), aktivum (dopadové), rizikové faktory.
3. Uživatel zadá hodnotu vyhledávajícího kritéria do alespoň jedné položky filtrovacího formuláře.
4. Uživatel klikne na tlačítko "Filtrovat".
5. Frontend pošle požadavek přes API na zobrazení vyfiltrovaného seznamu rizik. Uživatelem zadané hodnoty jsou součástí požadavku.

6. Backend načte z databáze rizika, která splňují vyhledávací kritéria.
7. Backend vrátí frontendu data nalezených rizik.
8. Frontend zobrazí rizika uživateli.

Alternativní scénář:

- Uživatel nezadal hodnotu ani jednoho filtrovacího kritéria. Tlačítko "Filtrovat"zůstává neaktivní.
- Backend nenalezl žádné výsledky pro zadaná filtrovací kritéria. Frontend zobrazí hlášku, že žádné rizika neodpovídají zadaným kritérium.

Akceptační kritéria:

- Všechna rizika, která splňují zadané filtrovací kritéria jsou zobrazena uživateli.

7.1.4.4 UC-4 Zobrazení detailu závislosti mezi riziky

Aktér: Uživatel

Vstupní data: N/A

Spouštěč: Tlačítko "Detail závislosti"v seznamu závislých rizik na stránce detailu rizika

Předpoklady:

- Uživatel je přihlášen.
- Uživatel má uložené alespoň dvě rizika, mezi kterými byla identifikována závislost.
- Uživatel je na stránce detailu jednoho ze závislých rizik.
- Frontend má načtené z backendu všechny závislosti daného rizika.

Hlavní scénář:

1. Uživatel klikne na tlačítko "Detail závislosti"u rizika, vůči kterému chce zobrazit detail závislosti.
2. Frontend zobrazí detail závislosti: typy identifikovaných závislostí, varovné hlášky pro rizikového manažera (definované v tabulce 7.3) a sílu vzájemné závislosti.

Alternativní scénář: N/A

Akceptační kritéria:

- Detail vzájemné závislosti dvou rizik je zobrazen.

7.1.4.5 UC-5 Přidání firemního uživatele

Aktér: Administrátor

Vstupní data: Informace o nově přidávaném uživateli

Spouštěč: Tlačítko "Přidat uživatele"v detailu uživatelského účtu

Předpoklady:

- Administrátor je přihlášen a má zakoupenou firemní licenci.

Hlavní scénář:

1. Administrátor klikne na tlačítko "Přidat uživatele".
2. Frontend zobrazí okno s formulářem pro přidání nového uživatele.
3. Administrátor zadá informace do formuláře: jméno, příjmení, uživatelské jméno, e-mailová adresa (pouze e-mailová adresa je povinná) a potvrdí přidání uživatele tlačítkem "Hotovo".
4. Frontend odešle požadavek přes API na přidání uživatele.
5. Backend uloží zadané informace o uživateli do databáze.
6. Backend odešle informace na zadanou e-mailovou adresu o nově zřízeném účtu a odkaz na nastavení hesla uživatele.
7. Backend zašle zpět potvrzení na frontend o úspěšném přidání uživatele.
8. Frontend zobrazí hlášku adminovi o úspěšném přidání uživatele.

Alternativní scénář:

- Současná licence neumožňuje přidání dalšího uživatele (maximální počet uživatelů je vyčerpán). Tlačítko "Přidat uživatele"je neaktivní.
- Zadaná e-mailová adresa ve formuláři nesplňuje formát. Frontend zobrazí varovnou hlášku o nesprávném formátu e-mailové adresy při kliknutí na tlačítko "Hotovo"a požadavek na backend není odeslán.

Akceptační kritéria:

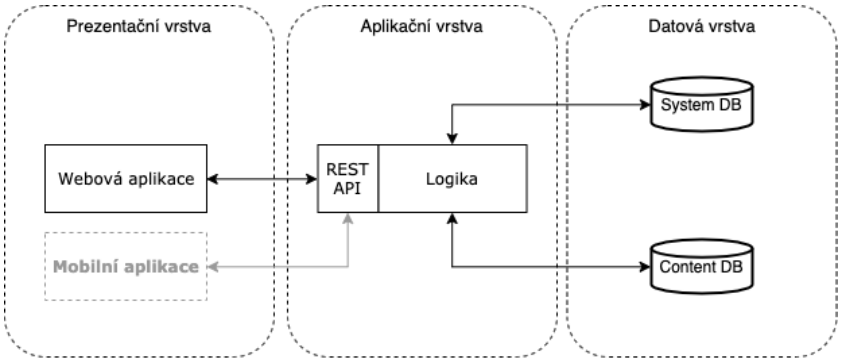
- E-mail s odkazem pro nastavení hesla je odeslán na e-mailovou adresu zadanou ve formuláři pro přidání uživatele.
- Nově přidaný uživatel je zobrazen v seznamu uživatelů.

7.2 Návrh

V druhé části této kapitoly – návrh – se věnuji návrhu architektury systému, datového modelu, komunikačního REST API a grafického uživatelského rozhraní.

7.2.1 Architektura

Systém je navržen v podobě třívrstvé architektury. Tenká prezentační vrstva bude realizována formou webové aplikace a do budoucna je možné rozšíření i na mobilní aplikaci. Prezentační vrstva slouží k interakci s uživatelem a aplikační logika bude implementována na apli-kační vrstvě, tj. webový server přístupný přes REST API. Na datové vrstvě budou vytvořeny dvě SQL databáze: jedna pro systémová data, jako jsou uživatelské účty, licence a přihlašovací údaje a druhá obsahová databáze pro samotná aplikační data – rizika a k nim přidružené entity. Pohled na tuto architekturu je vidět na obrázku 7.2. Hlavní výhodou třívrstvé architektury je obecně ten, že dochází k pružnějšímu rozdělení výkonu mezi zařízením uživatele a serverem. Prezentační vrstva může běžet i na velmi levných a nevýkonných zařízeních.



Obrázek 7.2: Třívrstvá architektura navrhovaného systému

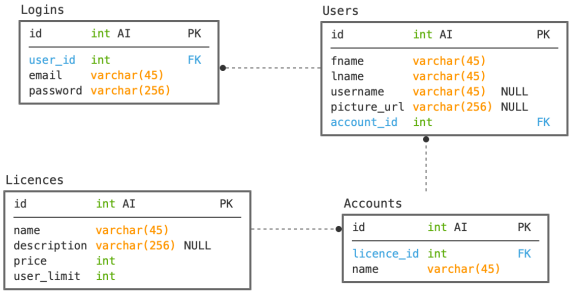
7.2.2 Datový model

Navržený systém obsahuje dvě databáze: systémovou a obsahovou.

7.2.2.1 Systémová databáze

Systémová databáze slouží k ukládání uživatelských informací a licencí. Schéma databáze je zobrazeno na obrázku 7.3.

Tabulka `Users` obsahuje seznam všech uživatelů systému a jejich osobní data: křestní jméno, příjmení, uživatelské jméno a odkaz k uloženému obrázku uživatele na webovém serveru.



Obrázek 7.3: Schéma systémové databáze

Tabulka `Logins` slouží k uložení přihlašovacího e-mailu a hesla každého uživatele. Je dobrou praxí oddělit přihlašovací údaje do samostatné tabulky, protože tím umožníme existenci uživatelů, kteří ještě nebyli přihlášení do aplikace a také tím vylepšíme výkonnost databáze – čtení přihlašovacích údajů bude mnohem frekventovanější než zapisování, a tudíž je dobré jej držet co nejjednodušší.

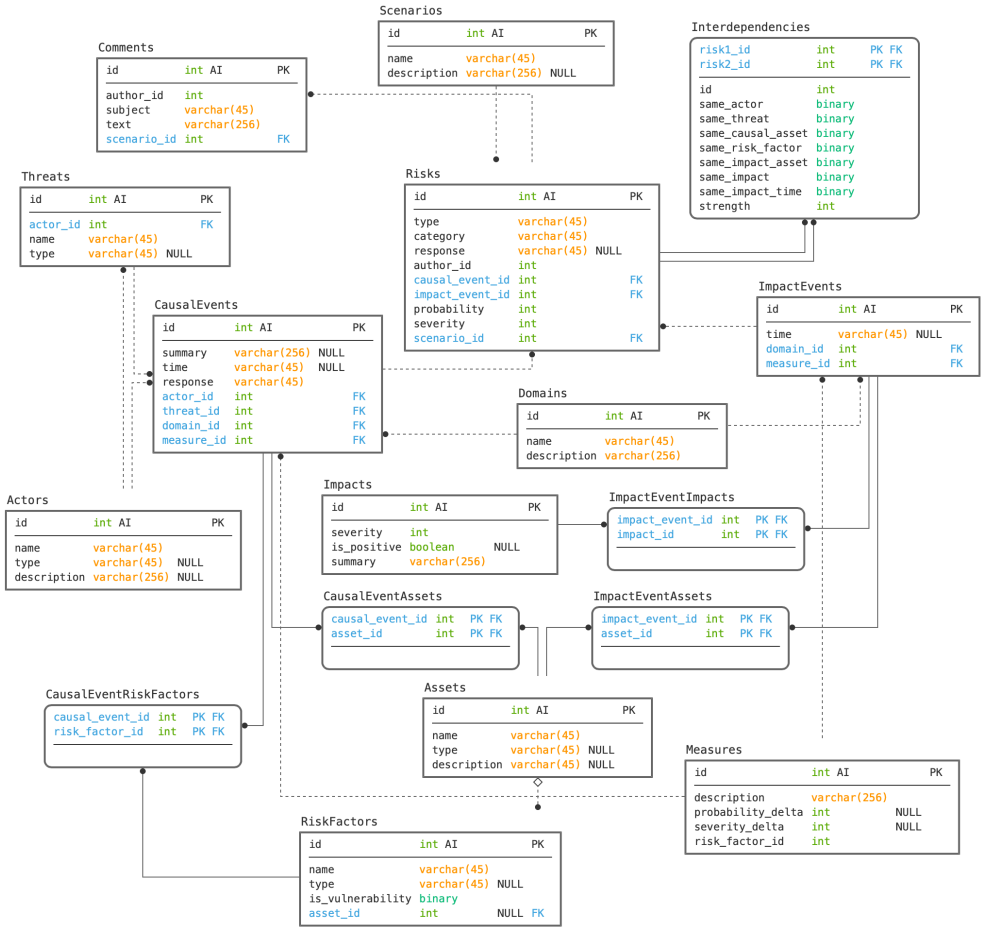
Tabulka `Accounts` slouží k seskupování více uživatelů pod jedním účtem. Odráží to funkční požadavek na existenci skupinových licencí. A tabulka `Licences` drží seznam aktuálně nabízených licencí.

7.2.2.2 Obsahová databáze

Schéma obsahové databáze vychází z velké části z navrženého rizikového scénáře v kapitole 6.1. Tento scénář jsem převedl do struktury relační databáze a doplnil o některé nutné entity a atributy. Obrázek 7.4 znázorňuje celé schéma této databáze.

Hlavní tabulka `Risks` – reprezentující jednotlivá rizika – sdružuje příčinnou událost (`CausalEvents`) a dopadovou událost (`ImpactEvents`). Tabulka aktérů (`Actors`) a hrozeb (`Threats`) je navázaná na příčinnou událost a navíc je vazba mezi aktérem a hrozbou, protože každý aktér disponuje jednou či více hrozbami. Tabulka aktiv (`Assets`) je navázaná na události obou typů (příčinné i dopadové) a kvůli M:N vztahu jsou zde navíc vazební tabulky. Dále jsou na příčinnou událost navázány rizikové faktory (`RiskFactors`), který jsou taky ve vztahu M:N. Navíc jsou rizikové faktory navázané na aktiva, protože rizikový faktor může představovat zranitelnost aktiva. Na dopadovou událost jsou dále navázány dopady (`Impacts`), které mají také vazvy M:N.

Vzájemné závislosti jsou reprezentované tabulkou `Interdependencies`. Tato tabulka reprezentuje entitu pro závislosti a vždy dává do vztahu dvě rizika. Jednotlivé atributy s binární doménou hodnot určují, jestli se v daných



Obrázek 7.4: Schéma obsahové databáze

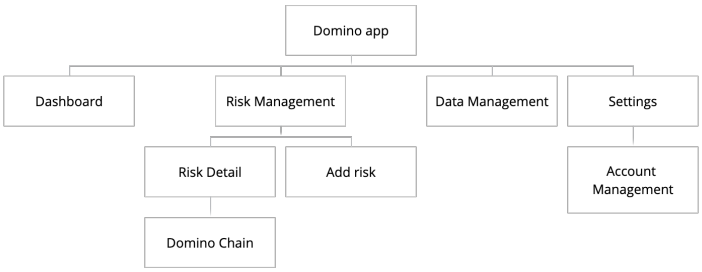
scénářích nachází shoda v prvku, který je dán ve jménu atributu. Atributy, které jsou porovnávány vychází z analýzy vzájemných závislostí v kapitole 6.2.

Tabulka `Measures`, která reprezentuje opatření, je navázaná na příčinnou i dopadovou událost. Dále je na události obou typů navázána doména (`Domains`). K rizikům je ještě přidružená tabulka komentářů (`Comments`), aby mohli uživatelé systému rizika komentovat. Poslední tabulkou je tabulka pro scénáře (`Scenarios`), která shromažďuje více rizik.

7.2.3 Grafické uživatelské rozhraní (GUI)

Grafické uživatelské rozhraní vychází z požadavků na systém a jednotlivých případů užití. Návrh rozhraní je proveden formou wireframů, čili je navrženo obsahové rozvržení jednotlivých obrazovek pro práci se systémem a vztahy

mezi nimi. Jednotlivé navržené obrazovky uživatelského rozhraní jsou přiloženy jako příloha D této diplomové práce. Grafické uživatelské rozhraní vychází z požadavků na systém a jednotlivých případů užití. Návrh rozhraní je proveden formou wireframů, čili je navrženo obsahové rozvržení jednotlivých obrazovek pro práci se systémem a vztahy mezi nimi. Jednotlivé navržené obrazovky uživatelského rozhraní jsou přiloženy jako příloha D této diplomové práce.



Obrázek 7.5: Mapa obrazovek navrženého systému

Na obrázku 7.5 je znázorněná mapa stránek (sitemap) systému. První stránkou je `Dashboard`, která zobrazuje nejdůležitější informace pro uživatele a to:

- graf znázorňující počty rizik v systému dle jejich polohy v rizikové matici (4 úrovně odpovídají čtyřem barvám v matici i grafu),
- graf zobrazující počet nalezených závislostí a jejich síly,
- počet řetězců domino efektu a počet rizik v jednotlivých řetězcích,
- naposledy provedené změny a
- odkaz na správu uživatelů.

Stránka `Risk Management` zobrazuje seznam všech rizik v systému s možností filtrace. Dále zobrazuje interaktivní rizikovou mapu. Z této stránky se dá prokliknout na detail jednotlivých rizik – `Risk Detail`. Zde je zobrazena příčinná a dopadová událost se všemi atributy a sekce zobrazující závislosti tohoto rizika. U závislostí typu domino je možné zobrazit modální okno `Domino Chain`, které znázorňuje řetězec vazeb tohoto rizika v rámci domino efektu. Tato stránka je důležitá pro přehlednost vazeb řetězce příčin a následků a také pro identifikaci první příčinné události, která celý řetězec spustí. Stránka `New Risk` slouží k přidávání nových rizik do systému přes interaktivní formulář.

Stránka `Data Management` slouží k přidávání, editaci a mazání datových položek jako jsou domény rizik, aktéři a aktiva. Na stránce `Settings` je možné provádět nastavení systému a stránka `Account Management` slouží ke správě uživatelského účtu a licence.

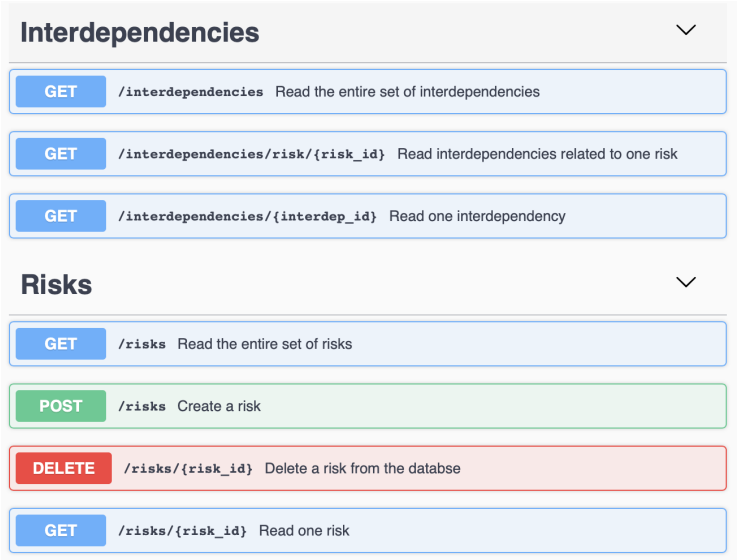
7.3 Implementace prototypu systému

Pro ověření navrženého systému a způsobu identifikace vzájemných závislostí jsem vytvořil prototyp tohoto systému. Prototyp z velké části vychází z návrhu v této kapitole, avšak nepokrývá veškerou funkcionalitu uvedenou ve funkčních požadavcích. Implementoval jsem pouze nezbytné části pro ověření správnosti návrhu identifikace vzájemných závislostí. Implementace jednotlivých částí je popsána níže a všechny zdrojové kódy jsou přiloženy na CD.

7.3.1 Backend

Pro vytvoření backendu systému jsem použil jazyk `Python`, který nabízí mnoho opensourceových knihoven a frameworků usnadňující vytváření webových aplikací. Jako webový server jsem použil framework `Flask` s nadstavbou `Connexion`, která zjednodušuje zpracování HTTP požadavků na základě definice OpenAPI. REST API backendu jsem navrhl ve standardu `Open API 3.0` s pomocí nástroje `Swagger`. Toto REST API má endpointy, které jsou vidět na obrázku 7.6.

Pro externí uživatelské rozhraní jsou tedy v rámci prototypu zpřístupněny přes API rizika a operace hromadného načtení, načtení konkrétního rizika, přidání rizika a smazání konkrétního rizika. A dále jsou zpřístupněny vzájemné závislosti a operace hromadného načtení všech závislostí, načtení závislostí ke konkrétnímu riziku a načtení jedné konkrétní závislosti.



Obrázek 7.6: Popis REST API

Všechna data jsou reprezentována formátem `JSON`, který je výhodný pro svou datovou úspornost a čitelnost. Pro serializaci a deserializaci dat, která

se přes API posílají, používám knihovnu `Marshmallow`. Pro práci s databází využívám knihovnu `SQLAlchemy` s techniku ORM (Object-relational mapping) a databázi `SQLite`. Datový model jsem v prototypu zjednodušil a pracuji pouze s objekty Scénář, Riziko, Aktivum, Rizikový faktor, Dopad a Závislost. Ostatní prvky rizikového scénáře jsou pouze atributy entity Riziko reprezentované pouze textovým řetězcem. Pro porovnání na podobnost těchto řetězců využívám levenshteinovu vzdálenost s experimentálně zvoleným prahem 0,95, čímž naleznu shodu prvků i když nejsou definované naprosto stejně (např. chybějící diakritika, velká/malá písmena, nadbytečná mezera na konci atd.). Opatření nejsou do prototypu zahrnuta z toho důvodu, že nemají význam pro ověření identifikace vzájemných závislostí rizik. Ze stejného důvodu není do prototypu určeného k testování identifikace vzájemné závislosti rizik zařazena funkcionalita uživatelských účtů a licencí.

7.3.2 Frontend

Frontend systému jsem realizoval s pomocí šablonovacího systému `Jinja2`, se kterým se pracuje v jazyku Python a je snadno integrovatelný do webového serveru Flask. Pro usnadnění definice vzhledu a CSS stylů používám knihovnu `Bootstrap`. Pro interakce s uživatelem využívám nadstavbu JavaScriptu `jQuery` a knihovnu `AJAX` pro volání REST API.

7.4 Testovací data

Pro testování prototypu jsem použil vytvořenou množinu 39 rizik, která je uvedena v podkapitole 6.2.1 a také je součástí přílohy C této práce.

7.5 Demonstrace prototypu

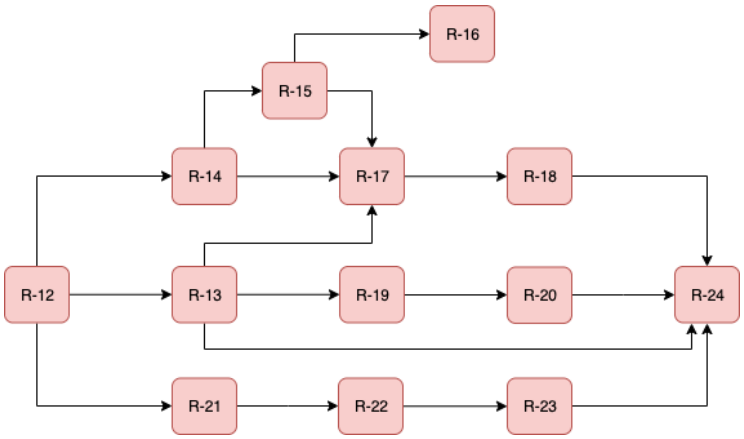
Cílem této podkapitoly je demonstrovat navržený přístup identifikace vzájemných závislostí užitím prototypu systému DOMINO na testovací množině rizik. Stěžejní myšlenkou navrženého přístupu je strukturované popisování rizik pomocí rizikových scénářů. Příklad vyjádření rizika ve schématu rizikového scénáře ve formátu JSON je vidět v ukázce kódu 1.

Pro účely testování jsem importoval množinu 39 rizik do prototypu systému DOMINO a následně spustil algoritmus identifikace vzájemných závislostí s testem síly nalezených závislostí. Mezi těmito riziky bylo identifikováno 24 závislostí kauzálního typu (vyvolávající možný domino efekt), které zde blíže popíši.

Těchto 24 kauzálních závislostí utváří několik izolovaných řetězců příčin a následků, přičemž největší řetězec obsahuje 17 závislostí mezi 13 riziky. Tento řetězec je zobrazen na obrázku 7.7, kde jednotlivé čtverečky reprezentují jednotlivá rizika a textový řetězec uvnitř udává ID rizika (viz příloha C).

```
{
    "id": "R-12",
    "category": "Projekt EIS",
    "actor": "Dodavatel softwaru EIS",
    "threat": "Zpoždění zadávacího řízení na dodávku infrastruktury
               produkčního prostředí",
    "assets_causal": "Infrastruktura EIS",
    "risk_factors": "Je nutná součinnost s˜dodavatelem software;
                     Součinnost s dodavatelem software
                     je problematická",
    "time_causal": "N/A",
    "domain_causal": "IT",
    "assets_impact": "Kritická cesta EIS",
    "impact": "Zpoždění kritické cesty v˜harmonogramu projektu",
    "time_impact": "N/A",
    "domain_impact": "IT",
    "probability": 3,
    "severity": 3
}
```

Ukázka kódu 1: JSON reprezentace rizika

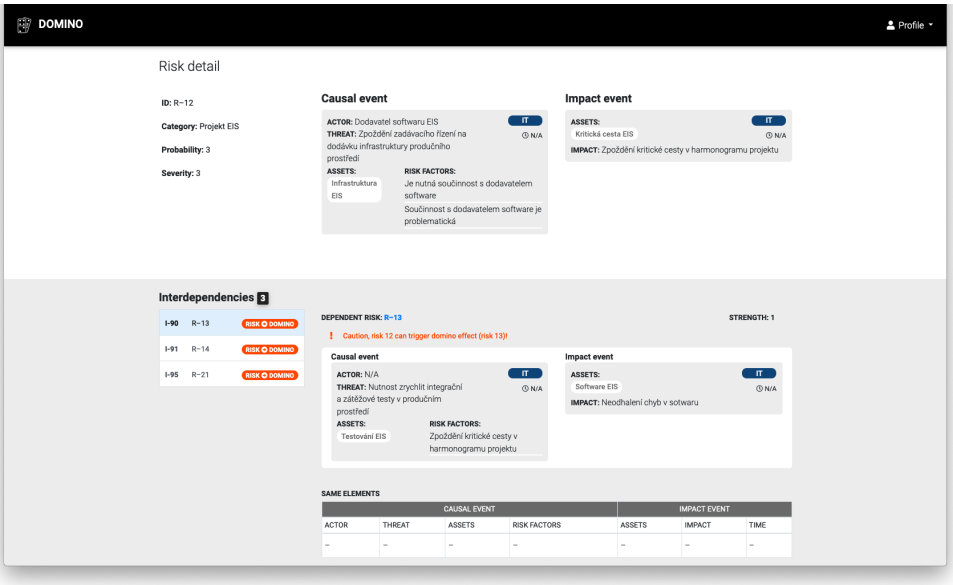


Obrázek 7.7: Největší identifikovaný domino efekt na množině testovacích rizik

Prvotním spouštěčem řetězce událostí je příčinná událost rizika R-12 s hrozbou *Zpoždění zadávacího řízení na dodávku infrastruktury produkčního prostředí.* Toto riziko může být izolovaně posouzeno jako riziko s řádově menším dopadem, než odhalí domino řetězec. Posledním rizikem v řetězci je riziko nespokojenosti koncových uživatelů, které má za dopad neakceptaci implementovaného systému jako celku. Na toto riziko navazuje více rizik, ale všechny jsou následkem prvotního spouštěcího rizika, které domino efekt vyvolá.

Na obrázku 7.8 je snímek obrazovky prototypu systému DOMINO, kde je detail rizika R-12 a detail vzájemné závislosti na riziku R-13. Tato závislost je označena jako kauzální (domino efekt) a je vypsána varovná hláška upo-

zorňující na vznik možného domino efektu.



Obrázek 7.8: Snímek obrazovky prototypu systému DOMINO

7.6 Shrnutí návrhu

Návrh systému vychází ze současných informačních systému pro řízení rizik, ale jelikož se žádný nevěnuje problematice závislostí rizik, tuto funkcionalitu jsem musel celou navrhnout a specifikovat. Funkcionalita systému tedy vychází z požadavků specifikovaných v této kapitole, které byly specifikovány na základě analýzy vzájemných závislostí rizik v kapitole 6.

Navržený systém formou webové aplikace s třívrstvou architekturou následuje současné moderní trendy a plně vyhovuje požadavkům na takový systém. Nejproblémovější oblastí systému je velká citlivost na data na vstupu. Kvalitní výstup vyžaduje kvalitní vstup. Obecně se takovým systémům říká ”garbage in – garbage out”(smetí dovnitř, smetí ven) a vyjadřuje to právě zmíněnou citlivost výstupu na vstupu. Úspěšné odhalení vzájemných závislostí mezi riziky vyžaduje konzistentní definici prvků rizikových událostí napříč riziky.

Kapitola 8

Hlavní zjištění a doporučení dalšího rozvoje

Tato kapitola shrnuje hlavní zjištění diplomové práce a na konci kapitoly uvádím doporučení pro další rozvoj řešené oblasti vycházející z dosažených výsledků.

8.1 Hlavní zjištění

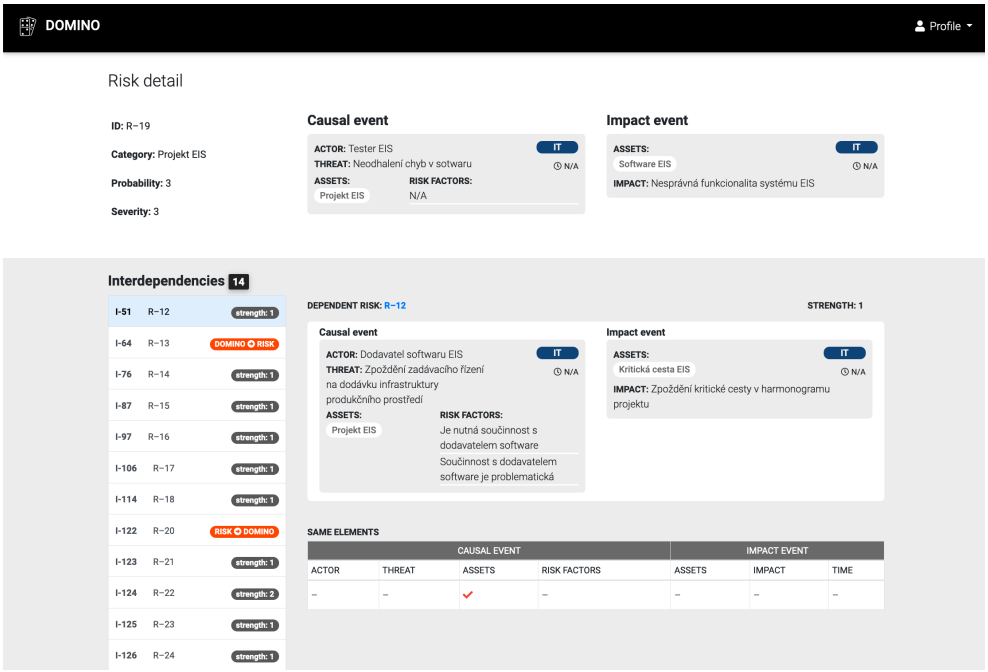
Na základě experimentů s prototypem navrženého systému DOMINO bylo nad množinou testovacích rizik potvrzeno, že typově existují následující závislosti rizik:

- závislost příčinná,
- závislost dopadová,
- závislost časová,
- závislost kauzální (domino efekt).

Zkoumáním těchto závislostí s využitím systému DOMINO jsem došel k řadě zjištění, která zde shrnuji.

8.1.1 Zjištění 1

Struktura (granularita) rizikových aktiv musí být volena pečlivě s ohledem na rozdílnost jejich vzniku. Není vhodné míchat dílčí aktiva s hierarchicky vyššími aktivy, která dílčí aktiva v sobě zahrnují. Aktiva mají být tak specifická, jak jen je to možné. V případě příliš široce zavedených aktiv vniká příliš mnoho triviálních závislostí. Systém DOMINO identifikoval velké množství závislostí, pokud byl aktivem označený např. celý projekt, viz obrázek 8.1.



Obrázek 8.1: Nalezení příliš mnoha závislostí kvůli široce zavedenému aktivu Projekt EIS

8.1.2 Zjištění 2

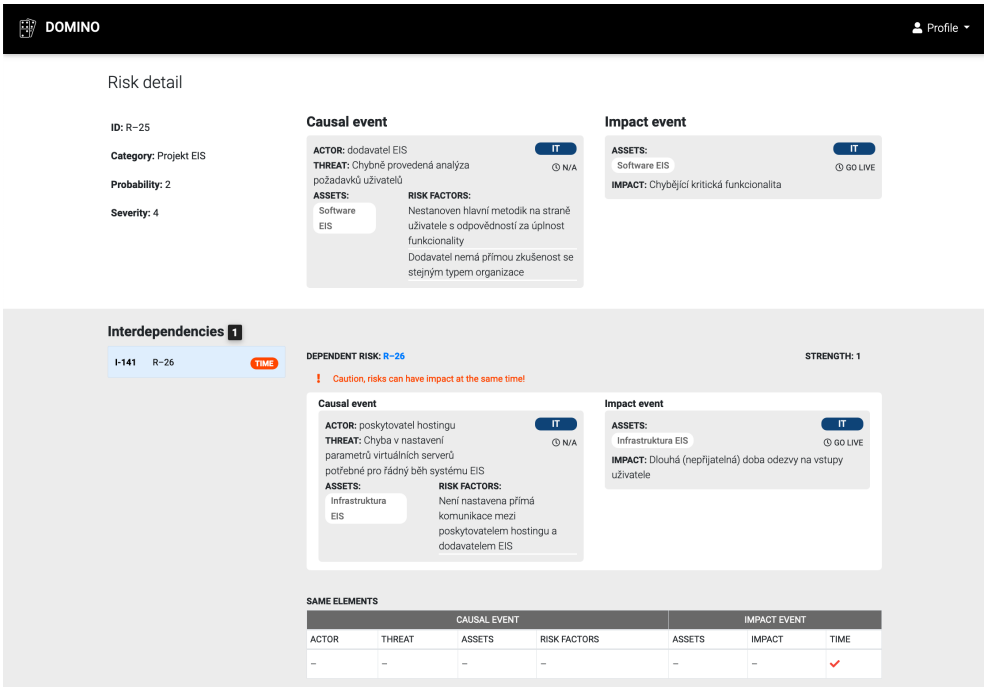
Síla závislosti rizik stupně 1 (nalezení jednoho společného prvku) ještě nemusí znamenat relevantní závislost mezi riziky a jde spíše o signalizaci, že spolu mohou souviset. Při experimentování se systémem DOMINO se prokázalo, že pokud je nalezena síla závislosti o více jak dvou prvcích včetně, je vzájemná závislost rizik již prokazatelná. V takovém případě musí rizikový manažer analyzovat rizika jako závislá a navrhovat proti nim opatření společně.

8.1.3 Zjištění 3

Časový typ závislosti se projevuje v situacích, kdy se v jednom plánovaném časovém okamžiku vytváří rozsáhlá změna. Příkladem je projekt s náběhem implementovaného systému do ostrého provozu k milníku GO-LIVE, ve kterém se může projevit více rizik s dopadovou časovou závislostí. Systém DOMINO tato rizika nalezne a označí způsobem na obrázku 8.2.

8.1.4 Zjištění 4

Domino efekt se dostaví tehdy, pokud je řetězení propuknutí rizik (rizikových událostí) bezprostředně kauzálně po sobě následující, tj. v krátkém časovém



Obrázek 8.2: Nalezení dopadové časové závislosti systémem DOMINO

období nebo i v jednom okamžiku se hromadně v navazujících krocích začnou spouštět všechna tato rizika. Opatření proti rizikům se v krátkém čase pak zpravidla nedají vyvinout a dochází tak ke krizové situaci, která by se z posouzení rizik izolovaně nedala předvídat. U rizik v domino efektu je také důležité více vnímat vzájemné vztahy než jen lineární řetězec příčin a následků.

8.1.5 Zjištění 5

Příčinná závislost mezi riziky je zpravidla jediný z typů závislostí, který je v hlavě srovnatelný a patrný a dá se dovodit i bez přímé podpory od systému DOMINO. To platí zejména tehdy, pokud různé rizikové události působí na shodné příčinné aktivum. Ostatní typy závislostí je již obtížnější odhalit bez analýzy a asistence v systému DOMINO. Složité je zejména odhalení kauzální závislosti rizik s přímou závislostí identifikovatelnou jen mezi dvojicemi rizik, které se na sebe jako příčina-následek zřetězí a tím dojde k propuknutí celého na sebe navázaného řetězce (domino efekt). Systém DOMINO při experimentování se závislostmi prokázal, že závislostí na posuzované oblasti je vždy mnohem více, než se dá při jednotlivém posuzování rizik odhalit a provázanost rizik je v praxi o mnoho intenzivnější, než renomované metodiky na řízení rizik připouštějí. (odkaz na kapitolu).

8.2 Doporučení dalšího rozvoje

Jsem přesvědčen, že navržený systém zdůvodňuje využitelnost a účelnost identifikace vzájemných závislostí rizik v podnikové praxi. Navazující úsilí by mohlo směřovat do vývoje analytického modulu, který by obsahoval rozsáhlou databázi známých rizik z různých odvětví (domén) a identifikoval by závislosti na základě porozumění kontextu uživatelsky definovaných rizik. Pokud by uživatelsky došlo k identifikaci konkrétního rizika, mohl by tak systém sám upozorňovat na typická doprovodná rizika, která nebyla uživatelsky identifikována, a podpořit tím aktivní práci s generickými rizikovými scénáři, jak je vytváří v poslední době pro oblast ICT např. ISACA (viz 2.2.4.3).

Mezi další funkcionalitu systému, která by usnadnila práci rizikovým manažerům, by mohlo patřit generování standardizovaných reportů vyhovujících ISO normám či jiným standardům pro řízení rizik. A také by mohla být vytvořena mobilní aplikace, která by se napojila na stávající REST API a umožňovala by používání systému z mobilních zařízení.

Závěr

Hlavním cílem práce bylo navrhnout systém pro identifikaci vzájemných závislostí rizik. Pro dosažení hlavního cíle práce bylo třeba splnit všechny postupové cíle.

Nejprve jsem prostudoval odbornou literaturu ke stěžejním metodickým přístupům řízení rizik (kap. 2). Pro hlubší pochopení problematiky rizik jsem dále analyzoval dualitu rizik (kap. 3), tj. negativní a pozitivní vlivy rizikových událostí (ztráta, zisk) a také agregaci rizik a vznik vzájemných závislostí rizik (především domino efektu) (kap. 4). Jako hlavní nedostatek současných stěžejních přístupů jsem identifikoval velmi malý důraz na posuzování rizik jako potenciálně vzájemně závislá a neexistenci metody pro nalezení vzájemných závislostí rizik. Dále jsem zkoumal dostupné systémy na trhu pro řízení rizik a neobjevil jsem žádný, který by se zaměřoval na identifikaci vzájemných závislostí rizik (kap. 5).

Pro navržení způsobu identifikace vzájemných závislostí rizik jsem nejprve navrhl nový rizikový scénář, tedy způsob popisování rizik pomocí příčinné a dopadové události, kde každá obsahuje několik prvků, které ji utvářejí (kap. 6.1). Dále jsem navrhl samotný způsob identifikace a posuzování vzájemné závislosti s využitím navrženého scénáře (kap. 6.2) a zejména jsem navrhl způsob identifikace kauzální závislosti mezi riziky vytvářející domino efekt (kap. 6.2.5). Výsledky návrhových činností jsem pak zrealizoval formou vývoje prototypu systému DOMINO vytvořeného za účelem ověření navržené identifikace vzájemné závislosti rizik (kap. 7). Prototyp jsem vyvinul jako webovou aplikaci s třívrstvou architekturou v jazyku Python. Konkrétní výsledky a zkušenosti s posuzováním vzájemné závislosti rizik jsem získal díky testování implementovaného prototypu systému DOMINO nad daty vycházejícími z generických rizikových scénářů v IT podle ISACA. Scénáře jsem dopracoval do konkrétní podoby a doplnil o prvky podle navrženého rizikového scénáře tak, aby mohlo docházet k posuzování vzájemné závislosti rizik (kap. 7.3). Přitom jsem vycházel z mé praxe, kterou jsem získal jako analytik na projektech společnosti Per Partes Consulting, s.r.o.

Navržený přístup se plně potvrdil a testováním vzájemných závislostí rizik jsem s pomocí systému DOMINO získal množství zpětných vazeb na návrhové předpoklady, které vedly k iteračnímu vylepšení celého přístupu a rovněž k získání důležitých zjištění, které jsou uvedeny v předchozí kapitole 8.

Literatura

[1] Vladimír, S.; Rais, K.: *Řízení rizik ve firmách a jiných organizacích.* Grada, 2013.

[2] Společnost pro projektové řízení, o. s.: *Národní standard kompetencí projektového řízení, v3.2.* 2012, [cit. 2019-12-17].

[3] Project Management Institute, Inc.: *Practice standard for project risk management.* 2009, [cit. 2019-12-01]. Dostupné z: http://www.innovativeprojectguide.com/documents/PMIPracticeStandardforProjectRiskManagement.pdf

[4] International Organization for Standardization: *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems – Requirements.* 2013, [cit. 2019-12-09].

[5] International Organization for Standardization: *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.* 2018, [cit. 2019-12-01].

[6] International Organization for Standardization: *ISO/IEC 10006:2003 Quality management systems – uidelines for quality management in projects.* 2003, [cit. 2019-12-09].

[7] International Organization for Standardization: *IEC 31010:2018 Risk management — Risk assessment techniques.* 2018, [cit. 2020-01-28].

[8] International Organization for Standardization: *ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems – Overview and vocabulary.* 2014, [cit. 2019-12-01].

[9] *COBIT 5 for Risk.* ISACA, Information Systems Audit and Control Association, 2013, ISBN 9781604204575. Dostupné z: https://books.google.cz/books?id=k_hgAwAAQBAJ

[10] Alberts, C.; Dorofee, A.; Marino, L.: Mission Diagnostic Protocol, Version 1.0: A Risk-Based Approach for Assessing the Potential for Success. Technická Zpráva CMU/SEI-2008-TR-005, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 2008. Dostupné z: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8665

[11] Alberts, C. J.; Dorofee, A. J.; Marino, L.: *Executive overview of SEI MOSAIC: managing for success using a risk-based approach*. Carnegie Mellon University, Software Engineering Institute, 2007.

[12] Alberts, C.; Dorofee, A.: Mission Risk Diagnostic (MRD) Method Description. Jan 2012, doi:10.21236/ada611114.

[13] Business Term of the Day – Risk appetite/Rizikový apetit. Dostupné z: http://www.englisheditorialservices.com/index.php?q=en/totd&trydate=2-Aug-2017

[14] Kaya, G.: *Good risk assessment practice in hospitals*. Dizertační práce, 03 2018.

[15] Čermák, M.: Inherent vs. residual risk. Jan 2013. Dostupné z: https://www.cleverandsmart.cz/inherent-vs-residual-risk/

[16] Rouse, M.: What is risk mitigation? - Definition from WhatIs.com. Jun 2018. Dostupné z: https://searchdisasterrecovery.techtarget.com/definition/risk-mitigation

[17] Risk Acceptance. Jan 2016. Dostupné z: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-acceptance

[18] *A guide to the project management body of knowledge (PMBOK guide)*. Project Management Institute, Inc., 2017.

[19] *The Risk IT Framework*. ISACA, Information Systems Audit and Control Association, 2009, ISBN 9781604201116.

[20] Pinobarile: The Domino effect. Oct 2007. Dostupné z: https://flic.kr/p/3mfbYG

[21] of Encyclopaedia Britannica, T. E.: Domino theory. Jan 2020. Dostupné z: https://www.britannica.com/topic/domino-theory

[22] THE DOMINO EFFECT: meaning in the Cambridge English Dictionary. Dostupné z: https://dictionary.cambridge.org/dictionary/english/domino-effect

[23] domino effect. Dostupné z: https://www.thefreedictionary.com/dominoeffect

[24] cesta s.r.o, V.: Analýza rizik. Dostupné z: https://www.vlastnicesta.cz/metody/kvalita-systemy-rizeni-iso/analyza-rizik-risk/

[25] Software 42, s. i.: . Dostupné z: https://www.software42.cz/rizika

[26] Software pro řízení rizik ve firmě. Dostupné z: https://www.onesft.com/cs/system-rizeni-rizik

[27] vsRisk – The leading risk assessment tool for ISO 27001 compliance. Dostupné z: https://www.vigilantsoftware.co.uk/topic/vs-risk

[28] IT Risk Management. Dostupné z: https://www.resolver.com/information-security-software/it-risk-management/

[29] Sommerville, I.: *Software engineering*. Pearson, 2011.

Příloha **A**

Seznam použitých zkratek

ISACA Information Systems Audit and Control Association

ISO International Organization for Standardization

SaaS Software as a service

HW Hardware

GUI Graphical User Interface

API Application Programming Interface

REST Representational state transfer

JSON JavaScript Object Notation

SPA Single-page application

Příloha **B**

Obsah přiložené SD karty

- `readme.txt` ..... stručný popis obsahu SD karty
- `src`
  - `impl` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `thesis.pdf` ..... text práce ve formátu PDF
- `wireframes` ..... návrh GUI
- `risks.xlsx` ..... množina testovacích rizik

Příloha C

Testovací množina rizik

ID	ISACA ref.	Kategorie	Příčinná událost						Dopadová událost				Pravděpodobnost	Závažnost
			Aktér	Hrozba	Aktiva příčinná	Rizikové faktory	Čas vzniku	Doména	Aktiva dopadová	Dopady	Čas dopadu	Doména		
01	0201	Projekt IoT Manager	Řídící výbor	Řídící výbor včas nerozhodne o ukončení projektu, který již není potřebný.	Projekt IoT Manager	Projekt je ztrátový	N/A	BUS	Firemní zdroje	Firemní zdroje jsou alokovány na nepotřebný projekt.	bezprostředně po vzniku	BUS	1	4
02	0202	Projekt IoT Manager	Konkurence	Klíčový zaměstnanec odejde ke konkurenci za lepsím platem	Zaměstnanec	Nespokojenost zaměstnance; Nízký plat	N/A	IT	Projekt IoT Manager	Zpoždění projektu Vývoj aplikace IoT Manager	Milestone go-live	IT	2	3
03	–	Projekt IoT Manager	N/A	Zpoždění projektu Vývoj aplikace IoT Manager	Software IoT M.	N/A	N/A	BUS	Finanční zdroje	Sankce jsou placeny kvůli zpoždění projektu	Milestone go-live	BUS	2	4
04	–	Projekt IoT Manager	Virus	Klíčový zaměstnanec onemocní	Zaměstnanec	Slabý imunitní systém	N/A	IT	Projekt IoT Manager	Zpoždění projektu Vývoj aplikace IoT Manager	Milestone go-live	IT	2	3
05	0802	Provoz DMS	Zaměstnanci	V době uzávěrkových operací zaměstnanci nárazově překročí stávající výkonnost infrastruktury.	Infrastruktura DMS	Výkon dimenzován na průměrné zatížení	Konec Q4	IT	Infrastruktura DMS	Výpadek systému DMS	bezprostředně po vzniku	IT	1	3
06	0802	Provoz DMS	Zaměstnanci	V době uzávěrkových operací zaměstnanci nárazově překročí stávající výkonnost infrastruktury.	Infrastruktura DMS	Výkon dimenzován na průměrné zatížení	Konec Q4	IT	Reputace na trhu	Ztráta reputace na trhu	bezprostředně po vzniku	BUS	2	1
07	0802	Provoz DMS	Klienti	V době uzávěrkových operací klienti nárazově překročí stávající výkonnost infrastruktury.	Infrastruktura DMS	Výkon dimenzován na průměrné zatížení	Konec Q4	IT	Infrastruktura DMS	Výpadek systému DMS	bezprostředně po vzniku	IT	4	2
08	0802	Provoz DMS	Klienti	V době uzávěrkových operací klienti nárazově překročí stávající výkonnost infrastruktury.	Infrastruktura DMS	Výkon dimenzován na průměrné zatížení	Konec Q4	IT	Reputace na trhu	Ztráta reputace na trhu	bezprostředně po vzniku	BUS	3	3
09	0804	Provoz DMS	Poskytovatel internetu	Výpadek připojení	Infrastruktura DMS	Není záložní zdroj připojení	N/A	IT	Infrastruktura DMS	Výpadek systému DMS	bezprostředně po vzniku	IT	1	3
10	0804	Provoz DMS	Poskytovatel internetu	Výpadek připojení	Infrastruktura DMS	Není záložní zdroj připojení	N/A	IT	Finanční zdroje	Dodavatel připojení je nucen zaplatit sankce za výpadek.	bezprostředně po vzniku	BUS	1	+1

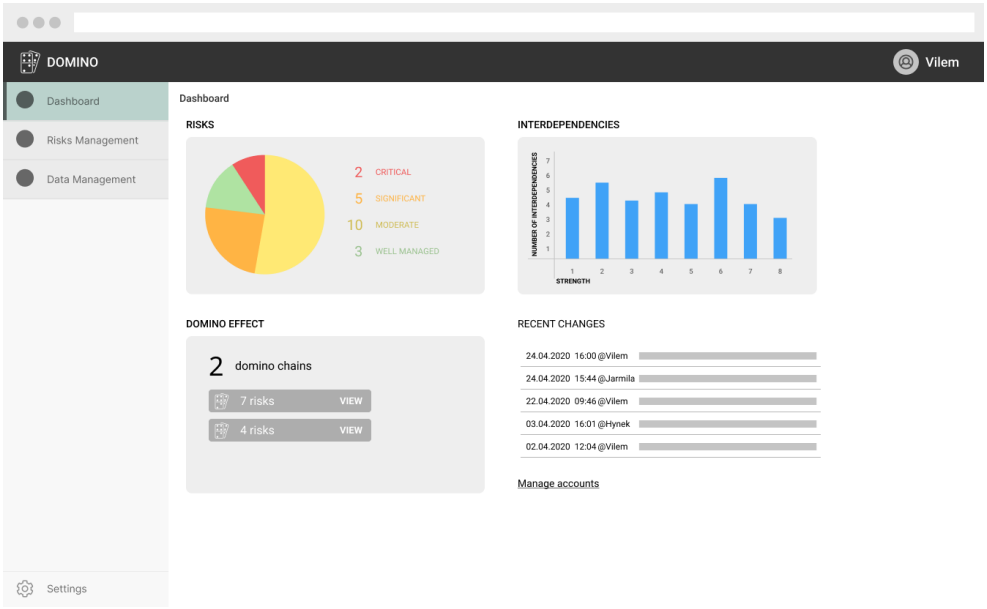
ID	ISACA ref.	Kategorie	Příčinná událost						Dopadová událost				Pravděpodobnost	Závažnost
			Aktér	Hrozba	Aktiva příčinná	Rizikové faktory	Čas vzniku	Doména	Aktiva dopadová	Dopady	Čas dopadu	Doména		
11	–	Provoz DMS	N/A	Výpadek systému DMS	Infrastruktura DMS	Není zajištěns záložní instance systému	N/A	IT	Reputace na trhu	Ztráta reputace na trhu	bezprostředně po vzniku	BUS	1	3
12	–	Projekt EIS	Dodavatel softwaru EIS	Zpoždění zadávacího řízení na dodávku infrastruktury produčního prostředí	Infrastruktura EIS	Je nutná součinnost s dodavatelem software; Součinnost s dodavatelem software je problematická	N/A	IT	Kritická cesta EIS	Zpoždění kritické cesty v harmonogramu projektu	N/A	IT	3	3
13	–	Projekt EIS	N/A	Nutnost zrychlit integrační a zátěžové testy v produkčním prostředí	Testování EIS	Zpoždění kritické cesty v harmonogramu projektu	N/A	IT	Software EIS	Neodhalení chyb v sotwaru	N/A	IT	3	3
14	–	Projekt EIS	N/A	Nutnost zrychlit integrační a zátěžové testy v produkčním prostředí	Testování EIS	Zpoždění kritické cesty v harmonogramu projektu	N/A	IT	Infrastruktura EIS	Chybné nastavení infrastruktury	N/A	IT	3	3
15	–	Projekt EIS	Dodavatel infrastruktury EIS	Chybné nastavení infrastruktury	Infrastruktura EIS	N/A	N/A	IT	Infrastruktura EIS	Výpadek infrastruktury	N/A	IT	3	3
16	–	Projekt EIS	N/A	Výpadek infrastruktury	Infrastruktura EIS	N/A	N/A	IT	Data EIS	Potřeba obnovy dat ze zálohy	N/A	IT	3	3
17	–	Projekt EIS	N/A	Výpadek infrastruktury	Infrastruktura EIS	Neodhalení chyb v sotwaru; Chybné nastavení infrastruktury	N/A	IT	Data EIS; Uživatelé EIS	Uživatelé přijdou o data z posledních nedokončených transakcí	N/A	IT	3	3
18	–	Projekt EIS	N/A	Uživatelé přijdou o data z posledních nedokončených transakcí	Data EIS; Uživatelé EIS	N/A	N/A	IT	Uživatelé EIS	Nespokojenost uživatelů	N/A	BUS	3	3
19	–	Projekt EIS	Tester EIS	Neodhalení chyb v sotwaru	Software EIS	N/A	N/A	IT	Software EIS	Nesprávná funkcionalita systému EIS	N/A	IT	3	3
20	–	Projekt EIS	N/A	Nesprávná funkcionalita systému EIS	Software EIS	N/A	N/A	IT	Uživatelé EIS	Nespokojenost uživatelů	N/A	BUS	3	3

ID	ISACA ref.	Kategorie	Příčinná událost						Dopadová událost				Pravděpodobnost	Závažnost
			Aktér	Hrozba	Aktiva příčinná	Rizikové faktory	Čas vzniku	Doména	Aktiva dopadová	Dopady	Čas dopadu	Doména		
21	–	Projekt EIS	N/A	Neumožnění provést čistění kvality dat	Data EIS	Zpoždění kritické cesty v harmonogramu projektu	N/A	IT	Data EIS	Zanesení chybných dat do systému EIS	N/A	IT	3	3
22	–	Projekt EIS	N/A	Zanesení chybných dat do systému EIS	Data EIS; Software EIS	N/A	N/A	IT	Software EIS	Nefunkčnost workflow EIS	N/A	IT	3	3
23	–	Projekt EIS	N/A	Nefunkčnost workflow EIS	Software EIS	N/A	N/A	IT	Uživatelé EIS	Nespokojenost uživatelů	N/A	BUS	3	3
24	–	Projekt EIS	N/A	Nespokojenost uživatelů	Uživatelé EIS; Software EIS;	Neodhalení chyb v sotwaru	N/A	BUS	Projekt EIS	Neakceptace systému EIS jako celku	N/A	BUS	3	3
25	–	Projekt EIS	dodavatel EIS	Chybně provedená analýza požadavků uživatelů	Software EIS	Nestanoven hlavní metodik na straně uživatele s odpovědností za úplnost funkcionality;	schválení návrhu	IT	Software EIS	Chybějící kritická funkcionalita	GO LIVE	IT	2	4
26	–	Projekt EIS	poskytovatel hostingu	Chyba v nastavení parametrů virtuálních serverů potřebné pro řádný běh systému EIS	Infrastruktura EIS	Není nastavena přímá komunikace mezi poskytovatelem hostingu a dodavatelem EIS	schválení technické studie	IT	Infrastruktura EIS	Dlouhá (nepřijatelná) doba odezvy na vstupy uživatele	GO LIVE	IT	2	2
27	–	Projekt IoT Manager	Programátor	Při závěrečném testování systému se odhalí závažné chyby v jeho naprogramování.	Software IoT M.	N/A	Během programování	IT	Projekt IoT Manager	Projekt je ukončen s předstihem; Zpoždění projektu Vývoj aplikace IoT Manager	Milestone testing	BUS	4	+2 -2
28	0403	Zaměstnanci	Zaměstnanci	Nedostatečná expertiza, kvůli které není možné přijmout nový projekt	Nový potenciální projekt	Vyžaduje přílišnou odbornost; Zaměstnanci nemají chuť učit se novým věcem	N/A	IT	Finanční zdroje	Ušlý potenciální zisk	N/A	BUS	1	3
29	0403	Zaměstnanci	Zaměstnanci	Nedostatečná expertiza, kvůli které není možné přijmout nový projekt	Nový potenciální projekt	Vyžaduje přílišnou odbornost; Zaměstnanci nemají chuť učit se novým věcem	N/A	IT	Zaměstnanci	Zaměstnanci jsou nedostatečně využití	bezprostředně po vzniku	BUS	2	2
30	0403	Zdroje	Zaměstnanci	Přílišné vytížení, kvůli kterému není možné přijmout nový projekt	Nový potenciální projekt	Zaměstnanci jsou nadměrně využití; Zaměstnanci si vezmou dovolenou	N/A	IT	Finanční zdroje	Ušlý potenciální zisk	N/A	BUS	2	2

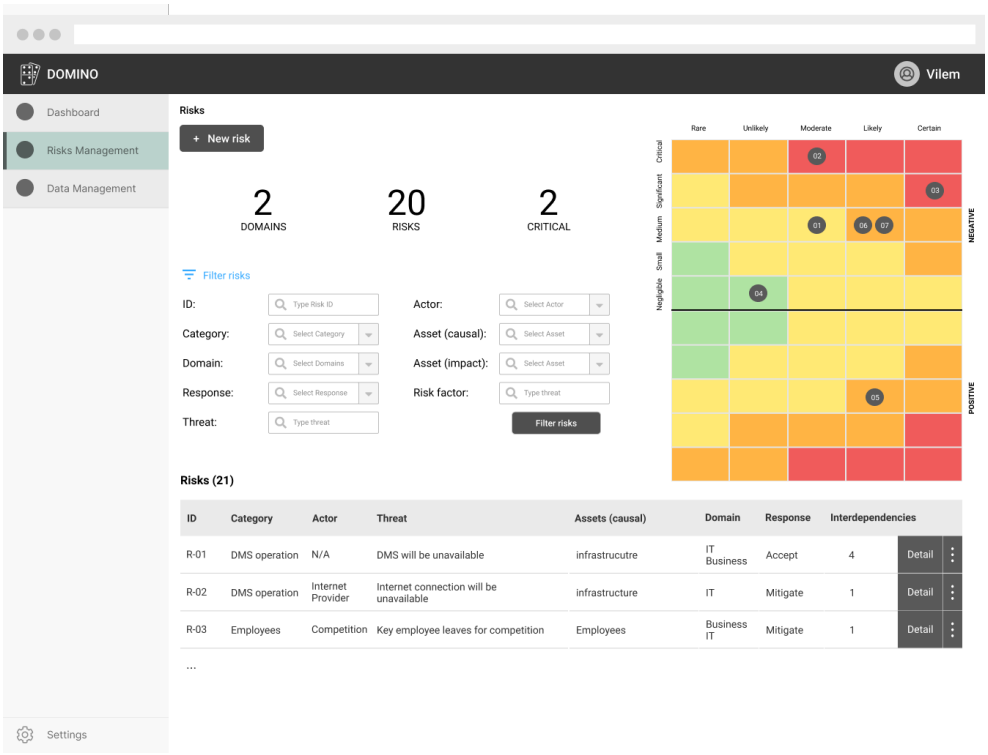
ID	ISACA ref.	Kategorie	Příčinná událost						Dopadová událost				Pravděpodobnost	Závažnost
			Aktér	Hrozba	Aktiva příčinná	Rizikové faktory	Čas vzniku	Doména	Aktiva dopadová	Dopady	Čas dopadu	Doména		
31	0605	Infrastruktura	Čas	Porucha zálohovacího disku	Zálohovací disk	Jedná se o magnetický disk náchylný k poškození	1.1.2024 (čtyři roky po koupi)	IT	FIremní data	Dojde ke ztrátě důležitých záloh	bezprostředně po vzniku	IT	4	3
32	–	Data	Zloděj	Odcizení notebooku zaměstnance	Notebook; Firemní data; Obchodní tajemství	Firemní data jsou uložena na notebooku zaměstnance; Součástí firemních dat je obchodní tajemství o	N/A	IT	Notebook	Ztráta notebooku v hodnotě 50 tis. Kč	bezprostředně po vzniku	IT	3	2
33	–	Data	Zloděj	Odcizení notebooku zaměstnance	Notebook; Firemní data; Obchodní tajemství	Firemní data jsou uložena na notebooku zaměstnance; Součástí firemních dat je obchodní tajemství o	N/A	IT	Obchodní tajemství	Vyzrazení obchodního tajemství	bezprostředně po vzniku	BUS	2	4
34	0610	Data	Zaměstnanec	Předání firemních dat konkurenci	Obchodní tajemství	Přístup zaměstnance k obchodnímu tajemství v době pracovního poměru; Propuštění zaměstnance proti jeho vůli;	N/A	IT	Konkurenční výhoda na trhu	Ztráta konkurenční výhody	bezprostředně po vzniku	BUS	3	2
35	1201	Legislativa	Hacker	Neoprávněný přístup k osobním údajům nechráněných z hlediska přístupu k obsahu	Přihlašovací údaje	Atraktivnost dat; Nezavedeno zabezpečení r	N/A	IT	Přihlašovací osobní údaje (jméno, heslo); Intranet	Průnik hackera do interního systému uniklými přihlašovacími údaji	bezprostředně po vzniku	IT	2	4
36	1201	Legislativa	Hacker	Neoprávněný přístup k osobním údajům nechráněných z hlediska přístupu k obsahu	Přihlašovací údaje	Atraktivnost dat; Nezavedeno zabezpečení r	N/A	IT	Finanční zdroje	Sankce kůli non-complience s GDPR	N/A	BUS	2	4
37	1504	Hacker	Hacker	Krádež přihlašovacích údajů zaměstnance phishingovým útokem	Přihlašovcí údaje	Zaměstnanec není školený na rozpoznání phisingového útoku	N/A	IT	Přihlašovací osobní údaje (jméno, heslo); Intranet	Průnik hackera do interního systému uniklými přihlašovacími údaji	bezprostředně po vzniku	IT	2	4
38	1602	Hacker	Hacker	Odstavení DMS DDoS útokem	DMS	Neefektivní ochrana proti DDos útokům	N/A	IT	DMS	Výpadek systému DMS	bezprostředně po vzniku	IT	2	3
39	2003	Strategie	C level	Nové IT trendy nejsou včas identifikovány	Nové služby	Přílišná zaměstnanost vedení jinými věcmi	Jednou za 4 roky	IT	Konkurenční výhoda na trhu	Prohloubení konkurenční výhody; Ztráta konkurenční výhody	N/A	BUS	2	+2 -3

Příloha D

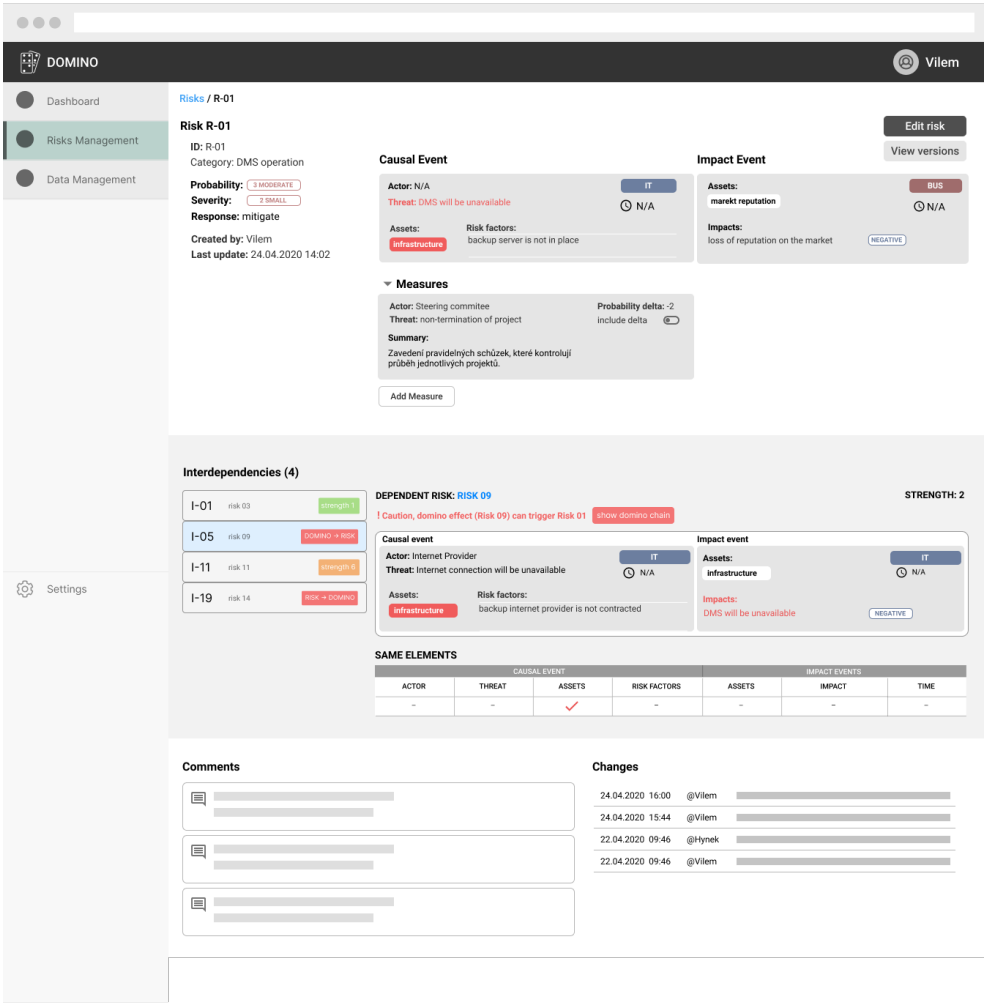
Návrh uživatelského rozhraní (GUI) systému DOMINO



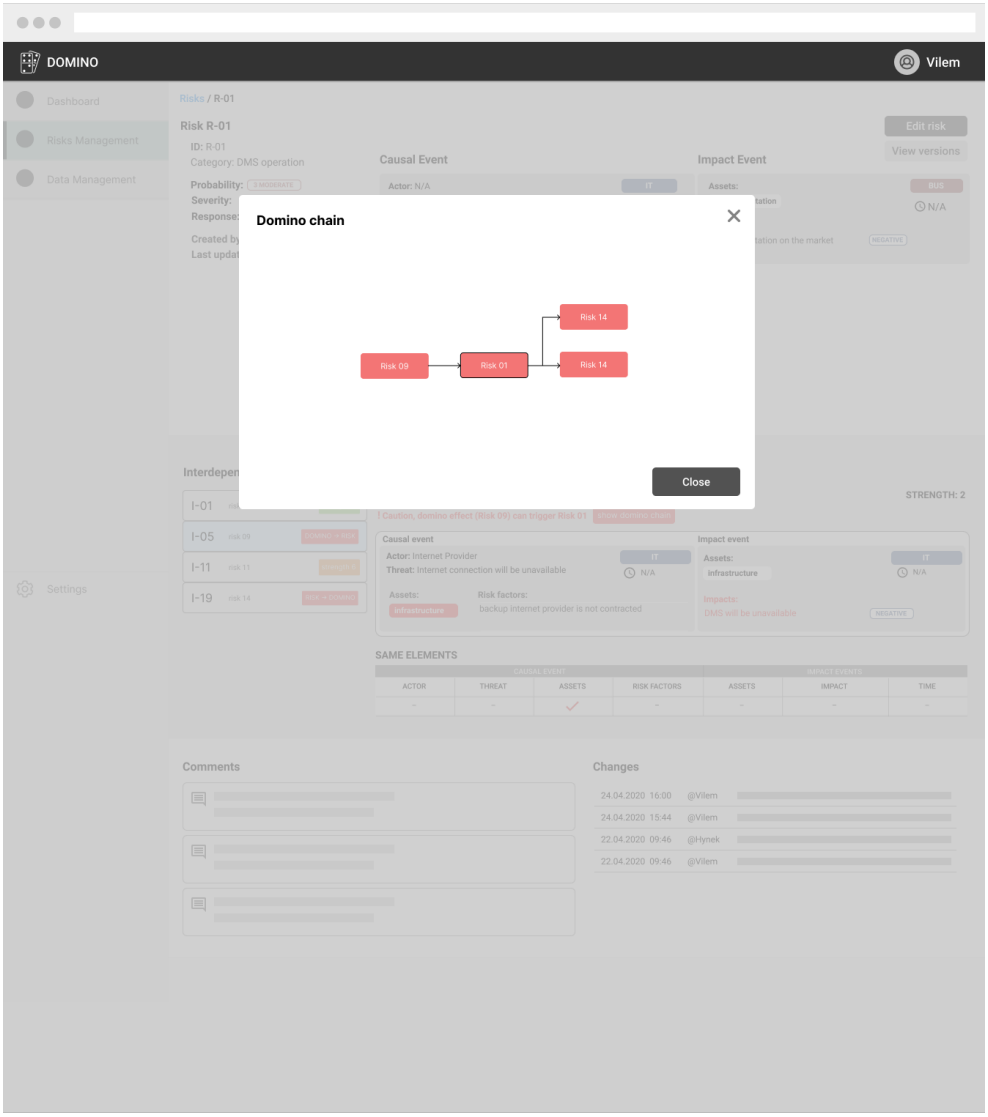
Obrázek D.1: Obrazovka Dashboard



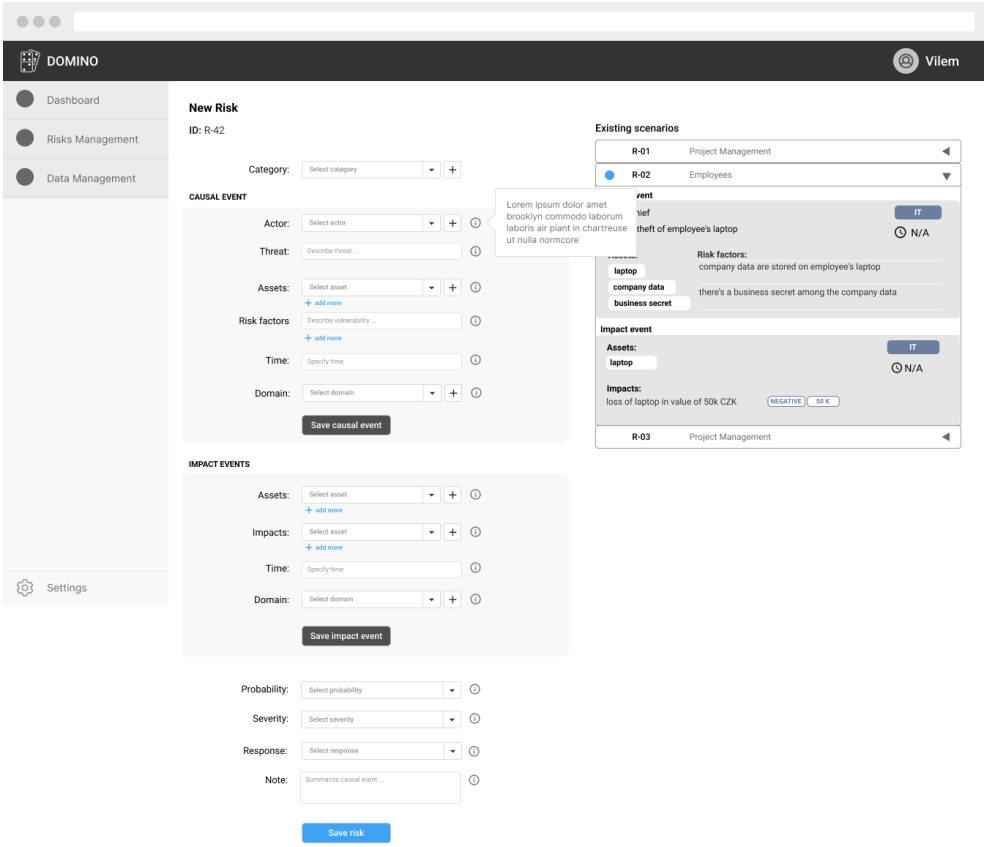
Obrázek D.2: Obrazovka seznamu rizik



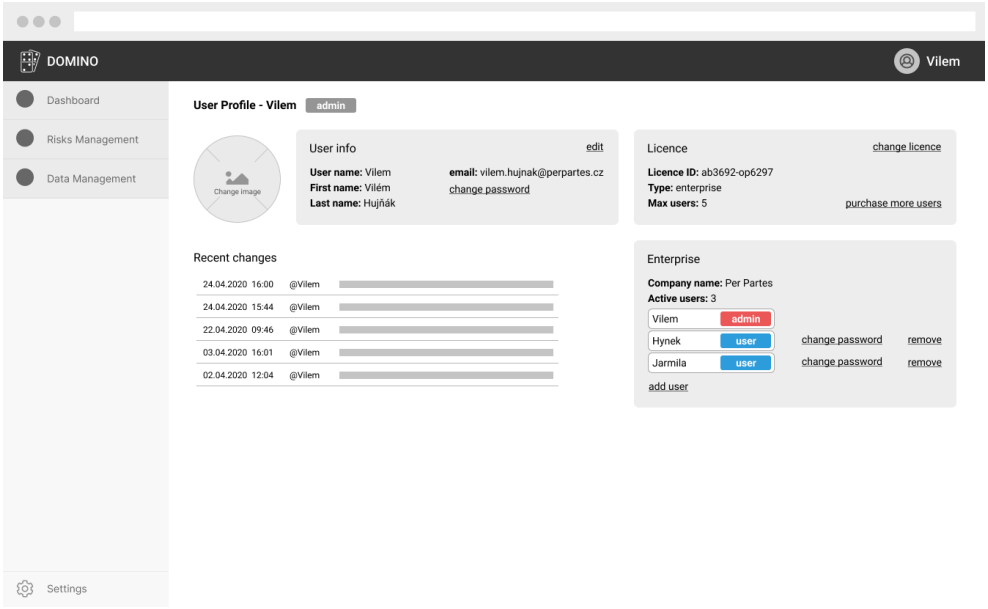
Obrázek D.3: Obrazovka detailu rizika



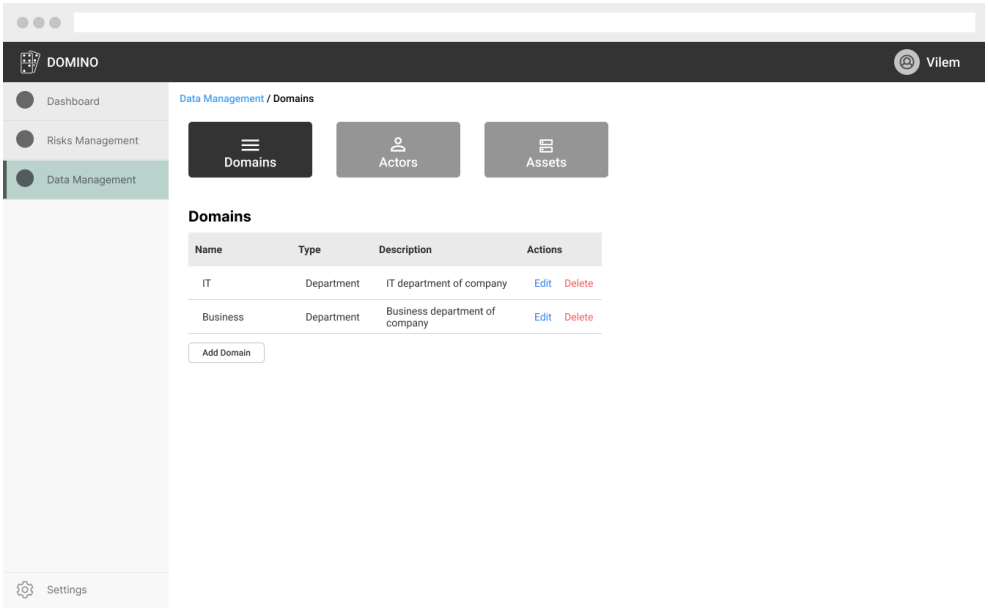
Obrázek D.4: Obrazovka zobrazení řetězce domino efektu



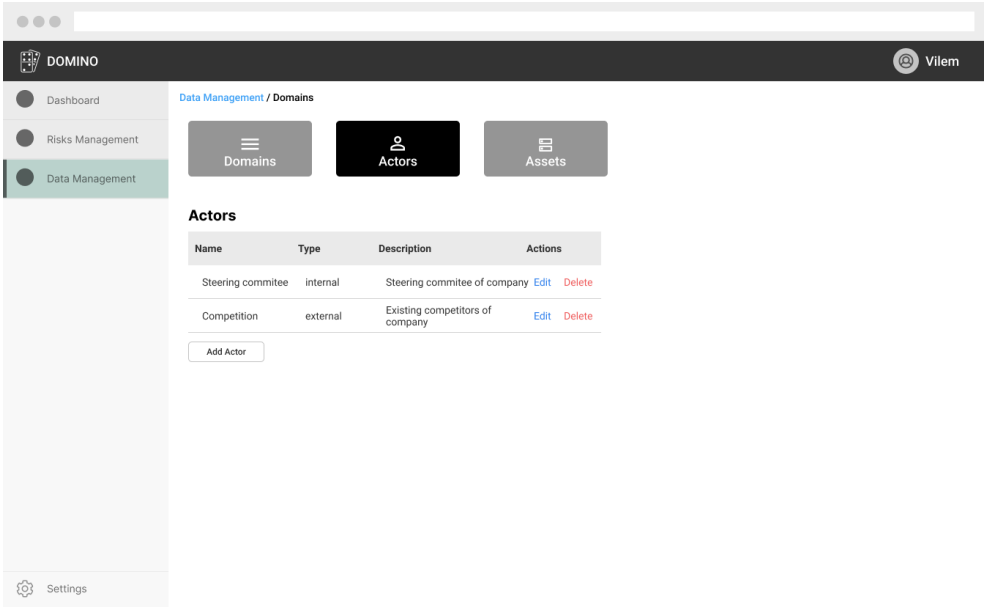
Obrázek D.5: Obrazovka pro přidání nového rizika



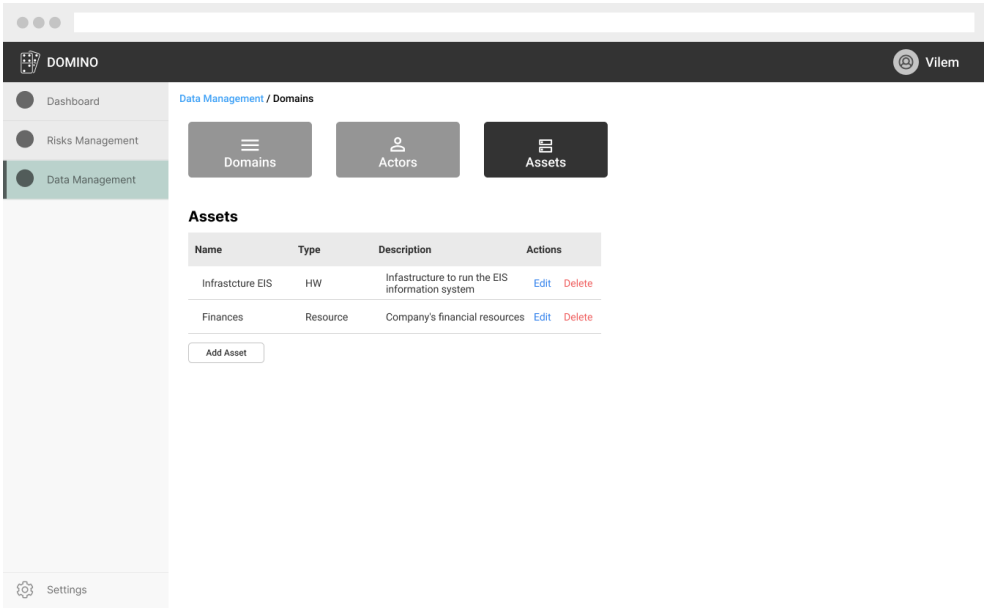
Obrázek D.6: Obrazovka správy uživatelského účtu



Obrázek D.7: Obrazovka pro správu dat – domény událostí



Obrázek D.8: Obrazovka pro správu dat – aktéři



Obrázek D.9: Obrazovka pro správu dat – aktiva