

Návrh zabezpečení podniku v souvislosti se získáním certifikace TISAX, s využitím metod multikriteriálního hodnocení

Bc. Tomáš Příkaský



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Tomáš Přikaský
Osobní číslo:	A23592
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní management
Forma studia:	Kombinovaná
Téma práce:	Návrh zabezpečení podniku v souvislosti se získáním certifikace TISAX, s využitím metod multikriteriálního hodnocení
Téma práce anglicky:	Business Security Proposal in Connection with Obtaining TISAX Certification, Using Multi-Criteria Evaluation Methods

Zásady pro vypracování

1. Uveďte charakteristiku problematiky související se zabezpečením podniku v kontextu certifikace používaném v automotive.
2. Vypracujte analýzu současného stavu použití softwarových nástrojů pro multikriteriální hodnocení variant a analýzy rizik.
3. Zpracujte metodiku zpracování analýzy rizik a multikriteriálního hodnocení informační bezpečnosti a zabezpečení objektu ve vybraném podniku.
4. Zpracujte analýzu rizik ve vybraném podniku.
5. Na základě analýzy rizik navrhnete přehled vhodných opatření.
6. S využitím multikriteriální analýzy vyberte nejvhodnější varianty opatření pro zabezpečení informační bezpečnosti v podniku.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. PROCHÁZKOVÁ, Dana. *Analýza a řízení rizik*. Praha: České vysoké učení technické v Praze, 2011. ISBN 978-80-01-04841-2.
2. JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-7318-456-7.
3. ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN EN ISO/IEC 27001, *Informační technologie – Techniky zabezpečení – Systémy managementu bezpečnosti informací – Požadavky*. Praha, 2023.
4. FOTR, Jiří. *Vícekriteriální rozhodování za nejistoty. Vysokoškolská skripta*. Praha: Oeconomica, 2020. ISBN 978-80-245-2399-6.
5. BARTSCH, Christian. *Information Security Based on VDA ISA TISAX Automotive Strategies*. Amazon Digital Services LLC – Kdp, 2023. ISBN 9798865062653.
6. ISHIZAKA, Alessio a NEMERY, Philippe. *Multi-criteria Decision Analysis, Methods and Software*. Wiley, 2013. ISBN 9781118644911.
7. KIM, Shiko a SHRESTHA, Rakesh. *Automotive Cyber Security – Introduction, Challenges, and Standardization*. Springer Nature Singapore, 2020. ISBN 9789811580536.

Vedoucí diplomové práce: **Ing. David Šaur, Ph.D.**
Ústav matematiky

Datum zadání diplomové práce: **29. listopadu 2024**

Termín odevzdání diplomové práce: **30. května 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 29. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne 20.5.2025

Tomáš Příkaský, v. r.
podpis autora

ABSTRAKT

Tato diplomová práce, si klade za hlavní cíl provést analýzu ve vybraném podniku s cílem zjistit a definovat jeho skutečný stav a navrhnout vhodná opatření tak, aby byl podnik schopen získat mezinárodní certifikaci TISAX, jenž je spjatá se zajištěním informační bezpečnosti v automobilovém průmyslu. Při výběru vhodných opatření práce využívá metodologii multikriteriálního hodnocení. Práce je rozdělena na dvě části, kdy teoretická část se zabývá objasněním základních pojmů spjatých s tématem informační bezpečnosti, popisem standardu TISAX a průzkumem dostupných softwarových nástrojů a metod pro multikriteriální analýzu a analýzu rizik. Praktická část je zaměřena na zpracování metodiky pro získání certifikace TISAX, provedení analýzy rizik a aplikace poznatků z teoretické části v oblasti využití multikriteriálního hodnocení, při výběru nejlepší varianty nápravných opatření.

Klíčová slova: TISAX, analýza současného stavu, informační bezpečnost, multikriteriální analýza, metodika, metodologie, analýza rizik.

ABSTRACT

The main objective of this thesis is to perform an analysis in the selected company in order to identify and define its actual situation and to propose appropriate measures so that the company is able to obtain the international certification TISAX, which is associated with the provision of information security in the automotive industry. In selecting the appropriate measures, the thesis uses a multi-criteria evaluation methodology. The thesis is divided into two parts, where the theoretical part deals with the explanation of basic concepts related to the topic of security, description of the TISAX standard and survey of available software tools and methods for multicriteria and risk analysis. The practical part focuses on the development of a methodology for obtaining certification, conducting risk analysis and applying the knowledge from the theoretical part in the field of the use of multicriteria assessment in the selection of the best variant of corrective measures.

Keywords: TISAX, Analysis of the current state, Information Security, Multicriteria Analysis, Methodology, Risk Analysis.

Rád bych zde vyjádřil srdečné poděkování svému vedoucímu práce, Ph.D. Davidu Šaurovi, za jeho cenné rady, podporu a trpělivost během celého procesu psaní této diplomové práce. Jeho odborné vedení mi pomohlo překonat mnohé výzvy a problémy, které se při psaní této práce objevily. Dále bych chtěl poděkovat své rodině a přátelům, za jejich neustálou podporu, motivaci a pochopení. Bez jejich povzbuzení, by realizace této práce nebyla možná.

Motto:

„Vzdělání je nejmocnější zbraní, kterou můžete použít ke změně světa“

Nelson Mandela

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	13
1 CHARAKTERISTA PROBLEMATIKY	14
1.1 INFORMAČNÍ BEZPEČNOST	14
1.1.1 Rozdíl mezi kybernetickou a informační bezpečností	15
1.2 TRIÁDA CIA (CONFIDENTIALITY, INTEGRITY, AVAILABILITY)	16
1.2.1 Důvěrnost (Confidentiality)	18
1.2.2 Integrita (Integrity)	19
1.2.3 Dostupnost (Availability)	19
1.3 SYSTÉM ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI (ISMS)	20
1.3.1 Cyklus PDCA (Plan-Do-Control-Act)	21
1.3.2 Metoda DMAIC	22
2 CERTIFIKACE TISAX.....	23
2.1 HLAVNÍ CÍLE	24
2.2 ISO/IEC 27001	28
2.2.1 Rozdíl mezi ISO/IEC 27001 a certifikací TISAX.....	30
2.3 PRŮBĚH CERTIFIKACE.....	31
2.3.1 Přípravná fáze a registrace	31
2.3.2 Hodnocení informační bezpečnosti	31
2.3.3 Výsledky a udržování certifikace	33
2.3.4 Faktory ovlivňující proces implementace	33
2.4 PŘÍKLADY PROLOMENÍ INFORMAČNÍ BEZPEČNOSTI V AUTOMOBILOVÉM SEKTORU	34
3 MULTIKRITERIÁLNÍ HODNOCENÍ	37
3.1 METODY STANOVENÍ VAH	38
3.2 METODY MULTIKRITERIÁLNÍHO HODNOCENÍ.....	42
3.3 SOFTWARE NÁSTROJE VYUŽITELNÉ PŘI MULTIKRITERIÁLNÍ ANALÝZE	52
4 ANALÝZA RIZIK	60
4.1 LEGISLATIVA V OBLASTI ŘÍZENÍ RIZIK	61
4.1.1 ČSN ISO 31000 Management rizik	61
4.1.2 ČSN EN IEC 31010 - Management rizik – Techniky posuzování rizik	63
4.2 NEJPOUŽÍVANĚJŠÍ METODY ANALÝZY RIZIK	64
4.3 SOFTWARE NÁSTROJE VYUŽITELNÉ PŘI ANALÝZE RIZIK	71
II PRAKTICKÁ ČÁST	76
5 ZAVEDENÍ CERTIFIKACE TISAX	77
5.1 PŘEDSTAVENÍ SPOLEČNOSTI LISI AUTOMOTIVE FORM A.S.	77

6	METODIKA PRO ZPRACOVÁNÍ PROJEKTU	79
6.1	VÝCHODISKA METODIKY	79
6.2	OBSAH METODIKY	82
7	PROJEKT PŘÍPRAVY A IMPLEMENTACE CERTIFIKACE TISAX.....	85
7.1	DEFINE	85
7.1.1	Stanovení cílů a rozsahu projektu	85
7.1.2	Určení projektového týmu a zainteresovaných osob.....	86
7.1.3	SWOT analýza	87
7.2	MEASURE	88
7.2.1	Stanovení cílové úrovně TISAX	88
7.2.2	Stanovení vhodných ukazatelů KPI a PI	90
7.3	ANALYZE.....	92
7.3.1	Metodika Analýzy rizik.....	92
7.3.2	Analýza rizik TISAX.....	98
7.3.3	Vyhodnocení analýz rizik.....	100
7.4	IMPROVE.....	101
7.4.1	Návrh opatření.....	101
7.4.2	Metodika pro multikriteriální hodnocení	105
7.4.3	Výběr nejlepších variant nápravných opatření	108
7.4.4	Vyčíslení nákladů projektu.....	115
7.4.5	Implementace nápravných opatření.....	117
7.5	CONTROL.....	121
7.5.1	Vyhodnocení přínosu	121
7.5.2	Stabilizace nového stavu	122
7.5.3	Doporučení pro další rozvoj	124
	ZÁVĚR.....	126
	SEZNAM POUŽITÉ LITERATURY	127
	SEZNAM OBRÁZKŮ	133
	SEZNAM TABULEK.....	135
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	137
	SEZNAM PŘÍLOH.....	140

ÚVOD

V současném dynamickém a vysoce konkurenčním prostředí automobilového průmyslu, se informační bezpečnost stává klíčovým faktorem pro úspěch a udržitelnost podniků. S rostoucí digitalizací a globalizací dodavatelských řetězců se zvyšují i rizika spojená s únikem citlivých dat, což může mít závažné důsledky nejen pro samotné společnosti, ale i pro jejich obchodní partnery a zákazníky.

Pro představu, magazín Cybercrime předpokládá, že celosvětové roční náklady na porušení informační bezpečnosti a kybernetickou kriminalitu dosáhly v roce 2024 minimálně do výše 9,5 miliardy dolarů.[1]

V tomto kontextu nabývá na významu certifikace TISAX (Trusted Information Security Assessment), která byla vyvinuta, za účelem zajištění standardizované úrovně informační bezpečnosti zejména v automobilovém průmyslu. Certifikace poskytuje společností rámec pro hodnocení a zlepšování jejich bezpečnostních procesů, což je nezbytné pro ochranu citlivých informací a dat, jako jsou například: technické specifikace, obchodní strategie, osobní údaje, nebo výrobní postupy.

Toto téma diplomové práce jsem zvolil především z důvodů aktuálnosti a provázanosti s mým současným zaměstnáním v automobilovém průmyslu, kde již třetím rokem působím na pozici manažera, tudíž vývoj informační bezpečnosti a dopady na každodenní fungování řeším v praxi. V neposlední řadě, dle mého názoru plně vystihuje a naplňuje podstatu studia bezpečnostního managementu což je směr, kterým bych se v profesním životě chtěl dále ubírat.

Hlavním cílem této diplomové práce je vyhodnotit a analyzovat současný stav informační bezpečnosti v konkrétním podniku, v souvislosti se získáním certifikace TISAX a navrhnout s využitím vhodných metod analýzy rizik a multikriteriálního hodnocení optimální opatření, která povedou k úspěšnému splnění požadavků certifikace.

V teoretické části práce bude podrobně vysvětlena problematika týkající se informační bezpečnosti, konkrétně v prostředí automobilového průmyslu a taktéž východiska a kontext konceptu TISAX. Následně bude provedena analýza a popis nejpoužívanějších metod, které lze využít pro multikriteriální hodnocení a analýzu rizik, včetně dostupných softwarových nástrojů pro každou z těchto oblastí.

Praktická část si klade za cíl vypracovat pro konkrétní podnik metodiku, zaměřenou na získání již zmíněné certifikace. Jako hlavní struktura této metodiky bude využita metoda DMAIC, jenž poskytne osnovu celého projektu, zaměřeného na úspěšnou přípravu a získání certifikace. Při tvorbě autor vychází z praktických zkušeností a navazuje a rozvíjí poznatky které získal již při psaní své bakalářské práce.

Součástí jednotlivých etap projektu, bude vytvoření obecných metodik pro analýzu rizik a multikriteriální hodnocení v konkrétních softwarech. Na základě těchto metodik, bude provedena analýza rizik v konkrétním podniku a hodnocení nejlepších variant nápravných opatření tak, aby projekt zdárně dosáhl vytyčeného cíle.

I TEORETICKÁ ČÁST

1 CHARAKTERISTA PROBLEMATIKY

Cílem této první kapitoly, je uvést čtenáře do kontextu problematiky, související s hlavním cílem diplomové práce. Podkapitoly této první části, jsou základními stavebními kameny, na kterých je moderní koncept certifikace TISAX postaven.

1.1 Informační bezpečnost

V digitálním věku 21. století se informace staly komoditou. Jejich hodnota přesahuje hranice státních tajemství či firemních patentů – i zdánlivě nevinná data o našich každodenních návycích mohou mít velkou cenu. S každým kliknutím, každou návštěvou webové stránky zanecháváme digitální stopu. Firmy nás bombardují upozorněními o sběru cookies, ale kolik z nás si skutečně uvědomuje dosah těchto zdánlivě nevinných souborů? V době, kdy se naše životy stále více propojují s digitálním světem, se ochrana dat stává nikoli luxusem, ale nutností.[2]

Kořeny informační bezpečnosti sahají do 80. let minulého století, kdy se papírové kartotéky začaly měnit v digitální databáze. Náhle se obyčejné počítače staly pokladnicemi nevyčíslitelných hodnot. Banky, továrny i armády svěřily své nejcennější informace těmto elektronickým zařízením.[3]

Cílem není jen zabránit úniku dat, ale být připraven i na nejhorší scénář. Když už k průlomů dojde, je třeba jednat rychle což znamená minimalizovat škody, obnovit systémy a najít viníka. V digitálním světě může i drobná chyba způsobit lavinu problémů.[3]

Dnes už nestačí zamknout server do trezoru. Zabezpečení informačních systémů se podobá ochraně pevnosti – každá zeď, každá brána musí být neprůstřelná. Nejde jen o technická opatření; klíčovou roli hraje i lidský faktor. Bezpečnostní politika musí prostupovat celou organizací, od vrátného až po generálního ředitele.[2]

Komplexní přístup k bezpečnosti zahrnuje vše od správy hesel přes pravidelné zálohy až po sofistikovanou antivirovou ochranu. Každý systém je jedinečný a vyžaduje na míru šitá řešení. V éře cloudových služeb a internetu věcí se hranice mezi fyzickým a digitálním světem stírají, a s tím rostou i bezpečnostní výzvy.[2]

Informační bezpečnost není jen technický problém ale filozofie, která musí prostupovat celou společností. V době, kdy naše identity, finance i vzpomínky existují v podobě bitů a bajtů, je ochrana dat otázkou přežití v digitálním a dynamickém prostředí 21. století.[2]

1.1.1 Rozdíl mezi kybernetickou a informační bezpečností

V odborných kruzích panují rozdílné definice a názory na vztah mezi informační a kybernetickou bezpečností. Někteří experti považují kybernetickou bezpečnost za podmnožinu informační bezpečnosti, zatímco jiní zastávají opačný názor. Tato otázka zůstává předmětem odborné diskuse. Níže jsou uvedeny příklady definic obou pojmů.

Informační bezpečnost, je ochrana informací a dat před neoprávněným přístupem, použitím, zveřejněním, narušením, změnou nebo zničením bez ohledu na jejich formu (elektronickou, tištěnou, ústní).[2]

Kybernetická bezpečnost, představuje komplexní soubor opatření zahrnující právní rámce, organizační struktury, technické nástroje a vzdělávací programy. Tyto prostředky jsou zaměřeny na ochranu různých složek informačních a komunikačních technologií (ICT), včetně počítačových systémů, aplikací, dat a jejich uživatelů.[4]

Tabulka 1 Základní odlišnosti mezi informační a kybernetickou bezpečností

	Informační bezpečnost	Kybernetická bezpečnost
Hlavní zaměření	Ochrana integrity, důvěrnosti a dostupnosti informací	Ochrana digitálních systémů a infrastruktury před digitálními hrozbami
Rozsah	Širší pojem zahrnující všechny typy informací	Zaměřeno specificky na digitální prostředí a počítačové systémy
Klíčové aspekty	Řízení přístupu, šifrování, fyzická bezpečnost, školení uživatelů	Ochrana sítí, detekce hrozeb, incident response, penetrační testování
Příklady hrozeb	Modifikace dat, zneužití citlivých informací, neoprávněný přístup k hmotným i nehmotným hodnotám, únik citlivých informací, krádež výrobních postupů	Malware, ransomware, kyberterrorismus, podvodné nabídky sociální inženýrství, phishing, hacking, kybernetické výpalné

(zdroj:[4])

Toto srovnání ukazuje, že zatímco informační bezpečnost se zabývá ochranou informací v jakékoli formě, kybernetická bezpečnost se soustředí specificky na digitální prostředí a technologie. Obě oblasti jsou však klíčové pro komplexní ochranu dat a systémů v moderním podniku.

1.2 Triáda CIA (Confidentiality, Integrity, Availability)

Triáda CIA představuje základní model informační bezpečnosti, který definuje tři klíčové principy ochrany dat (důvěrnost, integrita a dostupnost). Tato v podstatě jednoduchá koncepce tvoří osu moderních bezpečnostních strategií. V rámci této ochrany pak není podstatné, na jakém typu nosiče (papír, elektronická média aj.) či v rámci jakého systému jsou informace zpracovávány. Informační bezpečnost je pak aplikována na informace po celý jejich životní cyklus.[4]

Základní model CIA je možné rozšířit i o další 3 prvky: Lidé, technologie a procesy

Lidé

- Příjemci pravidel: Osoby, které buď dobrovolně nebo z nutnosti implementují již stanovená pravidla informační bezpečnosti.
- Objekty ochrany: Subjekty, které je nezbytné chránit před různými formami útoků, ohrožující informační bezpečnost.
- Cílová skupina pro vzdělávání: Jedinci, kterým je třeba poskytnout informace a školení o zásadách a pravidlech kybernetické bezpečnosti.
- Potenciální rizikový faktor: V kontextu vytváření a udržování kybernetické bezpečnosti mohou lidé představovat riziko nebo hrozbu.[4]

Lidský prvek lze bez nadsázky považovat za stěžejní, zejména z důvodu, že lidé mají často tendenci chybovat, podlehnout nátlaku a prozatím, i když se situace s AI (Artificial intelligence) neustále vyvíjí, jsou lidé tím, kdo má stroje a technologie na povel a dokážou je ovládat.

Technologie

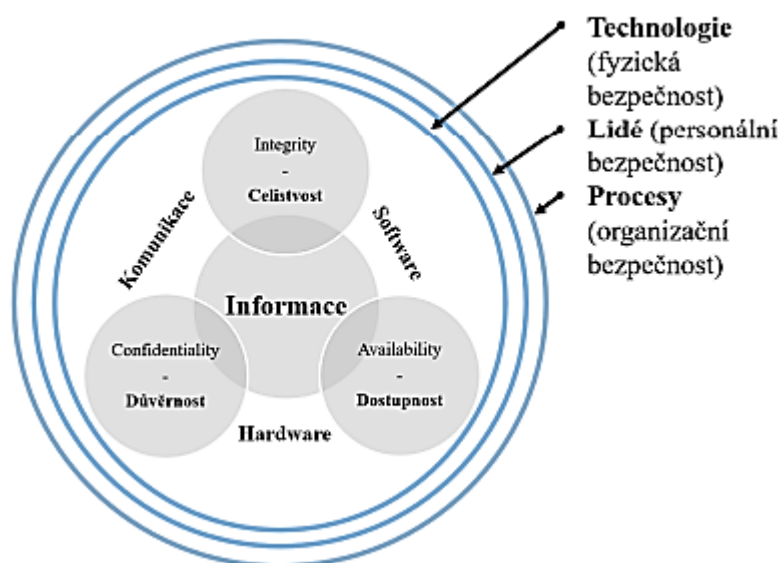
- Pokročilé monitorovací nástroje: Systémy pro detekci a prevenci průniků, které sledují síťový provoz a identifikují potenciální hrozby.
- Centralizované řízení: Jednotná správa uživatelských účtů a přístupových práv. Centrální systém pro klasifikaci a správu informací.
- Ochranné mechanismy: Vícevrstvá obrana proti škodlivému softwaru, zahrnující aplikační firewally, antivirové programy a antispamové filtry.

- Sledování aktivit: Sofistikované logovací systémy zaznamenávající činnosti všech prvků ICT infrastruktury, včetně aktivit administrátorů a běžných uživatelů.
- Zálohovací systémy: Kombinace aktivních a off-line zálohovacích systémů. Důraz na zálohování kritických serverů, aplikací a databází pro zajištění rychlé obnovy v případě incidentu.[4]

Procesy

- Hodnocení bezpečnosti: Pravidelné provádění auditů informační bezpečnosti pro identifikaci slabých míst a oblastí vyžadujících zlepšení.
- Krizové řízení: Implementace efektivních postupů pro rychlou a účinnou reakci na kybernetické útoky a další bezpečnostní incidenty.
- Zajištění kontinuity: Vytvoření a udržování procesů, které zajistí nepřerušovaný provoz kritických systémů i v případě bezpečnostních hrozeb.
- Rozvoj kompetencí: Organizace pravidelných školení a praktických cvičení pro zvýšení povědomí o kybernetické bezpečnosti a zlepšení schopností personálu reagovat na hrozby.[4]

Níže uvedený obrázek, převzatý z knihy CyberSecurity od Jana Koloucha, Pavla Bašty a kolektivu, znázorňuje rozšířený model CIA.[4]



Obrázek 1 Rozšířená triáda CIA

(zdroj:[4])

1.2.1 Důvěrnost (Confidentiality)

Důvěrnost je prvním z prvků triády CIA, který se zaměřuje na ochranu dat před neoprávněným přístupem. Tento aspekt zajišťuje, že k informacím mají přístup pouze autorizované osoby nebo systémy. Jinými slovy, jde o komplexní přístup k ochraně dat a informací, který kombinuje technická, organizační a lidská opatření s cílem minimalizovat riziko neoprávněného přístupu.[3]

Hlavní charakteristiky zahrnují:

Odstupňovanou ochranu

- Míra zabezpečení je přizpůsobena citlivosti dat, využívá se široká škála ochranných mechanismů, od fyzické kontroly přístupu až po sofistikované kryptografické metody.[2]

Klíčové komponenty

- Hodnocení kritičnosti a klasifikace informací, zajištění soukromí, izolace dat od neoprávněných osob a systémů, stanovení adekvátní úrovně zabezpečení.[2]

Klasifikace informací je rozdílná dle sféry využití, a vzhledem k zaměření této práce na komerční sféru se jedná o:

- Veřejné – informace dostupné široké veřejnosti, jejichž únik nebo neoprávněné nakládání s nimi, nebude mít jakýkoliv negativní dopad na společnost, například prezentace společnosti, nebo chystaných projektů.
- Interní – informace dostupné všem zaměstnancům organizace, neoprávněné nakládání s nimi, by mohlo sice mít potencionální dopad na společnost, ale nikoliv závažný, například interní oznámení zaměstnancům.
- Citlivé – informace dostupné pouze omezenému počtu zaměstnanců organizace, neoprávněné nakládání s nimi, by mohlo mít střední dopad na společnost, například informace o mzdách, výnosech projektů aj.
- Chráněné – informace dostupné vybraným zaměstnancům (většinou vrcholného managementu), neoprávněné nakládání s nimi by mohlo mít závažné dopady na fungování společnosti, například únik výrobních postupů, strategických plánů, údajů o zákaznících aj.[2]

Stupně důvěryhodnosti a určení vhodných způsobů pro likvidaci nosičů dat a informací jsou taktéž ustanoveny ve vyhlášce č. 82/2018 Sb. Jde o 4 stupně (nízká, střední, vysoká, kritická)[4]

1.2.2 Integrita (Integrity)

Integrita dat je druhým prvkem triády CIA, zajišťujícím důvěryhodnost a nezměnitelnost informací. Tento koncept je zásadní nejen pro ochranu dokumentů a databází, ale i pro ověření autenticity spustitelných souborů, čímž chrání uživatele před potenciálními hrozbami jako například malware. K zajištění integrity se využívají různé techniky, včetně hashovacích funkcí, blockchainových technologií a kontrolních součtů.[2]

Podle odborné definice je integrita charakterizována jako přesnost a úplnost dat, přičemž zahrnuje jejich platnost a konzistenci.[5]

V kontextu systémů, integrita znamená schopnost vykonávat zamýšlenou funkci bez nežádoucích zásahů. Celkově je integrita dat a systémů základním kamenem pro udržení bezpečnosti a spolehlivosti v digitálním prostředí, s významným dopadem na oblasti jako soudní spory či každodenní používání digitálních technologií.[3]

Taktéž u integrity jsou vyhláškou č. 82/2018 Sb., určeny stupně pro hodnocení integrity. Stejně jako u důvěrnosti jsou to 4 stupně (nízká, střední, vysoká a kritická).[4]

1.2.3 Dostupnost (Availability)

Dostupnost je nepostradatelným prvkem informační bezpečnosti, který zajišťuje, že uživatelé mají přístup k datům a systémům, kdykoliv to potřebují. Tento koncept jde daleko za pouhé zajištění přístupu v běžném provozu, zahrnuje i schopnost obnovit data po havárii nebo kybernetickém útoku. K dosažení vysoké dostupnosti je nezbytné implementovat řadu opatření, od pravidelného zálohování přes zajištění redundantní infrastruktury, až po sofistikovanou ochranu proti kybernetickým hrozbám.[2]

Klíčové je také minimalizovat prodlevy při přístupu k datům a zajistit jejich použitelnost. Bez spolehlivé dostupnosti, by i nejbezpečnější systém ztratil svou hodnotu. V kontextu informační bezpečnosti se narušení dostupnosti považuje za formu zničení informací, což podtrhuje její kritický význam v digitálním světě.[2]

Stejně jako u předchozích dvou prvků CIA, je i dostupnost hodnocena vyhláškou č. 82/2018 Sb., Stupně jsou totožné (nízká, střední, vysoká a kritická).[4]

1.3 Systém řízení informační bezpečnosti (ISMS)

V dnešní digitální éře, kdy informace představují klíčové aktivum každé organizace, nabývá na významu jejich efektivní ochrana. Právě zde je klíčový Systém řízení informační bezpečnosti, známý pod zkratkou ISMS (Information Security Management System).

Tento komplexní přístup k zabezpečení dat a informací se stal nepostradatelným nástrojem pro podniky všech velikostí a odvětví. Lze ho chápat jako soubor pravidel, postupů a technických opatření, které organizace zavádí s cílem chránit své informační zdroje. Nejde však o jednorázové řešení, ale o kontinuální proces, který vyžaduje neustálou pozornost a aktualizaci.[22]

Základním pilířem je důkladná analýza rizik (této problematice, bude věnována samostatná kapitola v třetí části této práce). Ta pomáhá identifikovat potenciální hrozby a zranitelnosti, které by mohly ohrozit bezpečnost informací. Na základě této analýzy se pak navrhuje a implementují vhodná bezpečnostní opatření. Tato opatření mohou zahrnovat širokou škálu aktivit – od zavedení bezpečnostních politik a školení zaměstnanců až po nasazení sofistikovaných technických řešení.[2]

Klíčovým aspektem konceptu ISMS je jeho cyklická povaha. Využívá se zde princip známý jako PDCA (Plan-Do-Check-Act) cyklus, který zajišťuje neustálé zlepšování bezpečnostních procesů. Tento přístup umožňuje organizacím pružně reagovat na měnící se bezpečnostní hrozby a nové technologické výzvy.[6]

Zdárná implementace přináší organizacím řadu výhod. Kromě zvýšené ochrany citlivých dat to může být i lepší pověst u zákazníků a obchodních partnerů, snížení nákladů spojených s bezpečnostními incidenty, či snadnější dodržování legislativních požadavků.[2]

Je třeba zdůraznit, že ISMS není jen záležitostí IT (Information Technology) oddělení. Aby byl skutečně účinný, musí se stát součástí firemní kultury a být podporován na všech úrovních organizace, od řadových zaměstnanců až po top management. V době, kdy kybernetické hrozby nabývají na sofistikovanosti a četnosti, představuje ISMS účinný nástroj, jak těmto výzvám čelit. Organizace, které dokážou tento systém efektivně implementovat a udržovat, získávají významnou konkurenční výhodu v podobě robustní ochrany svých informačních aktiv.[22]

1.3.1 Cyklus PDCA (Plan-Do-Control-Act)

Implementace systému řízení informační bezpečnosti, se v organizaci se typicky opírá o normu ISO/IEC 27001, která je považována za základní standard v oblasti správy bezpečnosti informací. Pro efektivní zavedení ISMS je vhodné postupovat podle metodiky založené právě na cyklu PDCA.[6]

Samotný cyklus, se opírá principy vědeckého přístupu k řešení problémů (formulace hypotézy, testování a vyhodnocení výsledků) a představuje systematický způsob implementace opatření. Po zavedení, se vyhodnocuje jejich dopad a pokud se prokáže jejich účinnost, proces se standardizuje a následně opakuje. Tento cyklus je základním kamenem pro kontinuální zlepšování procesů a klíčovým prvkem štihlého managementu (strategie řízení procesů, která klade důraz na maximální efektivitu a produktivitu při současném minimalizování plýtvání zdroji).[6]

Relativně jednoduchá struktura cyklu umožňuje rychlé opakování jednotlivých fází. Během těchto opakování se stav zkoumaného systému postupně mění s cílem dosáhnout požadovaného výsledku. Výhodou postupného zlepšování jsou minimalizované náklady, nízké riziko ztrát způsobených chybnými kroky a trvalý posun směrem k lepším výsledkům a trvalému zlepšení procesu.[6]

Popis jednotlivých kroků cyklu:

1. **Plánuj (Plan):** První fáze zahrnuje hloubkovou analýzu rizik, stanovení rozsahu platnosti ISMS, definování bezpečnostní politiky a výběr odpovídajících kontrolních mechanismů. Důraz je kladen na pochopení informačních aktiv, určení potenciálních hrozeb a stanovení cílů, kterých má být dosaženo.[7]
2. **Dělej (Do):** Druhá fáze, kdy dochází k praktickému zavedení technických a organizačních kontrolních opatření. Zahrnuje to také vzdělávání zaměstnanců v oblasti informační bezpečnosti a vytváření dokumentace, která podrobně popisuje procesy a zásady.[7]
3. **Kontroluj (Check):** Třetí fáze je zaměřena na neustálé sledování a hodnocení účinnosti zavedených opatření. Důležitou součástí je provádění interních auditů, které ověřují soulad ISMS s definovanými standardy a cíli.[7]

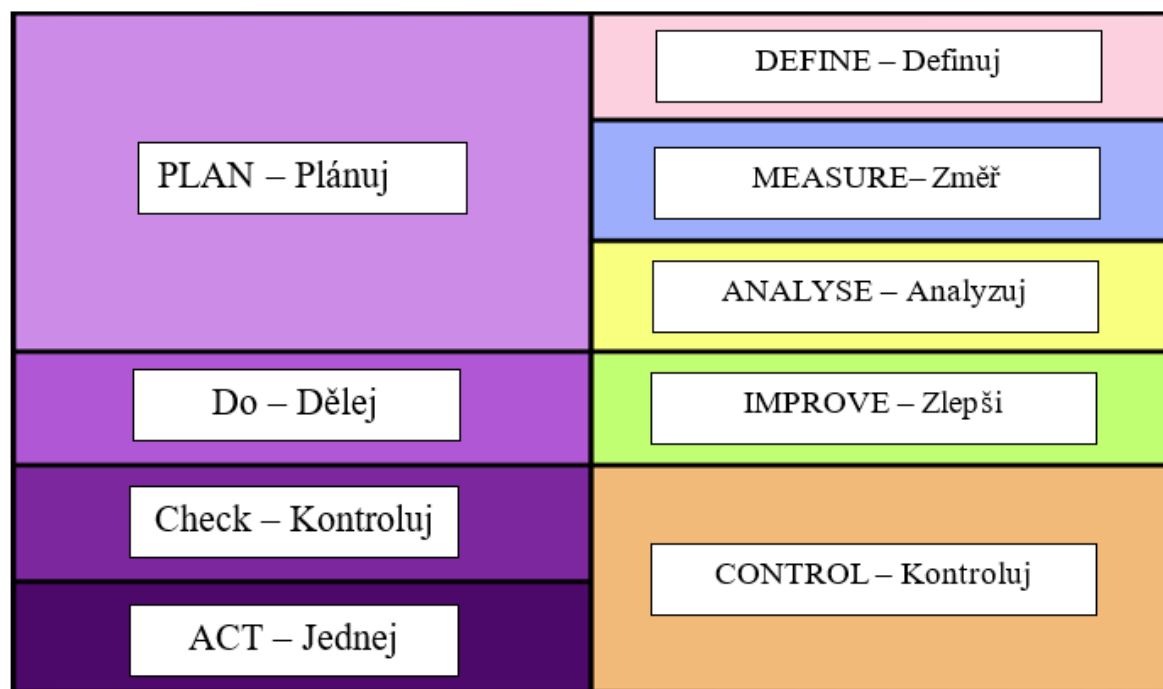
4. **Jednej (Act):** V této závěrečné fázi se identifikují a řeší nedostatky zjištěné během kontrol. Na základě získaných poznatků se provádějí úpravy a vylepšení systému, aby lépe reagoval na nové hrozby a změny v organizaci.[7]

1.3.2 Metoda DMAIC

Metoda je nedílnou součástí metodologie Lean Six Sigma, která je postavena na datově řízeném a strukturovaném přístupu k řešení problémů a byla autorem využita již při psaní bakalářské práce, která může poskytnout teoretická východiska této problematiky.[55]

Tento cyklus slouží ke kontinuálnímu zlepšování stávajících procesů, a to prostřednictvím jasně definovaných fází, které umožňují identifikovat příčiny neefektivnosti, problémů a chyb, navrhnout a implementovat opatření ke zlepšení a následně udržovat dosažené výsledky.[6]

V zásadě využívá stejného principu, jako cyklus PDCA, je ale robustnější a klade velký důraz na počáteční fázi projektu, kdy prvotní fáze PLAN, je rozčleněna na 3 dílčí fáze (DEFINE, MEASURE, ANALYZE). Díky tomu poskytuje hlubší analýzu a používá se při řešení složitějších problémů a rozsáhlejších projektů. Rozdíl mezi metodami je znázorněn na obrázku 2.[6]



Obrázek 2 Komparace metod PDCA a DMAIC

(zdroj:[64])

2 CERTIFIKACE TISAX

Jak již bylo zmíněno na začátku této práce, tak TISAX představuje standard pro hodnocení a zabezpečení informační bezpečnosti, který byl navržen specificky pro automobilový průmysl. Mimo označení „certifikace“ se setkáváme i označením program, nicméně podstata je stejná. Vznikl zejména jako odpověď, na rostoucí potřebu standardizované, efektivní a důvěryhodné metody hodnocení informační bezpečnosti v automobilovém průmyslu.[9]

První vznik je datován v roce 2017, pod záštitou asociace VDA (Verband der Automobilindustrie), která předstává německou asociaci automobilového průmyslu. V roce 2000 se přidala další, nová asociace evropských výrobců automobilů ENX (European Network Exchange), jenž mimo jiné působí jako neutrální, řídicí a eskalační orgán pro certifikaci TISAX.[9]

VDA vytvořila katalog ISA (Information Security Assessment), který tvoří základní rámec pro celý program a ENX schvaluje poskytovatele auditorských služeb a monitoruje kvalitu provedení a výsledky certifikace.[10]



Obrázek 3 Oficiální logo certifikace

(zdroj:[8])

Automobilový průmysl je charakterizován složitými dodavatelskými řetězci, kde různé subjekty sdílejí citlivé informace. Tato spolupráce zvyšuje riziko úniků dat a kybernetických hrozeb, což vyžaduje efektivní metody ochrany. S rostoucími obavami o ochranu osobních údajů a bezpečnost informací, se objevily i regulační požadavky, které nutily firmy k implementaci robustních systémů řízení bezpečnosti informací. Tyto dva faktory, byly klíčové pro vznik TISAXU.[9]

2.1 Hlavní cíle

TISAX má několik klíčových cílů, které přispívají k jeho významu v automobilovém sektoru. Obecně lze tyto cíle popsat v těchto konkrétních bodech.

Standardizace bezpečnostních požadavků

- Poskytovat standardizovaný rámec pro hodnocení informační bezpečnosti specificky navržený pro automobilový sektor. Před jeho zavedením existovaly různorodé požadavky od výrobců automobilů, což bylo pro dodavatele náročné a neefektivní.[9]
- Struktura standardu: základ katalog VDA ISA a postupy z normy ISO/IEC 27001. Normě ISO IEC 27001 bude věnována samostatná kapitola, proto v této části nebude dále rozváděna.[10]
- Rozlišuje tři úrovně hodnocení I až III, podle požadované úrovně ochrany. Úrovně ochrany jsou označeny jako AL (Assessment Level).[9]

Efektivita a úspora nákladů

- Přinést subjektům úspory zejména v oblasti administrativy a nákladů spojených s audity, zejména díky propojení a vzájemnému uznávání výsledků auditů. Společnostem tak stačí získat certifikaci jednou a nemusí tedy podstupovat opakované hodnocení pro každého nového partnera, nebo zákazníka.[9]
- Recertifikační audity probíhají v 3letém intervalu.[10]

Řízení rizik v dodavatelském řetězci

- Je nezbytné zavést komplexní systém ISMS. Tento systém vychází z osvědčené normy ISO/IEC 27001, ale je speciálně upraven tak, aby odpovídal jedinečným požadavkům automobilového sektoru. Díky tomu zajišťuje, že bezpečnostní opatření jsou nejen robustní, ale také relevantní pro specifická rizika a procesy typické pro automobilový průmysl.[10]
- Klíčové oblasti: Identifikace a zmírnění rizik spojených s informační bezpečností, implementaci postupů pro řízení kybernetických rizik, vytvoření reakčních plánů na bezpečnostní incidenty.[9]

Ochrana citlivých informací

- Ochrana citlivých informací představuje zásadní pilíř v automobilovém průmyslu. Tento aspekt nabývá na důležitosti s rostoucí digitalizací a propojením v rámci odvětví. Standardizovaný rámec pro hodnocení informační bezpečnosti kladе značný důraz na zabezpečení širokého spektra citlivých dat. [9]
- Příklady chráněných informací: Osobní údaje zaměstnanců a zákazníků, duševní vlastnictví. Obchodně citlivé informace, smluvní informace, výrobní postupy, technická dokumentace a informace týkající se prototypů, nebo jejich částí. [9]
- Již zde byli zmíněny úrovně ochrany AL. Každá úroveň je navržena tak, aby odpovídala různým potřebám organizací v závislosti na citlivosti zpracovávaných informací a požadované úrovni bezpečnosti. Níže uvedená tabulka je shrnuje a rozvádí o charakteristiky a specifické požadavky.[9]

Tabulka 2 Charakteristiky a specifické požadavky úrovní ochrany

Úroveň	Charakteristika	Specifické požadavky
AL I (základní úroveň)	Organizace zpracovávající běžné obchodní informace. Nízká úroveň důvěryhodnosti výsledků. Primárně pro interní účely organizace.	Sebehodnocení organizace, bez externího auditu.
AL 2 (střední úroveň)	Organizace pracující s citlivými informacemi, jako je duševní vlastnictví. Poskytuje vyšší úroveň jistoty pro partnery a zákazníky.	Externí audit, ověření dokumentace a implementace bezpečnostních opatření.
AL 3 (vysoká úroveň)	Organizace nakládající s vysoce citlivými informacemi, např. prototypy. Nejprísnější úroveň hodnocení. Poskytuje nejvyšší úroveň jistoty v dodavatelském řetězci.	Komplexní externí audit, důkazy o efektivní implementaci bezpečnostních opatření.

(zdroj:[10])

Reakce na rostoucí kybernetické hrozby

- Automobilový průmysl čelí stále složitějším kybernetickým hrozbám, které jsou důsledkem rostoucí digitalizace a propojení vozidel. Moderní automobily jsou dnes v podstatě počítače na kolech, vybavené složitými elektronickými systémy a připojené k internetu. Tato technologická vyspělost sice přináší řadu výhod pro řidiče, ale zároveň otevírá nové cesty pro potenciální útočníky. Výrobci automobilů a jejich dodavatelé proto musí neustále zdokonalovat své bezpečnostní strategie. To zahrnuje implementaci pokročilých technologií pro detekci a prevenci útoků, pravidelné bezpečnostní audity a školení zaměstnanců. Zároveň je klíčová spolupráce napříč odvětvím při sdílení informací týkající se aktuálních a budoucích hrozeb a osvědčených postupů, jak na tyto hrozby reagovat.[9]
- Základní technikou je proces neustálého zlepšování CI (Continuous Improvement), s využitím pravidelných auditů a recertifikací, sdílením prověřených a otestovaných postupů a zkušeností a podpory inovací v oblasti bezpečnosti a ochrany dat.[11]
- Úspěšná implementace TISAX zvyšuje nejen informační bezpečnost v automobilovém průmyslu, ale vytváří a udržuje mechanismus, pro systematickou a koordinovanou reakci na kybernetické hrozby v rámci celého automobilového odvětví.[11]

Tabulka 3 Příklady kybernetických hrozeb a nápravných opatření

Kybernetická hrozba	Příklad opatření v rámci TISAX
Neoprávněný přístup k citlivým datům	Implementace systému řízení přístupu, pravidelné přezkoumávání a monitorování přístupů, více faktorová autentizace.
Únik citlivých informací	Klasifikace a ochrana dat, šifrování citlivých dat v klidu i při přenosu, školení zaměstnanců o bezpečném zacházení s informacemi.
Rizika spojená s dodavatelským řetězcem	Hodnocení a řízení bezpečnostních rizik dodavatelů a partnerů, implementace bezpečnostních opatření v dodavatelském řetězci.

Malware a ransomware	Implementace technických obran proti hrozbám, pravidelné aktualizace a patche systémů, školení zaměstnanců o rozpoznávání a prevenci malwaru.
Fyzické bezpečnostní hrozby	Implementace fyzických bezpečnostních opatření, ochrana zařízení a prostor před neoprávněným přístupem.
Ztráta nebo krádež zařízení	Šifrování dat na přenosných zařízeních, implementace možnosti vzdáleného vymazání dat.
Sociální inženýrství	Školení zaměstnanců o rozpoznávání phishingových útoků, implementace technických kontrol pro filtrování podezřelých e-mailů.
Útoky na propojená vozidla	Implementace pokročilých technologií detekce hrozeb, kontinuální monitorování systémů propojených vozidel.

(zdroj:[12])

Podpora inovací a konkurenceschopnosti

- Společnosti, které přijaly tento bezpečnostní standard, získávají významnou konkurenční výhodu. Certifikace je vnímána jako známka důvěryhodnosti a otevírá dveře k novým partnerstvím v globálním měřítku. Demonstruje totiž závazek k nejvyšším standardům ochrany dat, což je v dnešní digitální éře klíčové pro budování důvěry mezi partnery i zákazníky. Tento přístup k informační bezpečnosti tak nejen zvyšuje odolnost odvětví vůči kybernetickým hrozbám, ale také vytváří prostředí, které podporuje rychlejší inovace a posiluje pozici certifikovaných firem na světovém trhu. V důsledku toho se stává hnací silou technologického pokroku a konkurenceschopnosti v automobilovém sektoru.[11]
- Lze tvrdit, že TISAX působí v roli katalyzátoru inovací v automobilovém průmyslu tím, že stanovuje jasné směrnice pro bezpečný vývoj produktů, podporuje integraci pokročilých bezpečnostních opatření a umožňuje firmám soustředit se na inovace místo řešení různorodých bezpečnostních požadavků.[11]

Soulad s regulačními požadavky

- Obecné regulační požadavky v rámci standardu pro hodnocení informační bezpečnosti v automobilovém průmyslu představují komplexní přístup k ochraně dat a systémů. Tento standard, vycházející z mezinárodně uznávané normy ISO/IEC 27001 a vyžaduje implementaci robustního systému řízení informační bezpečnosti. Pokrývá širokou škálu oblastí od správy a dohledu nad bezpečností informací, přes ochranu osobních údajů, až po technickou obranu proti hrozbám. Důraz je kladen na pravidelné hodnocení a aktualizaci bezpečnostních opatření, přičemž certifikace je platná po dobu tří let. Přestože standard vychází z obecných principů, je přizpůsoben specifickým potřebám automobilového průmyslu, včetně dodatečných požadavků na ochranu prototypů. Tímto přístupem pomáhá organizacím nejen splnit regulační požadavky, ale také zvýšit jejich důvěryhodnost a konkurenceschopnost v odvětví. [9]

2.2 ISO/IEC 27001

Norma ISO/IEC 27001 je klíčovým standardem v oblasti informační bezpečnosti a taky jeden ze základních pilířů TISAXU. Spolu s normou ISO/IEC 27002 tvoří ucelený systém pro řízení bezpečnosti informací. Tato norma, vyvinutá společně mezinárodní organizací pro normalizaci (ISO) a mezinárodní elektrotechnickou komisí (IEC), prošla technickou revizí a aktualizací, přičemž nejnovější verze harmonizuje strukturu s ostatními normami systému managementu. Aktualizace zohledňuje i ISO/IEC 27002:2022.[13]

Tento dokument stanovuje kritéria pro vytvoření, implementaci, údržbu a kontinuální zdokonalování systému řízení informační bezpečnosti v kontextu dané organizace. Zahrnuje také postupy pro hodnocení a zmírňování bezpečnostních rizik, které jsou přizpůsobitelné individuálním potřebám každé organizace.[14]

Uvedené požadavky jsou formulovány tak, aby byly aplikovatelné na všechny typy organizací, nezávisle na jejich zaměření, rozsahu nebo charakteru činnosti. Pokud organizace deklaruje soulad s tímto dokumentem, musí splnit všechny požadavky uvedené v kapitolách 4 až 10, bez výjimky.[13]

ISO/IEC 2700, je uspořádána do dvou částí. První část zahrnuje sérii ustanovení, z nichž ustanovení 4-10 jsou závazné pro organizace, usilující o soulad s touto normou. Následující tabulka, popisuje jednotlivé sekce první části a klíčové body, kterých se týkají. [13]

Tabulka 4 Popis ustanovení první části u normy ISO/IEC 27001

Číslo	Název ustanovení	Klíčové body
1	Předmět normy	Specifikace požadavků na ISMS, posuzování a ošetření rizik, obecné použití pro všechny organizace
2	Citované dokumenty	Odkazuje se na normu ISO/IEC 27000, konkrétně v oblastech termínů a definic
3	Termíny a definice	Platí termíny a definice podle ISO/IEC 27000
4	Kontext organizace	Porozumění organizaci a jejímu kontextu, porozumění potřebám zainteresovaných stran, stanovení rozsahu ISMS, systém managementu informační bezpečnosti
5	Vůdčí role	Vůdčí role a závazek, politika, role, odpovědnosti a pravomoci
6	Plánování	Činnosti zaměřené na rizika a příležitosti, cíle informační bezpečnosti a plánování jejich dosažení
7	Podpora	Zdroje, kompetence, povědomí, komunikace dokumentované informace
8	Provozování	Plánování a řízení provozu, posuzování rizik informační bezpečnosti, ošetření rizik informační bezpečnosti
9	Hodnocení výkonnosti	Monitorování, měření a analýza hodnocení, interní audit, přezkoumání vedením
10	Zlepšování	Neustálé zlepšování, Neshody a nápravné opatření

(zdroj:[13])

Druhá část (dodatek), obsahuje celkem 93 bezpečnostních opatření, kdy tato opatření jsou rozdělena do 4 kategorií, které poskytují komplexní rámec pro řízení informační bezpečnosti. Ty mohou organizace přizpůsobit svým specifickým potřebám a rizikům. Dodatek

není zamýšlen jako povinný kontrolní seznam, ale jako vodítko pro implementaci. Dělení jednotlivých kategorií a příkladů, je shrnuto v následující tabulce.[13]

Tabulka 5 Shrnutí kategorií obsažených v dodatku, včetně příkladů opatření

Kategorie	Počet	Příklady opatření
Organizační opatření	37	Politika organizace, řízení rizik, řízení dodavatelů
Personální opatření	8	Prověřování zaměstnanců, bezpečnostní školení, disciplinární proces
Fyzická opatření	14	Zabezpečení perimetru, kontrola vstupu, ochrana proti fyzickým hrozbám
Technologická opatření	34	Řízení přístupu, kryptografie, zálohování dat

(zdroj:[13])

2.2.1 Rozdíl mezi ISO/IEC 27001 a certifikací TISAX

Na základě poskytnutých informací, by se mohl zdát, že TISAX je prakticky stejný jako norma ISO/IEC 27001, v obou případech jde o standard zaměřený na informační bezpečnost, nicméně oba k této problematice přistupují jinak. Klíčový rozdíl je v zaměření. kdy norma ISO /IEC 27001 je určena pro všechny typy organizací rozličných velikostí, oproti tomu se TISAX zaměřuje na automobilový průmysl, výrobní sféru a dodavatelský řetězec.[15]

Tabulka 6 Rozdíly mezi normou ISO/IEC 27001 a TISAXEM

Oblast	ISO/IEC 27001	TISAX
Certifikační proces	Formální certifikační proces prováděný akreditovanými certifikačními orgány	Hodnocení prováděné schválenými auditory ENX, výsledkem je označení TISAX
Platnost	Certifikát platný 3 roky s ročními dohledovými audity	Označení platné 3 roky bez ročních přezkoumání
Sdílení výsledků	Žádná centrální databáze certifikátů	Výsledky hodnocení jsou uloženy v centrální databázi ENX a mohou být sdíleny s partnery

(zdroj:[15])

2.3 Průběh certifikace

Následující kapitola detailně pojednává o jednotlivých fázích certifikačního procesu, včetně kritických aspektů přípravy, auditu a následného udržování certifikace. Tento proces, vyžadovaný německou asociací VDA slouží k ověření souladu systémů řízení bezpečnosti informací s požadavky specifickými pro dodavatele v automobilovém sektoru.[17]

Průběh lze rozdělit do tří hlavních fází: příprava a registrace, hodnocení a výměny výsledků, které jsou dále členěny na dílčí kroky. Každá etapa vyžaduje aktivní spolupráci mezi certifikovanou organizací, poskytovatelem auditu a platformou ENX, která celý proces koordinuje.[17]

2.3.1 Přípravná fáze a registrace

Před zahájením formálního procesu certifikace musí organizace provést interní analýzu připravenosti. Tato fáze zahrnuje definici rozsahu certifikace v souladu s požadavky obchodních partnerů a identifikaci úrovně zabezpečení (AL1–AL3) odpovídající citlivosti zpracovávaných dat. Například, společnosti pracující s utajovanými prototypy vozidel obvykle volí úroveň AL3, která vyžaduje komplexní „on-site“ audit. Tento typ auditu se provádí fyzickou přítomností auditora v prostorách certifikované organizace a zahrnuje přímou interakci s procesy, infrastrukturou a personálem.[10]

Registrace na portálu ENX představuje první formalizovaný krok. Organizace zde uvádí základní údaje o své struktuře, lokalitě podléhajících certifikaci a požadovaném rozsahu hodnocení. Poplatek za registraci činí 405 EUR za každou lokalitu, přičemž platforma ENX umožňuje hromadné registrace pro snížení nákladů. Výstupem této fáze je takzvaný „Scope Excerpt“ – dokument specifikující parametry budoucího auditu.[10]

2.3.2 Hodnocení informační bezpečnosti

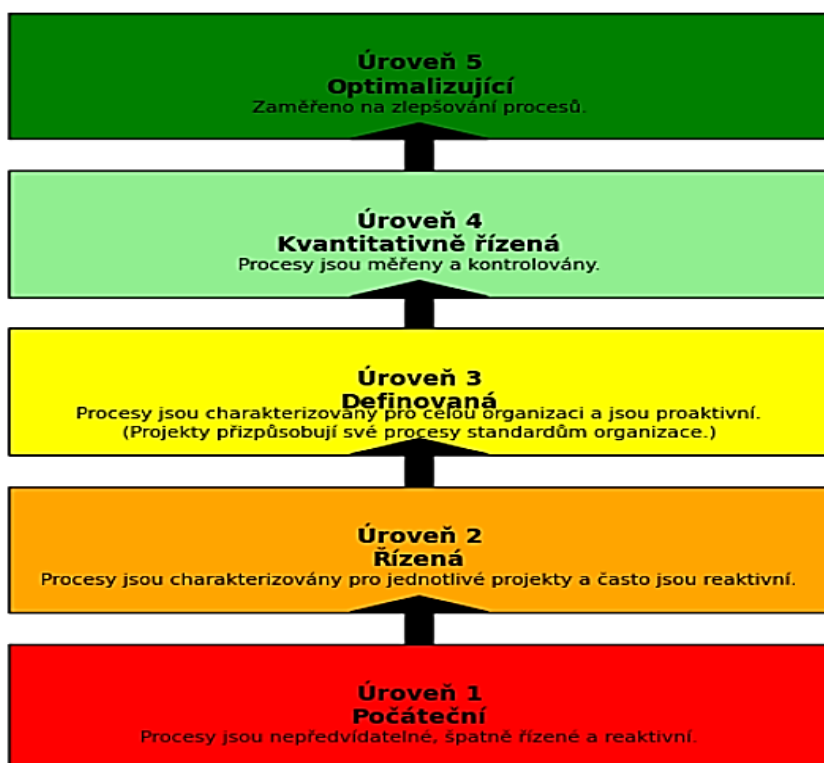
Prvním krokem hodnocení je vyplnění dotazníku VDA ISA, který porovnává stávající bezpečnostní opatření proti požadavkům TISAXU. Hlavním přínosem tohoto kroku, bývá odhalení odhalí mezer, které organizace řeší implementací dodatečných kontrol, jako je šifrování dat nebo revize přístupových práv. Dle doporučení konzultačních firem, je optimální provést tuto analýzu s předstihem 6–12 měsíců před plánovaným auditem.[17]

Organizace si volí akreditovaného auditora TISAX ze seznamu schválených subjektů. Kritériem výběru bývá odborná specializace (např. znalost cloudových technologií) a geografická dostupnost. Díky interaktivnímu portálu na oficiálním portálu ENX stačí, aby žadatel zadal polohu a portál mu automaticky nabídne možné auditory. Pro Českou republiku se jedná zejména o společnosti Bureau Veritas, KPMG, nebo TÜV NORD.[16]

Externí audit probíhá ve dvou variantách dle úrovně zabezpečení:

- **AL2:** Dokumentární revize bez fyzické přítomnosti auditora (doložení požadované dokumentace na dálku)
- **AL3:** Komplexní „on-site“ s fyzickou přítomností auditora [16]

Auditoři hodnotí vyspělost ISMS, například s využitím modelu zralosti CMM (Capability Maturity Model), pro úspěšné absolvování se vyžaduje minimálně třetí úroveň (definovaný proces). Průběžné zjištěné nedostatky řeší organizace formou akčních plánů, zaměřených na problematické oblasti. Akční plány musí být realizovány před vydáním závěrečné zprávy. Úrovně znalosti modelu CMM, jsou znázorněny na následujícím obrázku.[10]



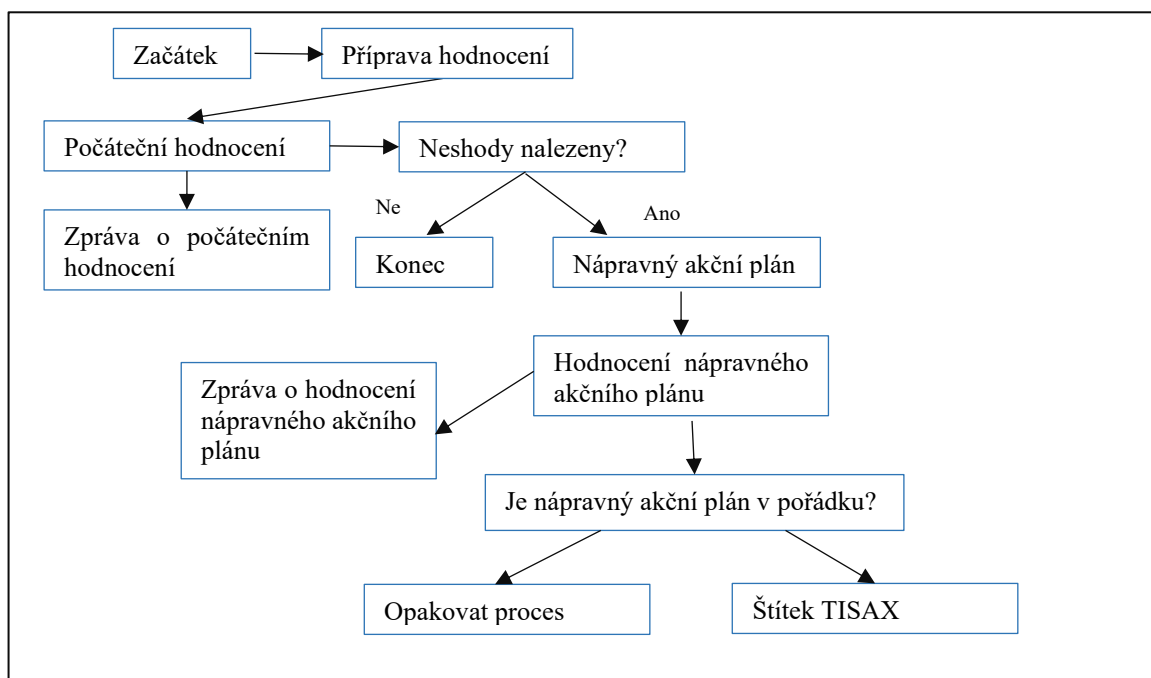
Obrázek 4 Popis jednotlivých úrovní modelu CMM

(zdroj:[6])

2.3.3 Výsledky a udržování certifikace

Po úspěšném auditu nahraje poskytovatel zprávu o hodnocení na portál ENX, kde je přístupná autorizovaným obchodním partnerům. Certifikát TISAX má platnost tří let. Velké automobilky OEM (Original Equipment Manufacturer), mohou během tříleté platnosti certifikátu požadovat dodatečné kontroly u svých dodavatelů v případě, pokud u nich dojde k významným organizačním změnám. Děje se tak z důvodu oprávněného zájmu, na zajištění bezpečnosti informací v celém svém dodavatelském řetězci.[10]

Prodloužení certifikace vyžaduje opakování celého procesu s aktualizovanou dokumentací, reflektující změny v technologiích nebo obchodních procesech. Některé společnosti kombinují TISAX s certifikací ISO/IEC 27001, čímž snižují administrativní zátěž při obou auditech. Shrnutí celého procesu je ztvárněno na následujícím diagramu. [10]



Obrázek 5 Proces implementace

(zdroj:[10])

2.3.4 Faktory ovlivňující proces implementace

Implementace představuje komplexní proces, který může mít významný dopad na fungování organizace. Při zavádění nového systému je třeba vzít v úvahu několik klíčových faktorů, které mohou ovlivnit úspěšnost celého projektu.

Jednou z nejčastějších překážek jsou finanční náklady spojené s celým procesem. Certifikační proces zahrnuje výdaje na externí audity, které mohou být zejména pro menší organizace velkou zátěží. Kromě toho organizace často musí investovat do nových technologií a bezpečnostních opatření, aby splnily požadavky. Tyto investice mohou zahrnovat nákup softwaru pro řízení informační bezpečnosti, nebo fyzických zabezpečovacích systémů.[22]

Další výzvou může být odpor ke změnám ze strany zaměstnanců. Zavádění nových procesů a systémů může vyvolat obavy, zejména pokud se jedná o nové bezpečnostní politiky nebo postupy. Firemní kultura může být neochotná přijmout změny, což může vést k frustraci a odporu vůči novým požadavkům.[22]

Nedostatek odbornosti v oblasti informační bezpečnosti je dalším faktorem, který může komplikovat proces certifikace. Mnoho organizací nemá interní odborníky, proto se často musí spoléhat na externí poradce nebo auditorské společnosti, což zvyšuje náklady a ztěžuje řízení celého procesu certifikace.[22]

Složitost certifikačního procesu může být také překážkou. Požadavky jsou podrobné a zahrnují různé aspekty informační bezpečnosti, což vyžaduje pečlivou analýzu systémů a procesů organizace. Délka procesu certifikace může trvat několik měsíců až let, což může být pro některé firmy frustrující a ovlivnit jejich obchodní operace.[22]

2.4 Příklady prolomení informační bezpečnosti v automobilovém sektoru

Cílem této kapitoly je přiblížit reálné dopady, které může narušení informační bezpečnosti přinést. Při shánění podkladů byla provedena rešerše a průzkum nejvíce medializovaných příkladů.

Renault 2017

Incident z května 2017, kdy ransomware „WannaCry“ paralyzoval globální IT infrastrukturu, zůstává varovným příkladem. Tato vlna digitálního vydírání tehdy zasáhla přes 200 tisíc zařízení napříč 150 státy, přičemž mezi nejpostiženější subjekty patřil francouzský automobilový výrobce Renault. V důsledku rozsáhlé infekce systémů, musela společnost okamžitě přerušit provoz ve výrobních halách ve Francii a Rumunsku, což vedlo k výpadkům v dodávkách komponentů pro celý evropský trh.[18]

Volkswagen 2022

Během únorové kampaně v roce 2022, cílili kyberzločinci na severoamerické pobočky koncernu Volkswagen Group, konkrétně na divize Audi a Volkswagen. Útok překvapil rozsahem úniku dat. Na veřejnost se dostaly citlivé informace včetně kontaktních údajů, čísel řidičských průkazů a finančních transakcí u 3,3 milionu zákazníků a potenciálních klientů v USA a Kanadě. Analýza bezpečnostních expertů odhalila, že útočníci využili kombinace phishingových emailů a zneužití neaktualizovaných síťových služeb k průniku do interních systémů organizace.[18]

Ferrari 2023

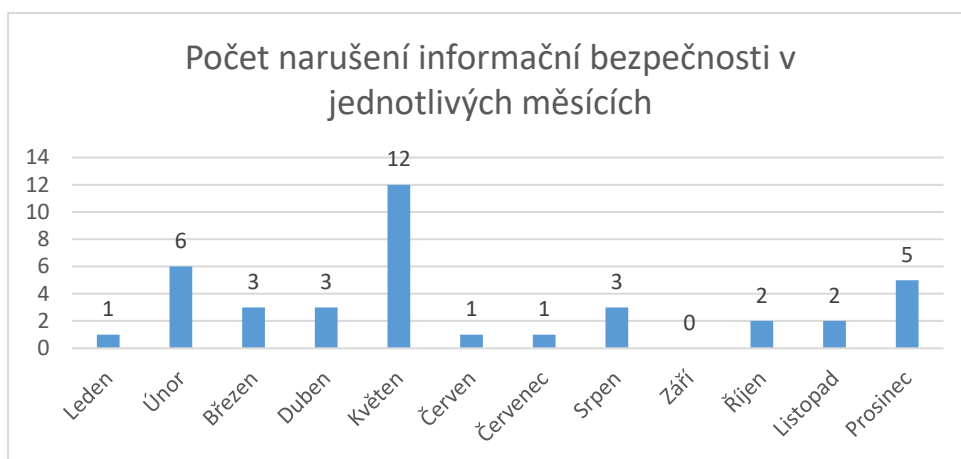
Italská automobilka proslulá výrobou luxusních sportovních vozů, čelila v roce 2023 závažnému kybernetickému napadení typu ransomware, jež vedlo k úniku citlivých informací majitelů jejich vozů. V reakci na extrémní požadavky neznámých útočníků společnost ve spolupráci s předními světovými experty na digitální bezpečnost okamžitě aktivovala krizový tým a současně informovala příslušné státní instituce. Tento incident navazuje na předchozí bezpečnostní problémy společnosti, kdy došlo k rozsáhlému úniku firemních dokumentů včetně technických specifikací a servisních manuálů. Podle investigativních zpráv médií, stál za touto událostí hackerský kolektiv „RansomEXX“, který zveřejnil na platformě darknet přes 7 GB dat, obsahujících důvěrné informace o klientech.[18][19]

Volkswagen 2024

V roce 2024 zasáhl koncern Volkswagen rozsáhlý bezpečnostní incident, při němž došlo k neoprávněnému přístupu k datům 800 000 majitelů elektromobilů napříč evropskými značkami skupiny včetně Audi, Škody a Seat. Ztráta ochrany informací vznikla vinou chybného nastavení cloudové infrastruktury provozované softwarovou divizí Cariad, která využívala úložné služby Amazon Web Services. Tato technologická nedbalost, umožnila externím subjektům po dobu několika měsíců sledovat pohybová data vozidel s přesností na metry a získávat osobní údaje řidičů, jako byly telefonní kontakty nebo domácí adresy. Interní audit Volkswagen Group následně identifikoval chybějící šifrování datových toků a nedostatečnou segmentaci přístupových práv jako hlavní příčiny průniku. Vedení koncernu avizovalo navýšení investic do zabezpečení „connected car“ technologií o 40 % pro rok 2025 s cílem obnovit důvěru zákazníků.[20]

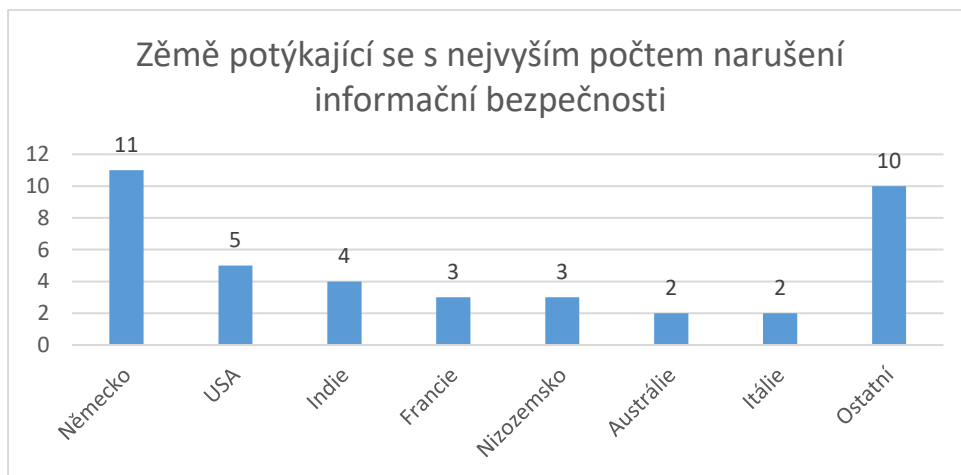
Přehled za kalendářní rok

V období, kdy tato diplomová práce vznikala, nebyla při rešerši nalezena logická a ucelená studie, která by byla zaměřena na rok 2024. Proto pro lepší představu o případech narušení informační bezpečnosti (dále již jen IB) byla využita studie z roku 2023, na jejímž základě byly z toho plynoucí výsledky zpracovány v následujících grafech.



Obrázek 6 Analýza měsíců, kdy došlo k nejvíce narušením IB

(zdroj:[21])



Obrázek 7 Analýza zemí, kde došlo k nejvyššímu počtu narušení IB

(zdroj:[21])

Z výsledků analýzy vyplývá, že nejkritičtější byl měsíc květen a z pohledu zemí největšímu tlaku čelí Německo. U jednotlivých zemí lze předpokládat, že tento trend bude pokračovat, z důvodu provázanosti německé ekonomiky s automobilovým sektorem, zejména koncernem Volkswagen.[21]

3 MULTIKRITERIÁLNÍ HODNOCENÍ

Třetí kapitola se věnuje problematice multikriteriálního hodnocení, které bude využito při praktické části diplomové práce. První část je zaměřena na základní pojmy, které s touto problematikou souvisí, následně budou popsány vybrané metody multikriteriálního hodnocení a provedena analýza v současnosti dostupných softwarových nástrojů, které lze využít.

Multikriteriálního hodnocení má interdisciplinární charakter, který zahrnuje matematiku, management, informatiku, psychologii, sociální vědy a ekonomii. Samotné uplatnění je široké, neboť jednotlivé metody, lze použít k řešení jakéhokoli problému, kde je třeba učinit významné rozhodnutí. Tato rozhodnutí mohou být buď taktická, nebo strategická, v závislosti na časové perspektivě důsledků řešení.[33]

Varianta

Varianty představují možná řešení rozhodovacího problému, mezi kterými volíme na základě posouzení podle souboru zvolených kritérií. V procesu multikriteriálního rozhodování jsou zvláště významné dva koncepty variant, které vymezují rozhodovací prostor. Ideální varianta reprezentuje hypotetické nebo v některých případech reálné řešení, které dosahuje nejlepších možných hodnot ve všech stanovených kritériích současně. Bazální varianta je protikladem ideální varianty a reprezentuje hypotetické nebo reálné řešení, které dosahuje nejhorších možných hodnot u všech stanovených kritériích současně.[33]

Kritérium

Kritérium představuje hledisko nebo měřítko, podle kterého hodnotíme jednotlivé rozhodovací varianty. Jde o klíčový prvek každého vícekritériálního rozhodovacího procesu, neboť právě kritéria určují rámec, v němž posuzujeme kvalitu a vhodnost jednotlivých variant. Kritéria dělíme na maximalizační, tj. taková u níž je preferována vyšší hodnota před nižší a minimalizační, kde je preferována nižší hodnota před vyšší.[33]

Váha kritéria:

Jedná se o číselné vyjádření relativní významnosti kritéria ve srovnání s ostatními kritérii použitými při hodnocení variant. Čím větší význam je kritériu přikládán, tím vyšší musí být jeho váha. Váhy jsou stanoveny subjektivně, nebo pomocí speciálních metod, které budou popsány v následující kapitole. Je nezbytné vyjádřit váhy v normované podobě tak, aby jejich celkový součet byl roven 1, přičemž normované váhy jsou v intervalu 0 až 1.[33]

Rozhodovatel

Tento expert, nese odpovědnost za finální selekci nejlepší varianty z dostupných alternativ. Význam jeho postavení spočívá především v tom, že obohacuje formální analytické postupy o nepostradatelný prvek expertního posouzení a praktických zkušeností. Zatímco matematické metody poskytují strukturovaný rámec analýzy, právě rozhodovatel vnáší do procesu kvalifikovaný úsudek, který je pro dosažení kvalitního rozhodnutí nenahraditelný.[33]

3.1 Metody stanovení vah

Tyto metody poskytují odrazové můstky a techniky pro nalezení kompromisního řešení. Vyznačují se tím, že do středu rozhodovacího procesu staví samotného rozhodovatele. Nejedná se o automatické metody, které by vedly ke stejnému řešení pro každého rozhodovatele, ale jsou to metody, které zahrnují subjektivní informace.[34]

Metody přímého stanovení vah kritérií

Metody přímého stanovení vah kritérií jsou jednoduché subjektivních metody, používaných při multikriteriálním hodnocení. Vyžadují od rozhodovatele přímé vyjádření významnosti kritérií bez nutnosti vzájemného srovnávání. Jsou vhodné pro situace s menším počtem kritérií nebo při časových omezeních.[34]

Bodovací metoda

1. Nejprve rozhodovatel vytvoří bodovací škálu v předem stanoveném intervalu
2. Následně subjektivně přiřazuje body jednotlivým kritériím, podle vytvořené bodovací stupnice. Toto hodnocení je založeno čistě na jeho vlastním úsudku a zkušenostech.
3. Posledním krokem je výpočet vah. Váha V se pro každé kritérium vypočítá podle níže uvedeného vzorce, kde k je počet bodů přidělených danému kritériu a n , je celkový součet bodů přidělených všem kritériím.[34]

$$V_{1,...,n} = \frac{k}{\sum n}$$

Tabulka 7 Ukázka postupu bodovací metody

Počet bodů	Vyjádření	Kritéria	Body (k)	Váhy (V)
1	Nejhorší	Kritérium 1	3	0,20

2	Špatné	Kritérium 2	4	0,27
3	Dobré	Kritérium 3	5	0,33
4	Výborné	Kritérium 4	2	0,13
5	Nejlepší	Kritérium 5	1	0,07
		Suma $\sum n$	15	1,00

(zdroj:[32])

Metoda pořadí

1. Prvním krokem je seřazení kritérií do pořadí. Nejdůležitějšímu kritériu se přiřadí hodnota rovná počtu kritérií (k). Každému dalšímu méně důležitému kritériu se přiřadí o jednotku nižší hodnota.
2. Výše zmíněný vztah je pro lepší přehlednost vyjádřen pomocným sloupcem „obrácené pořadí“.
3. Posledním krokem je výpočet vah. Váha V se pro každé kritérium vypočítá podle níže uvedeného vzorce, kde k je hodnota obráceného pořadí kritéria a n je suma hodnot všech kritérií.[34]

$$V_{1,...,n} = \frac{k}{\sum n}$$

Tabulka 8 Ukázka postupu metody pořadí

Kritéria	Pořadí	Obrácené pořadí	Váhy V
Kritérium 1	3	3	0,20
Kritérium 2	2	4	0,27
Kritérium 3	1	5	0,33
Kritérium 4	4	2	0,13
Kritérium 5	5	1	0,07
Suma $\sum n$		15	1,00

(zdroj:[32])

Metody párového porovnání

Metody párového porovnání, se zaměřují na srovnávání kritérií nebo alternativ ve dvojicích. Oproti přímým metodám, kde se váhy či body přidělují kritériím bezprostředně, párové porovnání nabízí detailnější diferenciaci preferencí, což může vést k vyšší přesnosti, především u komplexnějších rozhodovacích problémů s více kritérii.[34]

Fullerova metoda

1. Prvním krokem je sestavení Fullerova trojúhelníku. V tomto schématu, jsou kritéria uspořádána tak, že každá dvojice kritérií se vyskytuje pouze jedenkrát. Trojúhelník má vždy $k-1$ dvojřádků, kde k je počet kritérií.
2. Rozhodovatel, následně postupně porovnává každou dvojici kritérií, kdy z každé dvojice vybírá to kritérium, které považuje za důležitější. Preferované kritérium se zapíše do trojúhelníkové struktury.
3. Pro každé kritérium se sečte počet jeho označení (preferencí).
4. Posledním krokem je výpočet vah, kde k_i je nenormovaná váha i -tého kritéria a $\sum k_i$ je suma hodnot nenormovaných vah kritérií.[34]

$$v_i = \frac{k_i}{\sum_{i=1}^n k_i}$$

Tabulka 9 Ukázka postupu Fullerovi metody

Kritéria	K 1	K 2	K 3	K 4	K 5	Počet preferencí	Obrácené pořadí	Nenormované váhy	Normované váhy
Kritérium 1		2	3	1	1	2	3	4	0,27
Kritérium 2			3	2	2	3	2	3	0,20
Kritérium 3				3	3	4	1	5	0,33
Kritérium 4					4	1	4	2	0,13
Kritérium 5						0	5	1	0,07
Suma $\sum k_i$								15	1,00

(zdroj:[32])

Saatyho metoda

1. Konstrukce Saatyho matice: Vytvoří se čtvercová matice, kde řádky i sloupce reprezentují porovnávaná kritéria.
2. Párové porovnání: Každá dvojice kritérií se porovná a ohodnotí pomocí Saatyho bodové stupnice (1-9), kde 1 znamená rovnocennost a 9 absolutní preferenci. Preferované kritérium má celou hodnotu, nepreferované hodnotu zlomku čísla.
3. Následuje výpočet vah, kde G_i je hodnota geometrického průměru daného kritéria a $\sum G_i$ je suma hodnot geometrických průměrů kritérií.[34]

$$v_i = \frac{G_i}{\sum_{i=1}^n G_i}$$

Tabulka 10 Ukázka postupu Saatyho metody

Kritéria	K1	K2	K3	K4	K5	Geometrický průměr G_i	Normované váhy v_i
Kritérium 1	1	1/3	1/5	3	5	1,00	0,13
Kritérium 2	3	1	1/3	5	7	2,04	0,26
Kritérium 3	5	3	1	7	9	3,94	0,51
Kritérium 4	1/3	1/5	1/7	1	3	0,49	0,06
Kritérium 5	1/5	1/7	1/9	1/3	1	0,25	0,03
Suma $\sum k_i$						7,72	1,00

(zdroj:[32])

Každá z uvedených metod stanovení vah je využitelná při jiné situaci. Následující tabulka znázorňuje shrnutí výhod a nevýhod.

Tabulka 11 Výhody a nevýhody konkrétních metod pro stanovení vah

Metoda	Výhody	Nevýhody
Bodovací metoda	Jednoduchost, výpočetní nenáročnost na typ informací.	Riziko nadhodnocení kritérií při rozhodování jednoduchých problémů
Metoda pořadí	Časová nenáročnost.	Riziko zkreslení výsledků z důvodu subjektivního stanovování pořadí
Fullerova metoda	Jednoduchost při hodnocení kvantitativních kritérií s dosažením výborných výsledků.	Větší časová náročnost daná větším množstvím výpočtů
Saatyho metoda	Detailnější a jemnější rozlišení bodovací škály.	Větší časová náročnost daná specifiky této metody

(zdroj:[32])

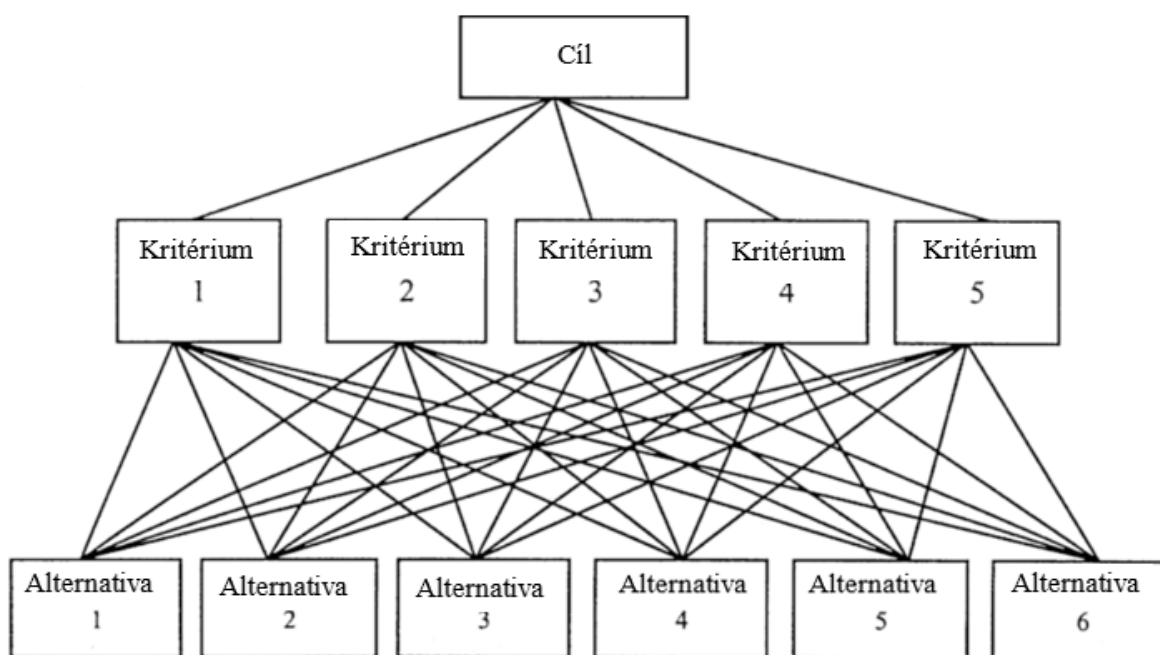
3.2 Metody multikriteriálního hodnocení

Metoda AHP (Analyticko-hierarchický proces)

Metoda byla vyvinuta Thomas L. Saaty. Umožňuje strukturovat složité rozhodovací problémy do hierarchického modelu, kde jsou jednotlivé úrovně tvořeny cílem, kritérii a alternativami. Tato metoda je založena na párovém srovnávání prvků, při kterém rozhodovatel určuje jejich relativní významnost pomocí devítibodové Saatyho škály. Výsledkem je výpočet vah kritérií a dílčích hodnocení alternativ, které jsou následně syntetizovány do celkového hodnocení.[34]

Obecný postup metody AHP:

1. Rozhodovací problém je rozdělen na úrovně, přičemž první úroveň představuje cíl, prostřední úrovně kritéria (případně sub kritéria) a poslední úroveň alternativy.
2. Kritéria i alternativy jsou párově porovnávány vzhledem k nadřazeným prvkům. Intenzita preferencí je určována pomocí Saatyho škály.
3. Váhy kritérií a hodnocení alternativ jsou odvozeny z vlastního vektoru příslušného maximálnímu vlastnímu číslu Saatyho matice nebo pomocí geometrického průměru řádků.
4. Celkové hodnocení alternativ se vypočítá jako vážený průměr dílčích hodnocení vzhledem k jednotlivým kritériím.[34]



Obrázek 8 Ukázka struktury AHP

(zdroj:[35])

PROMETHEE (Preference Ranking Organization Method for Enrichment Evaluation)

Metoda PROMETHEE byla vyvinuta profesory Jean-Pierre Brans a Bertrandem Mareschalem v počátku 80. let 20. století. První verze, PROMETHEE I a PROMETHEE II, byly představeny v roce 1982 na konferenci v Québecu. Později byla metoda rozšířena o další verze, jako jsou PROMETHEE III, IV, V a VI. Shrnutí použití jednotlivých typů je v následující tabulce.[34]

Tabulka 12 Typy metody PROMETHEE

Typ	Použití
PROMETHEE I	Pro částečné řazení alternativ na základě jednoho kritéria. Je užitečná pro identifikaci alternativ, které jsou jednoznačně lepší nebo horší než ostatní.
PROMETHEE II	Pro úplné řazení alternativ na základě více kritérií. Poskytuje kompletní pořadí alternativ, což je užitečné pro výběr nejlepší alternativy.
PROMETHEE III	Pro řazení založené na intervalech. Je vhodná pro situace, kdy hodnocení alternativ není přesné, nebo je vyjádřeno v intervalech.
PROMETHEE IV	Pro kontinuální sadu řešení. Je užitečná pro problémy, kde existuje kontinuum možných řešení.

PROMETHEE V	Pro problémy s omezeními segmentace. Je vhodná pro výběr více alternativ podléhajících určitým omezením
PROMETHEE VI	Pro reprezentaci lidského mozku. Je specifickou verzí, zaměřenou na simulaci rozhodování lidského mozku.
GAIA	Geometrická analýza pro interaktivní podporu, která poskytuje grafické znázornění a pomáhá při analýze stability pořadí

(zdroj:[34])

Základní princip metody PROMETHEE spočívá v párovém srovnání alternativ na základě více kritérií. Metoda používá preferenční funkce a váhy kritérií k vyhodnocení preference jedné alternativy nad druhou.[36]

Obecný postup metody PROMETHEE

1. Definice kritérií a alternativ: Identifikujeme relevantní kritéria, která budou použita pro hodnocení alternativ. Tato kritéria mohou zahrnovat ekonomické, environmentální, sociální nebo technické aspekty.
2. Přidělení vah kritériím: Každému kritériu jsou přiděleny váhy, podle jeho relativní důležitosti. Tyto váhy musí být normalizovány tak, aby jejich součet byl roven 1.
3. Výpočet preferenčních funkcí: Je zvolen vhodný typ preferenční funkce pro každé kritérium. Preference funkce kvantifikují preference jedné alternativy nad druhou na základě každého kritéria. Existuje několik typů preferenčních funkcí, jako je lineární, V – tvarová, nebo Gaussova. Dalším krokem je definice prahů lhostejnosti a preference pro každé kritérium, které pomáhají určit, kdy je rozdíl mezi dvěma alternativami zanedbatelný nebo významný.
4. Párové srovnání a výpočet jedno-kritériálních toků: Párové srovnání určuje, zda je jedna alternativa preferována nad druhou na základě daného kritéria a jedno-kritériální toky reprezentují, jak je jedna alternativa preferována nad ostatními na základě jednoho kritéria.
5. Výpočet globálních toků: Globální toky zahrnují celkovou preferenci jedné alternativy nad ostatními na základě všech kritérií. Rozlišujeme pozitivní tok (reprezentuje, jak je alternativa preferována nad ostatními), Negativní tok (reprezentuje, jak jsou ostatní alternativy preferovány nad danou alternativou) a čistý tok (jde o rozdíl mezi pozitivním a negativním tokem, který poskytuje finální pořadí alternativ).

6. Interpretace výsledků: Alternativa s nejvyšším čistým tokem je obecně považována za nejlepší volbu. Posledním krokem je provedení citlivostní analýzy, která ověřuje stabilitu pořadí v případě změny váhy kritéria nebo preferenční funkce.[36]

ELECTRE (Elimination Et Choix Traduisant la Realité)

Metoda byla vyvinuta v polovině 60. let 20. století Bernardem Royem, jako reakce na potřebu řešit komplexní rozhodovací problémy, kde tradiční metody váženého součtu nebyly dostatečně efektivní. Vyznačuje se zejména schopností porovnávat alternativy na základě variace kritérií, přičemž bere v úvahu preference a důležitost kritérií stanovených rozhodovatelem. Metoda ELECTRE je založena na principu takzvaných „outranking“ relací (převahy), které umožňují přímé porovnání alternativ podle definovaných kritérií.[34]

Základním prvkem metody, je tedy konstrukce relací mezi všemi páry alternativ na základě dvou hlavních testů. Prvním, je test konkordance, který ověřuje, zda skupina kritérií podporující hypotézu (alternativa A je alespoň stejně dobrá jako alternativa B) je dostatečně silná. Druhým je test diskordance, který ověřuje, zda neexistuje žádné kritérium, ve kterém by alternativa B byla výrazně lepší než alternativa A, což by tuto hypotézu anulovalo.[37]

Podobně, jako u metody PROMETHEE, existuje několik typů, které se liší použitím dle typu řešeného problému. Shrnutí je v následující tabulce.

Tabulka 13 Typy metody ELECTRE

Typ	Použití
ELECTRE I	Pro výběr nejlepší varianty, vhodný pro selekční problémy.
ELECTRE II	Pro určení pořadí alternativ, rozšíření ELECTRE I o detailnější řazení.
ELECTRE III	Pro určení pořadí alternativ, vhodný pro složité problémy s vysokou mírou neurčitosti.
ELECTRE IV	Pro určení pořadí alternativ, bez vah kritérií. Nepoužívá explicitní váhy kritérií.
ELECTRE TRI	Pro třídění alternativ do kategorií (klasifikační problémy).

(zdroj:[34])

Obecný postup metody ELECTRE

1. Definice problému a identifikace alternativ: Prvním krokem je definice rozhodovacího problému, určení cíle rozhodování a identifikace množiny možných alternativ.
2. Stanovení množiny hodnotících kritérií: Rozhodovatel určí kritéria, na základě kterých, budou jednotlivé varianty vzájemně srovnávány. Tato kritéria mohou mít jak kvantitativní, tak kvalitativní charakter a měla by odpovídat řešenému problému.
3. Sestavení a normalizace rozhodovací matice: Sestaví se kritériální matice, ve které jsou jednotlivé alternativy uspořádány do řádků a kritéria do sloupců. Každý prvek této matice představuje hodnocení určité alternativy vzhledem k příslušnému kritériu. Pro zajištění porovnatelnosti hodnot, se provádí normalizace, přičemž obvykle je využívána metoda vektorové normalizace.
4. Určení vah a prahových hodnot jednotlivých kritérií: Každému kritériu jsou přiřazeny váhy podle jejich důležitosti pro rozhodovatele. Dále mohou být definovány prahové hodnoty preference, indiference a práva veta, které určují citlivost rozhodovatele vůči rozdílům mezi alternativami.
5. Výpočet konkordanční matice: Pro každou dvojici alternativ se stanoví konkordanční index, který určuje, do jaké míry lze podpořit tvrzení, že jedna alternativa je přinejmenším stejně vhodná jako druhá. Tento index se získá součtem vah těch kritérií, u kterých jedna alternativa vykazuje lepší výsledky než alternativa druhá.
6. Výpočet diskordanční matice: Diskordanční index představuje míru nesouhlasu s tvrzením, že jedna alternativa převyšuje druhou. Jeho výpočet vychází z největšího rozdílu v hodnocení alternativ podle jednotlivých kritérií, který překračuje předem určené prahové hodnoty.
7. Konstrukce matice kredibility: Kombinací konkordančních a diskordančních indexů se sestaví matice kredibility („outrankingová“ matice), která určuje výslednou relaci převahy mezi jednotlivými alternativami. Tato matice obsahuje informace o tom, zda jedna alternativa dostatečně „převyšuje“ jinou.
8. Využití matice kredibility k finálnímu pořadí nebo třídění alternativ: V závislosti na typu použité metody může být výsledkem: výběr nejlepší alternativy (ELECTRE I), pořadí všech alternativ od nejlepší po nejhorší (ELECTRE II, III), nebo rozdělení alternativ do kategorií (ELECTRE TRI).[37]

PAPRIKA (Potentially All Pairwise RanKings of all possible Alternatives)

Metoda PAPRIKA byla vyvinuta novozélandskými vědci, Paulem Hansenem a Franzem Omblérem, kteří jsou zároveň zakladateli společnosti 1000minds, která nabízí softwarový produkt, založený právě na této metodě. Vznikla jako odpověď na potřebu efektivnějších a uživatelsky přívětivějších přístupů k multikriteriálním rozhodovacím problémům, které by současně poskytovaly robustní teoretické základy. Metoda se specificky zaměřuje na hodnotové modely s kategoriemi výkonnosti (diskrétní hodnota nebo kategorie která vyjadřuje, jak dobře daná alternativa splňuje určité kritérium). Na rozdíl od tradičnějších metod, které často vyžadují složité matematické operace nebo abstraktní hodnocení kritérií, přináší inovativní přístup založený na jednoduchých párových srovnáních, která jsou pro rozhodovatele intuitivnější a kognitivně méně náročná.[29]

V aplikacích multikriteriálního hodnocení, je metoda PAPRIKA využívána rozhodovateli k určení vah kritérií pro dané rozhodnutí, které reprezentují jejich relativní důležitost. Tyto váhy jsou následně použity k seřazení, prioritizaci nebo výběru mezi alternativami. Rozhodovatel je tak postaven před sérii jednoduchých otázek, založených na výběru mezi dvěma hypotetickými alternativami, definovanými vždy pouze na dvou kritériích nebo attributech.[34]

Obecný postup metody PAPRIKA

1. Identifikace kritérií a jejich úrovní: Prvním krokem je definování relevantních kritérií pro daný rozhodovací problém a stanovení možných úrovní výkonnosti pro každé kritérium. Tato fáze je zásadní, protože kvalita konečného rozhodnutí závisí na vhodném výběru kritérií, která komplexně pokrývají všechny důležité aspekty problému.
2. Párová srovnání s kompromisy: Jádrem metody tvoří série otázek založených na volbě mezi dvěma hypotetickými alternativami. Rozhodovatel je systematicky dotazován na své preference, které se liší pouze ve dvou kritériích. V jednom kritériu je lepší první alternativa, v druhém kritériu je lepší druhá alternativa.
3. Iterativní proces a minimalizace počtu otázek: Otázky jsou postupně opakovány s různými páry hypotetických alternativ, definovaných na různých kombinacích kritérií pro danou aplikaci, dokud nejsou preference rozhodovatele dostatečně zachyceny. Díky sofistikovanému algoritmu, není nutné provádět všechna možná párová srovnání, což významně snižuje časovou náročnost celého procesu.

4. Odvození vah kritérií: Na základě odpovědí rozhodovatele na párová srovnání, jsou matematicky odvozeny váhy jednotlivých kritérií. Tyto váhy reprezentují relativní důležitost, kterou rozhodovatel přikládá jednotlivým kritériím a jsou použity k hodnocení a seřazení alternativ v aditivním modelu (model vyznačující se tím, že celkovou hodnotu alternativy reprezentuje součet dílčích hodnot, které jsou přiřazeny jednotlivým kritériím).[29]

TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution)

Metoda TOPSIS byla vyvinuta americkým vědcem Ching-Lai Hwangem v roce 1981. Postupem času byla neustále rozvíjena, až se stala jednou z nejpoužívanějších metod multikritériálního rozhodování napříč různými obory, což vedlo k dalšímu systematickému rozvoji její metodologie. Řadí se mezi tzv. kompenzační metody, které umožňují vzájemné vyvažování kritérií. To znamená, že špatný výsledek v jednom kritériu, může být vykompenzován dobrým výsledkem v jiném kritériu. Tento přístup poskytuje realističtější formu modelování než nekompenzační metody, které zahrnují nebo vylučují alternativní řešení na základě pevně stanovených limitů.[38]

Základní princip spočívá v myšlence, že optimální alternativa by měla mít nejkratší geometrickou vzdálenost od pozitivního ideálního řešení (PIS) a zároveň nejdelší geometrickou vzdálenost od negativního ideálního řešení (NIS). Pozitivní ideální řešení představuje hypotetickou alternativu, která dosahuje nejlepších hodnot ve všech kritériích, zatímco negativní ideální řešení reprezentuje hypotetickou alternativu s nejhoršími možnými hodnotami kritérií.[38]

Obecný postup metody TOPSIS

1. Vytvoření rozhodovací matice: V prvním kroku se sestavuje rozhodovací matice, která obsahuje m alternativ a n kritérií. Průsečík každé alternativy a kritéria představuje konkrétní hodnotu kritéria pro danou alternativu.
2. Normalizace rozhodovací matice: Na základě vytvořené matice je provedena normalizace za účelem sjednocení měrných jednotek různých kritérií.
3. Výpočet vážené normalizované rozhodovací matice: Ve třetím kroku se vytváří vážená normalizovaná rozhodovací matice, kde každá hodnota je násobena příslušnou váhou kritéria.

4. Určení ideálního a bazálního řešení: Ideální alternativa obsahuje nejlepší hodnoty každého kritéria, zatímco bazální alternativa obsahuje nejhorší hodnoty.
5. Výpočet vzdáleností od ideálního a bazálního řešení.
6. Výpočet relativní blízkosti k ideálnímu řešení.
7. Seřazení alternativ dle preferenčního pořadí: V posledním kroku jsou alternativy seřazeny sestupně podle hodnoty koeficientu, od nejlepší po nejméně vhodnou.[38]

SAW (Simple Additive Weighting)

Metoda váženého součtu představuje jeden z nejstarších a nejintuitivnějších přístupů k multi-kriteriálnímu rozhodování. Ačkoliv přesné datum jejího vzniku není v literatuře jednoznačně uvedeno, metoda se začala formálně používat v rámci rozhodovací teorie v polovině 20. století jako součást rozvoje operačního výzkumu a systémové analýzy. V praxi se můžeme setkat s několika názvy: „Weighted Sum Model“ (WSM), „Simple Additive Weighting“ (SAW), nebo „Weighted Linear Combination“ (WLC).[45]

Díky své jednoduchosti a srozumitelnosti se metoda stala oblíbenou v mnoha oblastech rozhodování, včetně ekonomiky, managementu, inženýrství a environmentálních studií. Její rozšíření bylo podpořeno i rychlým vývojem výpočetní techniky, která umožnila snadnější zpracování komplexnějších rozhodovacích problémů. Její hlavní princip spočívá v lineární agregaci hodnot kritérií vážených jejich relativní důležitostí. Důležitým předpokladem pro správnou aplikaci metody WSM je, že všechna data musí být vyjádřena ve stejných jednotkách. V případě, že kritéria mají různé jednotky, je nutné před aplikací metody provést normalizaci hodnot.[45]

Obecný postup metody SAW

1. Definování rozhodovacího problému: Identifikace alternativ, které mají být hodnoceny, stanovení kritérií použitých při hodnocení a určení relativních vah důležitosti jednotlivých kritérií.
2. Vytvoření rozhodovací matice: Vytvoří se matice, kde řádky představují alternativy a sloupce představují kritéria. Každý prvek tak matice reprezentuje výkonnost alternativy podle určitého kritéria.
3. Normalizace kritérií:

4. Stanovení vah kritérií: K stanovení vah kritérií se běžně využívá Saatyho metoda, která se opírá o porovnávání významnosti kritérií v párech. Je nezbytné, aby tyto váhy byly normalizovány takovým způsobem, že jejich celkový součet je roven hodnotě 1.
5. Výpočet celkového skóre pro každou alternativu: Vypočítá se takzvané „WSM-score“ pro každou alternativu, které je zohledňuje vážený součet všech kritériálních hodnot.
6. Seřazení alternativ a výběr nejlepší varianty: Alternativy se seřadí podle jejich celkového skóre. V případě maximalizačního problému je nejlepší alternativou ta s nejvyšším skóre.
7. Analýza citlivosti: Proveďte se analýza citlivosti pro ověření, jak by se změnilo pořadí alternativ při změně vah nebo výkonnostních hodnot.[45]

MACBETH (Measuring Attractiveness by a Categorical Based Evaluation Technique)

Metoda byla vyvinuta v 90. letech 20. století týmem Carlose A. Bana a Costy, v akademickém prostředí London School of Economics, v reakci na potřebu řešit komplexní rozhodovací problémy s více kritérii, které nelze adekvátně kvantifikovat tradičními metodami. Teoretické základy vycházejí z teorie užitečnosti a aditivních hodnotových modelů. Klíčovým předpokladem je možnost reprezentovat preferenční vztahy pomocí intervalových škál, které zachovávají ordinální i kardinální vlastnosti soudů.[34]

Na rozdíl od AHP, která využívá párová srovnání na základě poměrových škál. MACBETH pracuje se sedmi sémantickými kategoriemi, popisujícími rozdíl atraktivity (žádný, velmi slabý, slabý, střední, silný, velmi silný, extrémní). Tato kvalitativní východiska umožňují rozhodovateli soustředit se na relativní rozdíly mezi možnostmi, nikoli na absolutní čísla, což zvyšuje validitu výsledků.[34]

Obecný postup metody MACBETH:

1. Strukturování problému: Definice hodnotového stromu s kritérii a subkritérii.
2. Konstrukce hodnotových funkcí: Probíhá prostřednictvím párových srovnání možností v každém kritériu.
3. Kontrola konzistence soudů: ověřuje se, zda zadané soudy respektují ordinální uspořádání a splňují podmínky kardinální konzistence (například pokud rozdíl A-B je "silný" a B-C je "střední", pak rozdíl A-C musí být alespoň "silný").

4. Přiřazení vah kritériím: Určení relativní důležitosti kritérií.
5. Agregace: Výpočet celkového hodnocení alternativ.
6. Analýza citlivosti a robustnosti: Testování stability výsledků při změně parametrů modelu.[34]

Všechny metody, které zde byly uvedeny, lze použít v jiných situacích a všechny mají své výhody a nevýhody. Shrnutí těchto výhod, nevýhod a příkladů rozhodovacích problémů, je popsáno v níže uvedené tabulce.

Tabulka 14 Shrnutí jednotlivých metod multikriteriálního hodnocení.

Metoda	Výhody	Nevýhody	Rozhodovací problém
AHP	Strukturovaný přístup, zahrnuje kvantitativní i kvalitativní faktory, nabízí možnost zapojení více stakeholderů.	Komplexní výpočetní proces, Nutnost konsistence při porovnávání.	Hierarchické problémy s mnoha kritérii a alternativami.
PROMETHEE	Účinná při konečném počtu kritérií, poskytuje částečné i úplné pořadí.	Neposkytuje podporu při přiřazování vah kritériím.	Problémy vyžadující pořadí nebo klasifikaci alternativ.
ELECTRE	Používá implicitní dominanci, účinná pro eliminaci tzv. slabých alternativ.	Vyžaduje přesné měření kritérií.	Problémy s eliminací slabých alternativ.
PAPRIKA	Jednoduchá a intuitivní, podporuje více účastníků, používá párové srovnání.	Omezený rozsah aplikací, závislost na softwaru.	Problémy vyžadující spolupráci a jednoduché srovnání.
TOPSIS	Jednoduché výpočty, funguje i s chybějícími údaji. Používá nejlepší a nejhorší možnou variantu pro srovnání.	Obtížná interpretace při použití váženého hodnocení kritérií.	Problémy s kompenzovatelnými kritérii a hledáním optimální volby.
SAW	Jednoduché výpočty, intuitivní pro rozhodování.	Není vhodná pro komplexní problémy.	Základní rozhodovací problémy s kompenzovatelnými kritérii.

MA-CBETH	Používá kvalitativní soudy, které převádí je na číselné hodnoty, je účinný pro strategické plánování.	Omezený rozsah aplikací, závislost na softwaru.	Problémy vyžadující kvalitativní hodnocení a strategické plánování.
----------	---	---	---

(zdroje:[29][34][35][36][37][38][45])

3.3 Softwarové nástroje využitelné při multikriteriální analýze

MC&S2 analyzer

Aplikace MC&S2 analyzer představuje softwarové řešení pro komplexní hodnocení různých možností. Tento nástroj je založen na principu analytického hierarchického procesu, nachází své hlavní uplatnění v oblasti bezpečnosti, ačkoliv jeho využití může být v kterýchkoliv jiných oblastech. Jedná se o tuzemský program vyvinutý společností CALS servis s.r.o., která se zabývá implementací technologie CALS (Continuous Acquisition & Life-cycle Support). Tyto technologie jsou zaměřeny na zvýšení efektivity akvizic ve státní správě a konkurenceschopnosti výrobních podniků.[24]

Předností tohoto nástroje, je jeho schopnost zpracovávat širokou škálu proměnných. Uživatelé mohou do programu zadat rozmanité faktory jako bezpečnostní rizika přes ekonomické ukazatele až po výkonnostní parametry a uspořádat je do přehledné hierarchické struktury. Každému prvku lze přiřadit specifickou váhu, což umožňuje zohlednit jemné nuance hodnotícího procesu.[25]

Matematické jádro aplikace pracuje na principu porovnávání jednotlivých kritérií, přičemž bere v úvahu jejich relativní důležitost. Zajímavou funkcí je možnost definovat, zda je u daného kritéria žádoucí vyšší či nižší hodnota, což dále zvyšuje flexibilitu systému. Výsledky analýzy jsou prezentovány v podobě snadno čitelných grafů a tabulek, což usnadňuje interpretaci dat a následné rozhodování. Tato vlastnost činí MC&S2 analyzer cenným nástrojem nejen v oblasti bezpečnosti a obrany, ale i při hodnocení nabídek ve veřejných zakázkách či v personalistice.[25]

Díky všestrannosti a schopnosti objektivizovat složité rozhodovací procesy, se tento software jeví jako užitečný pomocník pro manažery a odborníky napříč různými odvětvími. Nejedná se o software s bezplatným užíváním. Přístup do něj je možný pouze přes fakultu aplikované informatiky v rámci studia.[25]

The screenshot shows the MC&S2 analyzer interface. At the top, there is a yellow navigation bar with the user's name 'Tomáš Pílkový' and several menu items: 'Seznam úloh', 'Editace úloh', 'Kritéria', 'S2', 'Nápověda', 'O programu', 'Odhlásit se', and 'MC&S2 analyzátor'. Below the navigation bar, the 'Úloha' (Task) section shows a dropdown menu with '275 - Vyběr vhodného kandidáta'. The 'Varianta' (Variant) section has a dropdown menu with 'Vyběr ...' and two checkboxes: 'Zobrazit všechny varianty' (checked) and 'Přepočítat body' (unchecked). Below this, there is a button 'PŘIDAT KRITÉRIUM' with a plus icon. The interface displays two variants of criteria and weights:

Varianta 1: RCH

1. Rok	50,00 Rok	0.07	
2. Zkušenosti s lisovnou	15,00 Rok	0.33	
3. Leadership	35,00 %	0.2	
4. Akceptace týmu	90,00 %	0.27	
5. Práce office	80,00 %	0.13	

Varianta 2: EZ

1. Rok	30,00 Rok	0.07	
2. Zkušenosti s lisovnou	1,00 Rok	0.33	
3. Leadership	65,00 %	0.2	
4. Akceptace týmu	10,00 %	0.27	
5. Práce office	20,00 %	0.13	

Obrázek 9 Ukázka prostředí MC&S2 analyzeru

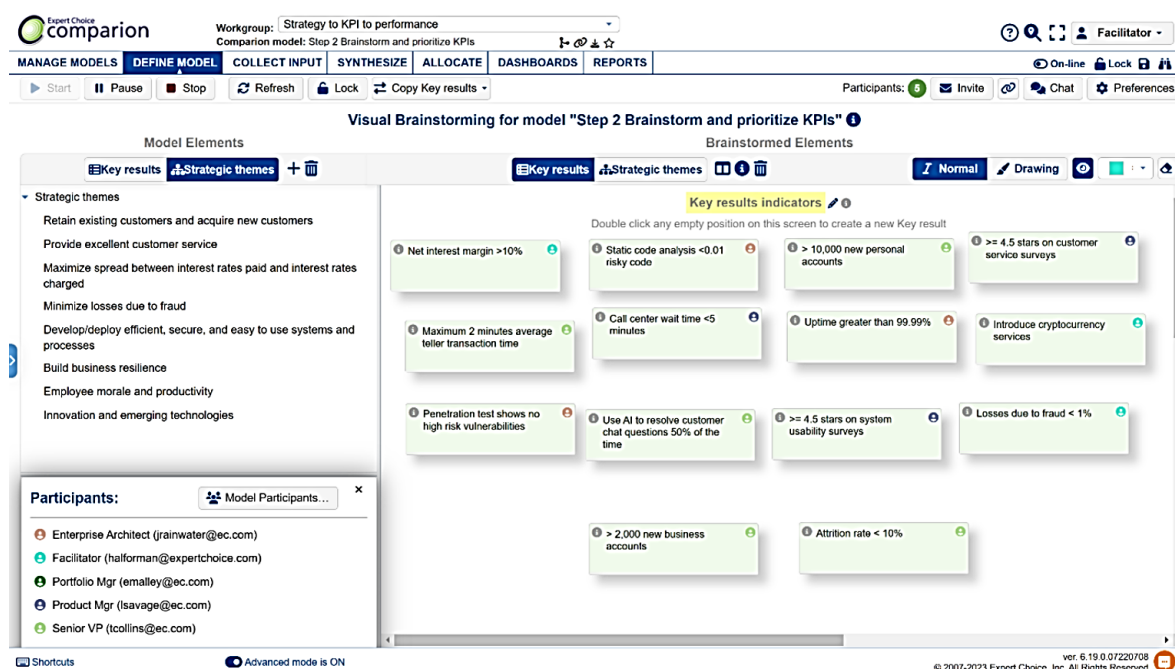
(zdroj:[23])

Expert Choice

Expert Choice je software pro podporu rozhodování, který kombinuje kolaborativní týmové nástroje s principem analytického hierarchického procesu. Proces rozhodování zde zahrnuje několik klíčových kroků.[26]

Nejprve se strukturuje komplexnost problému identifikací alternativních postupů a cílů, které jsou uspořádány do hierarchie. Následně se měří důležitost konkurenčních cílů a alternativ pomocí párového srovnávání nebo absolutních hodnotících stupnic. Tento přístup umožňuje zahrnout jak objektivní data, tak subjektivní úsudky založené na znalostech a zkušenostech.[26]

Po měření následuje syntéza informací, která automaticky kombinuje všechna měření podle hierarchie cílů. Unikátnost tohoto procesu spočívá v tom, že zahrnuje jak objektivní informace, tak subjektivní vstupy od rozhodovatelů. Software také umožňuje provádět analýzy typu "co kdyby" a citlivostní analýzy, díky tomu lépe zohledňuje možné dopady různých faktorů na konečné rozhodnutí.[26]



Obrázek 10 Ukázka uživatelského prostředí Expert Choice

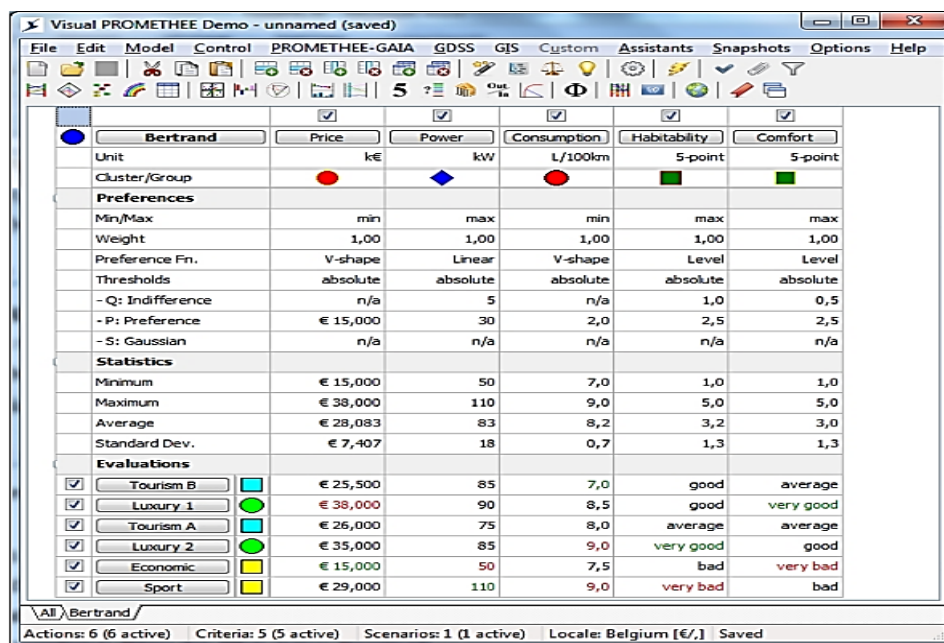
(zdroj:[26])

Visual PROMETHEE

Visual PROMETHEE je software pro vícekritériální rozhodovací analýzu, který pomáhá uživatelům hodnotit a porovnávat různé možnosti rozhodnutí na základě vícero (často protichůdných) kritérií.[27]

Hlavní funkce zahrnují hodnocení různých možných rozhodnutí nebo položek, podle vícero kritérií, identifikaci nejlepšího možného rozhodnutí, seřazení možností od nejlepší po nejhorší, třídění položek do předem definovaných tříd a vizualizaci rozhodovacích problémů pro lepší pochopení. Software také pomáhá dosáhnout jednomyslných rozhodnutí, když mají různí rozhodovatelé protichůdné názory.[27]

Program využívá metody PROMETHEE I a II pro částečné a úplné seřazení alternativ a citlivostní analýzu pro zkoumání vlivu změn vah kritérií. Uživatelské rozhraní je navrženo tak, aby bylo intuitivní a snadno použitelné, s možností definovat více scénářů pro porovnání různých pohledů.[27]



Obrázek 11 Ukázka uživatelského prostředí Visual PROMETHEE

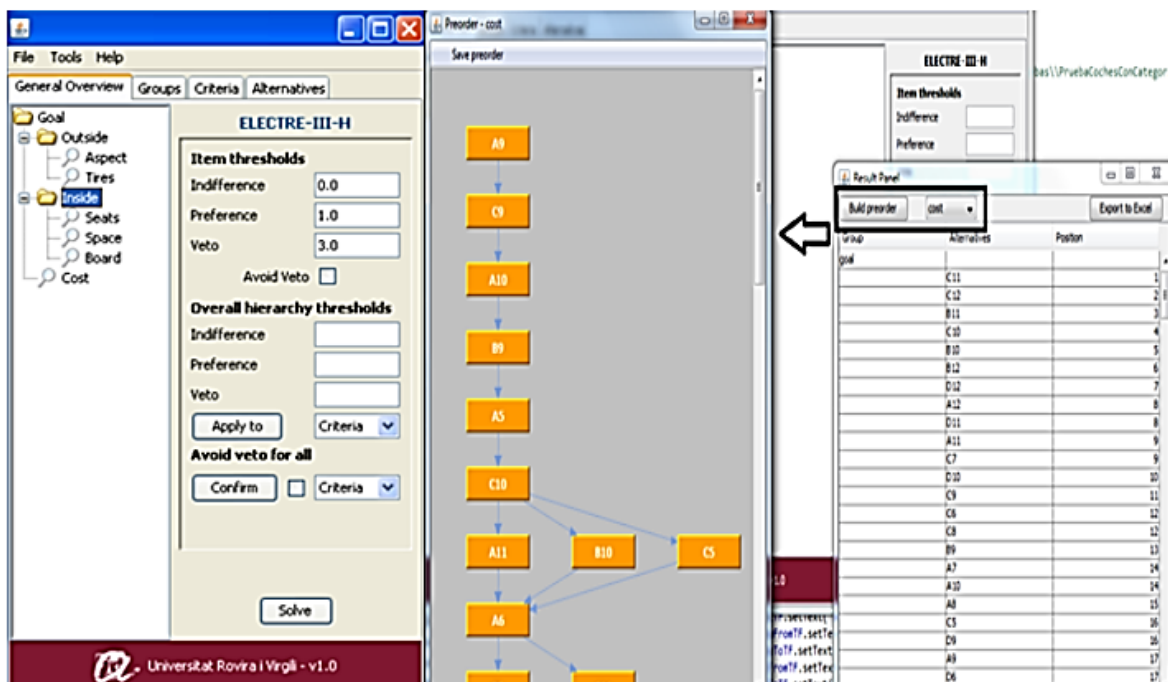
(zdroj:[27])

ELECTRE-H

ELECTRE-H je nástroj pro podporu rozhodování, který implementuje dvě metody pro problémy řazení a uspořádané klasifikace s více kritérii strukturovanými do hierarchie. Tento software rozšiřuje možnosti tradičních metod ELECTRE tím, že umožňuje hierarchické rozložení rozhodovacích problémů, což pomáhá rozhodovatelům lépe organizovat komplexní problémy na základě jejich odborných znalostí a potřeb.[28]

Klíčovou vlastností je jeho schopnost aplikovat standardní postup převýšení na všech úrovních hierarchie kritérií. To znamená, že rozhodovatelé získají výsledky (pořadí nebo klasifikaci) na každém mezilehlém uzlu hierarchie i na kořenovém uzlu. Software také umožňuje řízení nejistoty preferencí a právo veta na příslušných uzlech, což poskytuje větší flexibilitu při rozhodování.[28]

Software podporuje různé měřicí stupnice pro elementární i mezilehlá kritéria, což zvyšuje jeho všestrannost. Uživatelské rozhraní je navrženo tak, aby bylo přehledné a snadno srozumitelné, s podporou vstupních souborů Excel pro snadné zadávání dat. K dispozici jsou také vizualizační nástroje, které graficky zobrazují výsledky a umožňují jejich export jako obrázky PNG nebo textové soubory.[28]



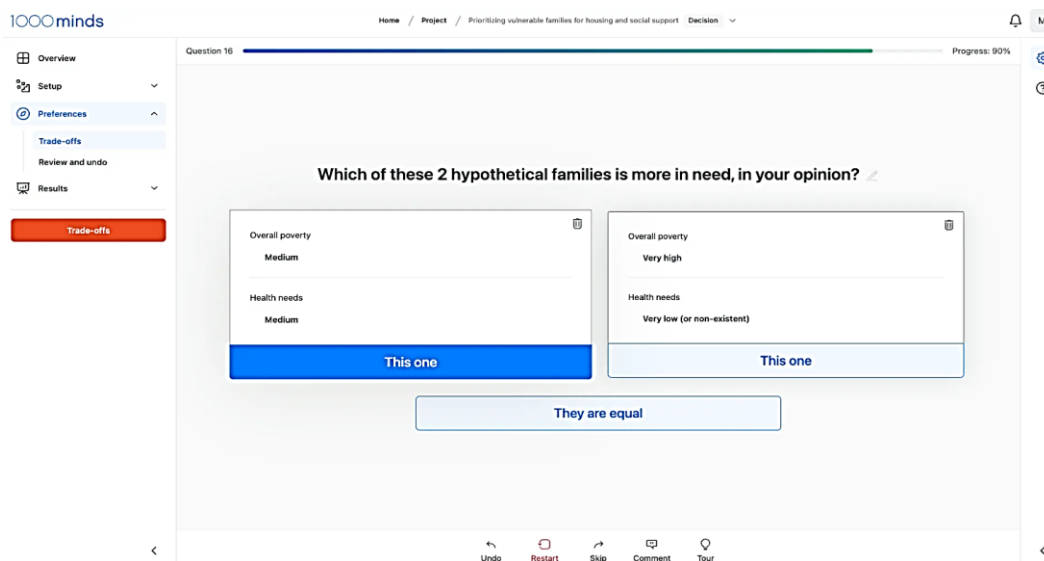
Obrázek 12 Ukázka uživatelského prostředí ELECTRE-H

(zdroj:[28])

1000minds

Mechanismus tohoto softwaru pro podporu rozhodování je založen na metodě PAPRIKA (Potentially All Pairwise Rankings of all possible Alternatives) a funguje v několika krocích. Nejprve rozhodovatel definuje rozhodovací problém, včetně alternativ a kritérií. Následně software prezentuje sérii párových srovnání mezi hypotetickými alternativami, přičemž každé srovnání se týká pouze dvou kritérií současně.[29]

Adaptivní algoritmus na základě předchozích odpovědí vybírá další relevantní párová srovnání, čímž minimalizuje počet potřebných otázek. Z těchto odpovědí software matematicky odvozuje váhy jednotlivých kritérií, které pak využívá k hodnocení všech dostupných alternativ a vytvoření jejich pořadí. Rozhodovatelé mohou provádět analýzu citlivosti pro zjištění vlivu změn vah kritérií na celkové pořadí. V případě skupinového rozhodování software agreguje preference jednotlivých účastníků a identifikuje oblasti shody a neshody. Tento přístup umožňuje efektivní a transparentní rozhodování i v komplexních situacích s mnoha kritérii a alternativami.[29]



Obrázek 13 Ukázka uživatelského prostředí 1000minds

(zdroj:[29])

TOPSIS

Tento nástroj umožňuje rozhodovatelům pracovat s libovolným počtem kritérií a alternativ, automatizuje klíčové kroky analýzy včetně normalizace dat, přiřazování vah kritériím a výpočtu vzdáleností od ideálního a nežádoucího řešení. Integrace s Excelem zjednodušuje import dat, zatímco podrobné reporty s postupem výpočtů zajišťují transparentnost.[30]

Rozhodovatel nejprve definuje kritéria (např. cena, výkon) s přiřazenými váhami a typem optimalizace (maximalizace/minimalizace), poté vloží data o alternativách přímo z Excelu nebo ručně. Software automaticky normalizuje hodnoty kritérií na jednotkovou škálu, aplikuje váhy a vytvoří váženou matici. Následně určí ideální (nejlepší možné hodnoty) a anti-ideální (nejhorší možné hodnoty) řešení pro každé kritérium. Pro každou alternativu vypočítá Euklidovskou vzdálenost od těchto dvou extrémů a na jejím základě stanoví koeficient blízkosti (0–1), který určuje pořadí alternativ – čím vyšší koeficient, tím lepší pozice.[30]

Výsledky zobrazí v podrobném reportu s maticemi, vzdálenostmi a žebříčkem, včetně možnosti exportu do Excelu nebo PDF. Uživatelé mohou provádět analýzu citlivosti změnou vah kritérií, přičemž software okamžitě přepočítá pořadí alternativ.[30]

Topsis Software
Best college

1 Project name 2 Project info 3 Data entry 4 Output

Alternatives

Number of alternatives: 5 [Create table of alternatives](#)

	name
1	College 1
2	College 2
3	College 3
4	College 4
5	College 5

Criteria

Number of criteria: 4 [Create table of criteria](#)

	name	type	weight
1	Management	+	0.35
2	Facility	+	0.25
3	Professors	+	0.3
4	Students	-	0.1

[Back](#) [Next](#)

Obrázek 14 Ukázka uživatelského prostředí TOPSIS

(zdroj:[30])

SAW

Metoda váženého součtu SAW (Simple Additive Weighting), implementovaná v tomto softwaru, je známá svou jednoduchostí a intuitivností. Umožňuje rozhodovatelům hodnotit a seřadit alternativy na základě jejich výkonu v různých kritériích. Proces zahrnuje standardizaci rozhodovací matice, přiřazení vah jednotlivým kritériím a výpočet celkového skóre pro každou alternativu. Tato metoda je obzvláště užitečná v situacích, kde je potřeba zohlednit více konfliktních cílů.[31]

Klíčové funkce SAW Software zahrnují neomezený počet kritérií a alternativ, možnost nastavení vah a typů kritérií, a flexibilitu v úpravách projektu. Software umožňuje snadný import dat z Excelu a poskytuje detailní výstupní zprávu, která zahrnuje rozhodovací matici, normalizovanou matici a podrobný výpočet. Výsledky lze exportovat do formátů Excel a Word.[31]

Saw Software
Best college

1 Project name 2 Project info 3 Data entry 4 Output

Expert 1 [Delete Expert] [Save Expert] [Add Expert] [Experts status] [Mean]

decision matrix (expert 1)

	Management	Facility	Professors	Students
college 1	3	5	7	2
college 2	7	4	3	3
college 3	2	1	2	2
college 4	3	1	4	5
college 5	2	1	4	2

[Back] [Next]

Obrázek 15 Ukázka uživatelského prostředí SAW

(zdroj:[31])

Třetí kapitola byla zaměřena na principy a metody multikriteriálního hodnocení, které umožňují objektivní rozhodování mezi více variantami na základě několika kritérií. Podrobně popisuje způsoby stanovení vah kritérií, jednotlivé rozhodovací metody a softwarové nástroje, využitelné pro tuto analýzu v praxi.

4 ANALÝZA RIZIK

Analýza rizik je klíčovým procesem v rámci řízení rizik, který umožňuje organizacím identifikovat, vyhodnotit a prioritizovat potenciální hrozby a příležitosti. Tato kapitola se zaměří na teoretické základy analýzy rizik, včetně jejích metod a dostupných softwarových nástrojů, které lze v praxi využít pro efektivní řízení rizik. Vybrané metody včetně softwarového nástroje, budou použity při praktické části této práce.

Analýza rizik hraje důležitou roli při plánování a rozhodování v organizacích jakékoliv velikosti. Pečlivé zjišťování, posuzování a řešení možných hrozeb tvoří základní součást úspěšného vedení projektů i běžného fungování organizací. Zavedení systému pro práci s riziky pomáhá snížit nepříznivé následky a zároveň zvyšuje šanci na úspěch díky včasnému rozpoznání důležitých rizikových prvků.[39]

Samotný proces řízení rizik, můžeme rozdělit do několika hlavních kroků: určení základního rámce pro práci s riziky, vyhledávání možných rizik, jejich důkladné posouzení, zavedení řešení k jejich omezení nebo odstranění a průběžné sledování spojené s pravidelným přehodnocováním. Každý z těchto kroků má v celkovém systému řízení rizik své vlastní postupy a jedinečný význam.[39]

Riziko

Riziko lze definovat jako možnost, že s určitou pravděpodobností dojde k události, která je nežádoucí z hlediska bezpečnosti. Jedná se o subjektivní koncept, který vychází z konkrétní hrozby. Úroveň rizika je určována pravděpodobností vzniku škodlivých důsledků, které jsou spojeny s danou hrozbou a zranitelností chráněného zájmu.[40]

Scénář

Popisuje průběhu možného budoucího vývoje děje, který může nastat v důsledku výskytu hrozby, v určitém časovém horizontu.[40]

Pravděpodobnost

Pravděpodobnost rizika je míra, s níž dojde k uskutečnění rizika. Čím vyšší je tato hodnota, tím větší je riziko, že se událost skutečně projeví. Pravděpodobnost se odvozuje z historických dat nebo subjektivních odhadů odborníků, přičemž zohledňuje faktory jako zranitelnost aktiv a existující hrozby.[41]

Dopad

Dopad představuje přímý negativní účinek, který nastane v případě uskutečnění rizika. Jedná se o konkrétní následky, jež ovlivňují procesy, aktiva nebo cíle organizace. Dopad se projevuje formou škody nebo zhoršení stavu, který může mít provozní, finanční, právní nebo reputační charakter.[41]

Aktivum

Všechno, co má pro organizaci hodnotu a může být ohroženo hrozbou. Tato hodnota nebo důležitost vyplývá z toho, že organizace dané aktivum potřebuje ke svému fungování.[41]

4.1 Legislativa v oblasti řízení rizik

Standardizace v oblasti řízení rizik poskytuje organizacím systematický přístup k identifikaci, analýze a ošetření potenciálních rizik. Mezinárodní organizace pro standardizaci ve spolupráci s Mezinárodní elektrotechnickou komisí, vyvinuly komplexní soubor standardů, které poskytují rámec pro efektivní řízení rizik.

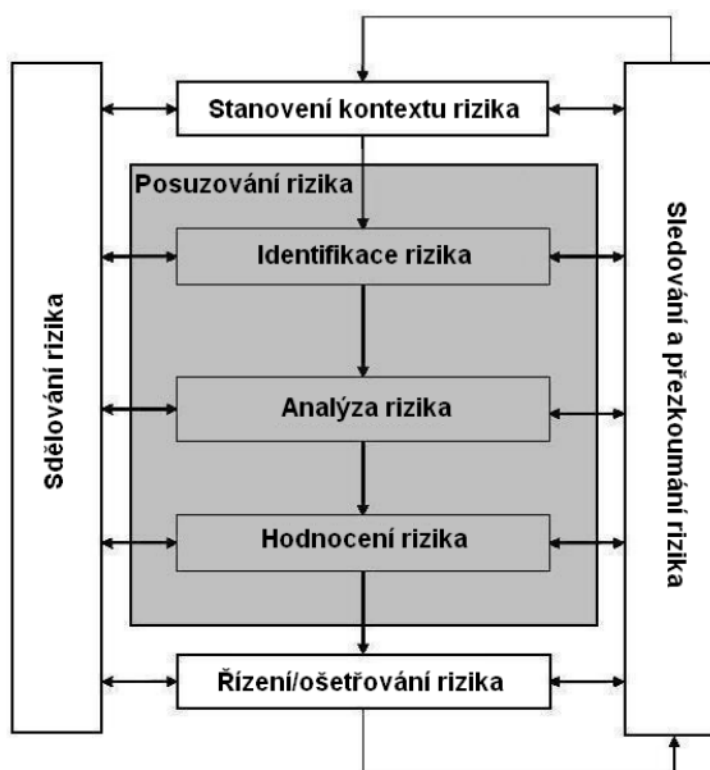
4.1.1 ČSN ISO 31000 Management rizik

Norma ISO 31000 byla původně vydána v roce 2009 jako první mezinárodně uznávaný standard poskytující komplexní přístup k řízení rizik. V roce 2018 byla vydána aktualizovaná verze ISO 31000:2018, která nahradila předchozí vydání z roku 2010.[42]

Tato revize přinesla několik významných změn, jako:

- Revize zásad managementu rizik, které jsou klíčovými kritérii pro jeho úspěch.
- Zdůraznění významu vedení ze strany vrcholového managementu a integrace řízení rizik.
- Větší důraz na iterativní povahu managementu rizik.
- Zefektivnění obsahu s větším zaměřením na udržování modelu otevřených systémů.[42]

Norma poskytuje společný přístup pro řízení jakéhokoliv typu rizika a není specifická ani pro konkrétní typ průmyslu, nebo pro specifické sektory. Lze ji využívat po celou dobu života organizace a aplikovat na jakoukoliv činnost, včetně rozhodování na všech úrovních. Obrázek 16, ilustruje průběh procesu management rizik.[42]



Obrázek 16 Proces managementu rizik, dle ČSN ISO 31000

(zdroj:[43])

Základní principy a struktura

1. Zásady managementu rizik: Principy, které jsou základem efektivního řízení rizik.
2. Rámec (struktura): Organizační uspořádání podporující řízení rizik.
3. Proces managementu rizik: Systematická aplikace politik, postupů a praktik pro komunikaci, konzultace, stanovení kontextu a identifikaci, analýzu, hodnocení, ošetření, monitoring a přezkoumání rizik.[42]

Podrobnější popis rámce managementu rizik podle ISO 31000 je znázorněno tabulce 15.

Tabulka 15 Rámec managementu rizik dle ISO 31000

Vedení a závazek	Integrace	Zajištění, že management rizik je integrován do všech činností
	Prohlášení o závazku	Vypracování prohlášení o politice managementu rizik

	Přidělení zdrojů	Zajištění odpovídajících zdrojů pro management rizik
Návrh	Porozumění organizaci	Analýza externího a interního kontextu organizace
	Vyjádření závazku	Demonstrace závazku prostřednictvím politiky a strategie
	Přidělení rolí	Ustanovení odpovědností a pravomocí
	Alokace zdrojů	Zajištění potřebných zdrojů pro management rizik
	Komunikace	Definování přístupu ke komunikaci a konzultaci
Implementace	Plán	Specifikace časového horizontu a strategie
	Rámec	Aplikace rámce managementu rizik v organizaci
	Implementace procesu	Realizace procesu managementu rizik
Hodnocení	Měření výkonnosti	Pravidelné měření výkonnosti vůči indikátorům
	Přiměřenost	Hodnocení efektivity a přiměřenosti rámce
Zlepšování	Adaptace	Přizpůsobení rámce změnám v externím a interním kontextu
	Neustálé zlepšování	Kontinuální zlepšování vhodnosti, přiměřenosti a efektivnosti

(zdroj:[42])

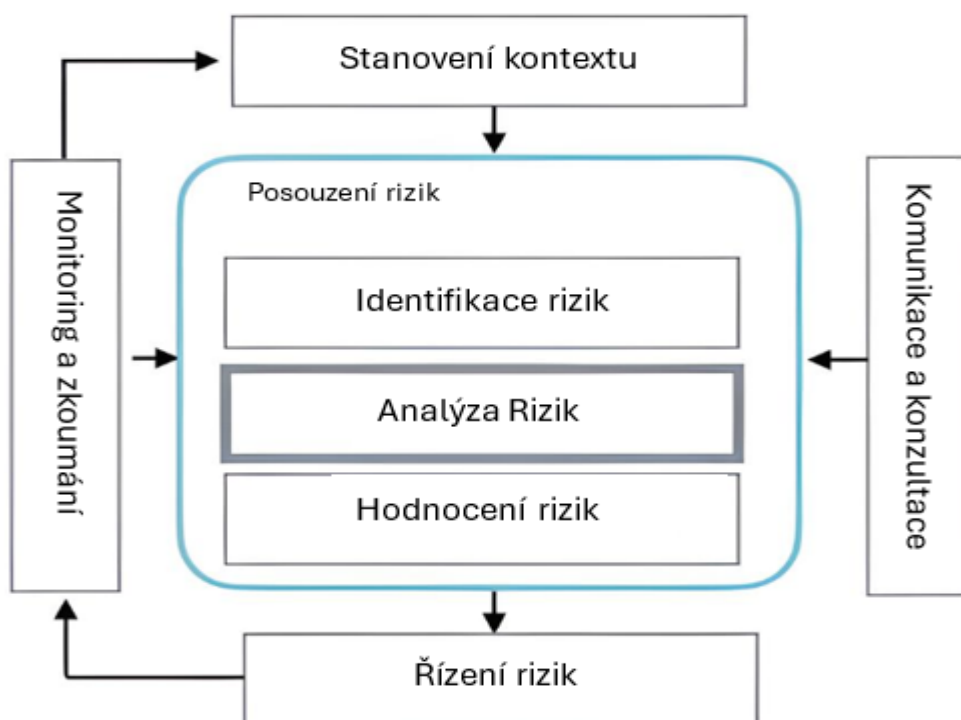
4.1.2 ČSN EN IEC 31010 - Management rizik – Techniky posuzování rizik

Jedná se o podpůrný standard pro ISO 31000, který poskytuje detailní návod na výběr a aplikaci systematických technik pro posuzování rizik. Zatímco ISO 31000 poskytuje obecný rámec pro řízení rizik, ISO/IEC 31010 se zaměřuje specificky na techniky posuzování rizik.[44]

Norma byla původně vydána v roce 2009 a její nejnovější verze pochází z roku 2019 (IEC 31010:2019). Aplikovatelnost je v různých odvětvích a organizacích, bez ohledu na

jejich velikost či zaměření. Podobně jako ISO 31000 není určena specificky pro určitý sektor nebo průmysl.[44]

Posuzování rizik je zde definováno jako: "celkový proces identifikace rizik, analýzy rizik a hodnocení rizik". Tento proces zahrnuje následující kroky, které jsou znázorněny na následujícím obrázku.[44]



Obrázek 17 Vizualizace procesu posuzování rizik dle ČSN EN IEC 31010

(zdroj:[44])

Jedním z nejvýznamnějších přínosů normy ISO/IEC 31010 je právě katalog 31 technik a metod využívaných pro posuzování rizik. Jejich kompletní souhrn je uveden v příloze I. této diplomové práce. Vybrané nepoužívanější techniky budou popsány v následující kapitole.[44]

4.2 Nepoužívanější metody analýzy rizik

Metody, které jsou zmíněny v této kapitole, byli vybrány na základě zkušeností a praxe v automobilovém sektoru. Použití jednotlivých metod se může lišit v závislosti na situaci a oboru kde jsou využívány.

SWOT analýza

SWOT analýza je jedním z nejpoužívanějších typů analýzy v široké škále organizací. Své uplatnění nachází především v prvotních fázích projektu a může být považována za součást procesu analýzy rizik. Tato metoda nabízí ucelený přehled rizikového prostředí organizace či projektu tím, že zkoumá jak interní aspekty (silné a slabé stránky), tak externí faktory (příležitosti a hrozby). Díky své schopnosti poskytnout komplexní pohled na situaci je SWOT analýza často aplikována v kontextu strategického managementu, řízení projektů a při rozhodování o strategiích zmírňování rizik.[6]

Obecný postup metody SWOT

1. Přípravná fáze: V této fázi je nezbytné jasně definovat předmět analýzy a sestavit tým, který bude analýzu provádět. Tým by měl zahrnovat odborníky z různých oblastí relevantních pro analyzovaný subjekt.
2. Identifikace interních faktorů: Druhý krok se zaměřuje na analýzu vnitřních aspektů organizace nebo projektu. Zahrnuje identifikaci silných stránek, které představují například konkurenční výhody, a slabých stránek, které mohou bránit dosažení cílů.
3. Analýza externího prostředí: V této fázi se provádí průzkum vnějšího prostředí s cílem identifikovat příležitosti, které mohou přispět k rozvoji a hrozby, které mohou představovat rizika pro organizaci nebo projekt.
4. Vyhodnocení a interpretace dat: Po shromáždění informací následuje analýza a interpretace získaných dat. Cílem je porozumět vzájemným vztahům mezi jednotlivými faktory a jejich potenciálnímu dopadu na organizaci nebo projekt.
5. Formulace strategií: Na základě provedené analýzy se formulují strategie, které maximalizují využití silných stránek a příležitostí, minimalizují slabé stránky a eliminují nebo zmírňují hrozby.
6. Implementace a monitoring: Poslední fáze zahrnuje vytvoření akčního plánu pro implementaci navržených strategií. Součástí této fáze je také stanovení mechanismů pro průběžné sledování a vyhodnocování efektivity zvolených strategií.[6]

Brainstorming

Brainstorming představuje účinnou metodu, která umožňuje využít rozmanité pohledy, zkušenosti a názory členů skupiny. Díky této různorodosti lze identifikovat široké spektrum rizik, včetně těch spojených s technickými problémy, omezenými zdroji, požadavky a očekáváními zainteresovaných stran či dalšími klíčovými aspekty projektu. Metoda nachází své největší uplatnění zejména v úvodních fázích projektu, kdy je potřeba důkladně definovat rizikové prostředí a vytvořit základ pro jejich následnou analýzu a řízení. Pro její efektivitu je důležité zajistit, aby prostředí bylo nekritické a účastníci neměli obavy vyjádřit své názory. Tato povinnost přísluší moderátorovi celého setkání.[46]

Obsahový postup metody Brainstorming

1. Zahájení: Brainstorming začíná přípravou, kde je definován cíl, vybrána skupina účastníků a jmenován moderátor který představí cíle a stanoví pravidla pro otevřenou komunikaci.
2. Generování nápadů: Účastníci navrhuji potenciální rizika, která jsou zaznamenávána bez hodnocení a kritiky. Jde zejména o kvantitu.
3. Kategorizace a prioritizace: Identifikovaná rizika jsou kategorizována a prioritizována podle oblastí jako jsou například: technické výzvy, omezení zdrojů apod.
4. Analýza a zpřesnění: Skupina diskutuje o rizicích a zpřesňuje jejich formulace. Mohou být použity další techniky pro lepší vizualizaci.
5. Závěr: Zde je provedeno shrnutí rizik a stanoveny další kroky pro jejich analýzu a řízení. Jsou určeny odpovědnosti za zpracování rizik.[6]

Check list

Checklist představuje soubor otázek nebo položek, které jsou důležité pro specifickou situaci či proces. Tyto seznamy jsou obvykle vytvářeny na základě praktických zkušeností a odborných znalostí v příslušné oblasti. Jeho hlavním cílem je zajistit, aby byly všechny relevantní faktory nebo kroky systematicky zkontrolovány a nezůstaly opomenuty.[44]

Obecný postup metody Checklist

1. Příprava checklistu: Sestavení seznamu relevantních otázek nebo bodů, které jsou důležité pro identifikaci a řízení rizik v dané oblasti. Seznam by měl být přehledný a snadno použitelný.
2. Aplikace checklistu: Systematická kontrolu všech bodů. Každý bod by měl být vyhodnocen a případně doplněn o další informace nebo komentáře.
3. Vyhodnocení výsledků: Na základě provedené kontroly jsou vyhodnoceny identifikovaná rizika a stanoveny priority pro jejich řešení.[44]

FMEA (Failure Mode and Effects Analysis)

Tato metoda představuje systematický nástroj pro identifikaci potenciálních poruch, jejich příčin a následků v technických systémech, výrobních procesech nebo službách. Její kořeny sahají do 40. let 20. století, kdy byla vyvinuta pro vojenské účely, a později adaptována v kosmickém programu NASA (National Aeronautics and Space Administration). Dnes se využívá napříč průmyslovými odvětvími, veřejnou správou i službami jako součást strategického řízení rizik.[46]

Hlavní princip je založen na analýze možných způsobů selhání a jejich důsledků, přičemž se hodnotí závažnost každého potenciálního selhání, pravděpodobnost jeho výskytu a schopnost detekce. Tyto faktory se kvantifikují pomocí parametrů závažnosti (S), pravděpodobnosti výskytu (O) a detekce (D), z nichž se vypočítá ukazatel RPN (Risk Priority Number). Tento ukazatel umožňuje priorizovat rizika a navrhnout preventivní opatření pro minimalizaci nebo eliminaci potenciálních problémů.[46]

Obecný postup metody FMEA

1. Příprava analýzy: Tým složený z expertů definuje rozsah analýzy, např. konkrétní výrobní proces nebo hrozbu. Klíčové je stanovit hranice systému a kritéria pro hodnocení rizik
2. Identifikace hrozeb: Jsou identifikovány konkrétní hrozby, které jsou následně metodou hodnoceny (například v kontextu tématu této diplomové práce se může jednat o nepřijetí změn zaměstnanců organizace, selhání softwaru apod.)
3. Kvantitativní hodnocení: Každá z těchto hrozeb je ohodnocena dle stanovený škály, většinou 1–10 a to z hlediska závažnosti, pravděpodobnosti a detekovatelnosti, viz

obrázek 18. Následně je počítána hodnota RPN (na obrázku 18, se jedná o sloupec riziko), dle vzorce $S \times O \times D$.

Aktivum	Hrozba	Závažnost	Pravděpodobnost výskytu	Možnost odhalení	Riziko
Lidé	Napadení	2	2	2	8
Lidé	Úraz	4	2	3	24
Lidé	Útok zaměstnance	4	3	1	12
Majetek návštěvníků	Krádež	2	2	3	12
Majetek návštěvníků	Poškození	2	3	4	24
Majetek návštěvníků	Zničení	4	1	4	16
Hmotný majetek společnosti - hotovost	Krádež	1	1	2	2
Hmotný majetek společnosti - výrobní zařízení	Krádež	5	1	1	5
Hmotný majetek společnosti - výrobní zařízení	Poškození	3	3	3	27
Hmotný majetek společnosti - výrobní zařízení	Zničení	5	2	2	20
Hmotný majetek společnosti - drobné nástroje	Krádež	2	3	3	18
Hmotný majetek společnosti - drobné nástroje	Poškození	1	3	4	12
Hmotný majetek společnosti - drobné nástroje	Zničení	2	2	4	16
Nehmotný majetek společnosti - know-how	Krádež	5	1	4	20
Nehmotný majetek společnosti - know-how	Poškození	1	1	4	4
Nehmotný majetek společnosti - know-how	Zničení	1	1	4	4
Nehmotný majetek společnosti - pověst společnosti	Poškození	5	2	3	30
Majetek dodavatelů externích služeb	Krádež	4	2	2	16
Majetek dodavatelů externích služeb	Poškození	4	3	3	36
Majetek dodavatelů externích služeb	Zničení	5	2	2	20
Budova	Poškození	2	3	4	24
Budova	Požár	5	2	2	20
Kontinuita	Výpadek el. proudu	4	2	5	40
Kontinuita	Špatné počasí	3	3	3	27
Kontinuita	Narušení atmosféry	5	2	3	30

Obrázek 18 Ukázka metody modifikované metody FMEA

(zdroj:[23])

- Řazení: Po provedení výpočtů jsou hrozby řazeny dle od nejvyšší hodnoty RPN. Tyto kritické hrozby by měli být přednostně řešeny formou nápravných opatření, standardně ve formě akčních plánů.

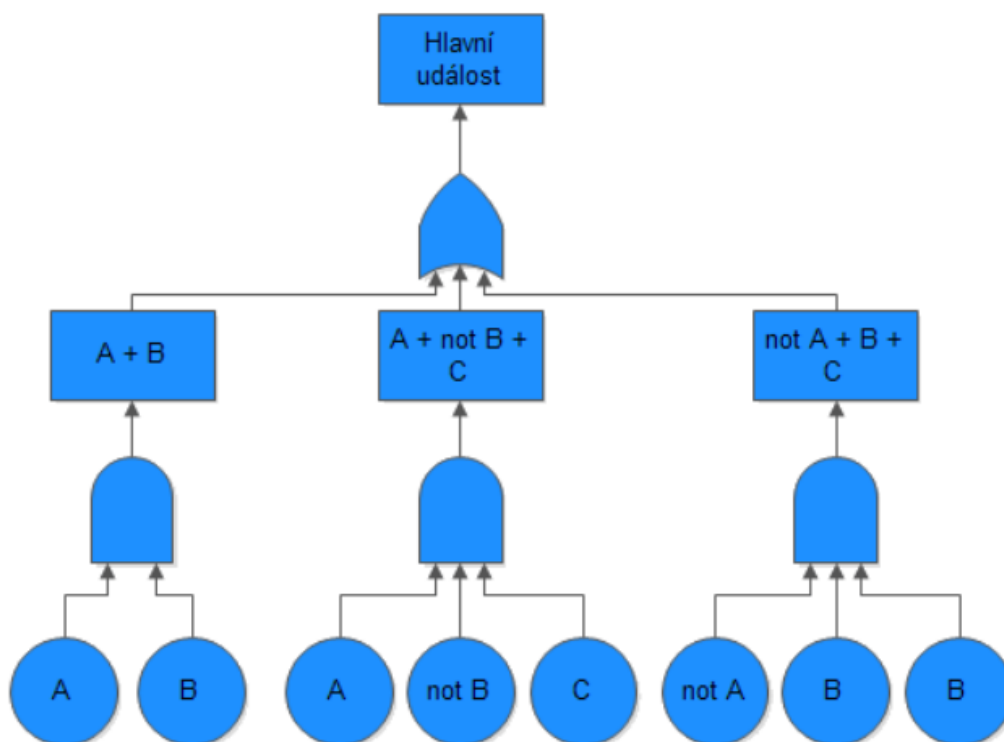
FTA (Fault Tree Analysis)

FTA (Analýza poruchových stromů) je deduktivní metoda pro identifikaci a hodnocení příčin systémových selhání. Vyvinuta v 60. letech 20. století pro potřeby amerického vojenského a kosmického programu. Dnes se využívá v kritických odvětvích včetně jaderné energetiky, letectví a chemického průmyslu. Metoda modeluje kauzální řetězce pomocí logických operátorů (AND/OR) a umožňuje kvantifikovat pravděpodobnost nežádoucích událostí. [44]

Obsahový postup metody FTA

1. Definice top eventu a rozsahu analýzy: Analýza začíná přesným vymezením nežádoucí události (top event), která musí být specifická a měřitelná, přičemž současně dochází k jasnému stanovení hranic analyzovaného systému, což zajišťuje fokus a efektivitu celého procesu.
2. Konstrukce poruchového stromu: V této fázi se vytváří grafická reprezentace kauzálních vztahů vedoucích k top eventu, přičemž se využívá multidisciplinární expertízy k identifikaci bezprostředních příčin, které jsou následně logicky dekomponovány pomocí AND a OR bran až na úroveň základních, dále nedělitelných událostí.
3. Kvalitativní analýza: Tento krok zahrnuje určení minimálních množin pomocí algoritmických metod, což umožňuje identifikovat kritické kombinace událostí vedoucích k top eventu, a následnou prioritizaci rizik na základě počtu událostí v množině a závažnosti jejich potenciálních dopadů.
4. Kvantitativní analýza: V rámci kvantitativní analýzy dochází ke sběru historických dat o poruchovosti komponent, výpočtu pravděpodobnosti výskytu top eventu pomocí matematických modelů a provedení analýzy citlivosti pro identifikaci komponent s největším vlivem na celkovou spolehlivost systému.
5. Návrh mitigačních opatření: Na základě výsledků předchozích analýz se navrhuje konkrétní opatření ke snížení rizika, jako je implementace redundancí, optimalizace preventivní údržby či instalace detekčních systémů, přičemž se zohledňuje jejich potenciální dopad na snížení pravděpodobnosti výskytu top eventu.
6. Validace a aktualizace: Závěrečná fáze zahrnuje ověření reálného chování systému vůči FTA modelu pomocí simulačních testů a zajištění periodické revize a aktualizace poruchového stromu tak, aby reflektoval změny v designu nebo provozních podmínkách analyzovaného systému.[6]

Celá struktura je znázorněna na následujícím obrázku 19.



Obrázek 19 Ukázka struktury FTA analýzy

(zdroj:[47])

CCA (Cause Consequence Analysis)

Analýza příčin a následků je komplexní analytická metoda kombinující prvky analýzy stromu poruch a analýzy stromu událostí. Zaměřuje na identifikaci a kvantifikaci příčinných řetězců vedoucích od iniciačních událostí k potenciálním následkům. CCA umožňuje vizualizaci a analýzu komplexních scénářů rizik, přičemž zohledňuje časovou posloupnost událostí. Metoda je zvláště účinná při hodnocení bezpečnostních funkcí a jejich vlivu na vývoj nežádoucích událostí.[46]

Obecný postup metody CCA

1. Systémová analýza a definice rozsahu: Prvním krokem je důkladné prozkoumání analyzovaného systému, včetně jeho rozhraní a funkčních diagramů. Na základě tohoto přehledu se definuje rozsah analýzy a identifikují se klíčové komponenty.
2. Identifikace iniciační události: Vybere se kritická událost, která může spustit řetězec nežádoucích následků. Tato událost tvoří výchozí bod pro konstrukci diagramu příčin a následků

3. Analýza následků: Vytvoří se strom událostí zobrazující možné scénáře vývoje po iniciační události. Každá větev stromu reprezentuje různé stavy bezpečnostních systémů a jejich vliv na průběh události.
4. Analýza příčin: Pro každou kritickou událost nebo selhání bezpečnostní funkce se konstruuje strom poruch, který identifikuje základní příčiny a jejich kombinace vedoucí k dané události
5. Integrace příčin a následků: Stromy poruch se integrují do stromu událostí, čímž vzniká komplexní diagram příčin a následků. Tento krok umožňuje vizualizaci vztahů mezi příčinami a jejich potenciálními dopady.
6. Kvantitativní analýza: Pokud jsou k dispozici spolehlivá data, přiřadí se pravděpodobnosti k jednotlivým větvím a událostem. To umožňuje výpočet celkové pravděpodobnosti různých koncových stavů
7. Vyhodnocení a dokumentace: Analyzují se výsledky, identifikují se kritické cesty a slabá místa systému. Výstupy se dokumentují, včetně grafické reprezentace diagramu příčin a následků, pravděpodobností koncových stavů a doporučení pro snížení rizik. [44]

4.3 Softwarové nástroje využitelné při analýze rizik

RISKAN

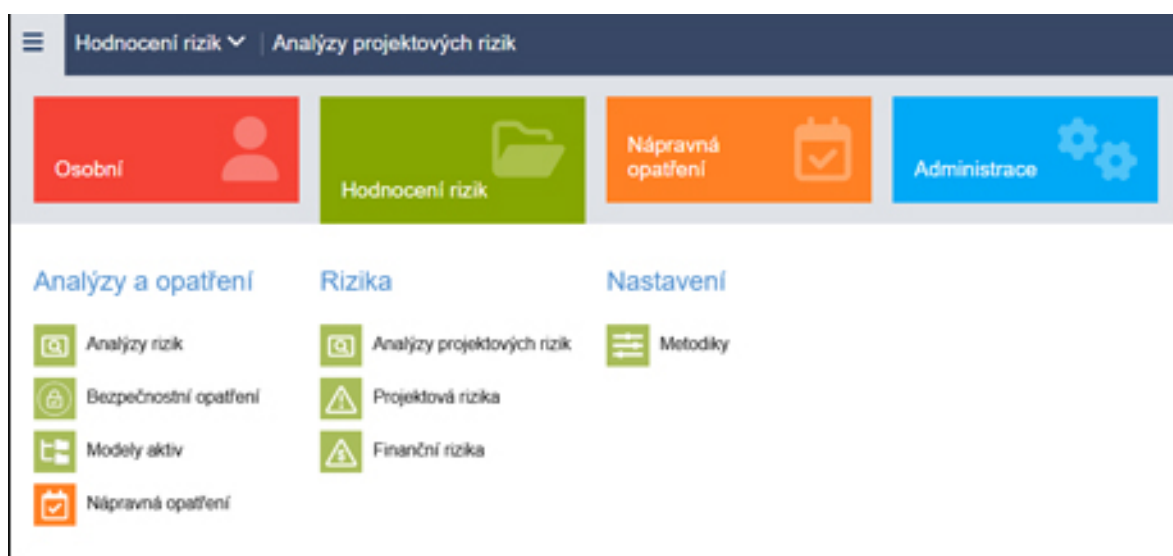
V rámci analýzy softwarových nástrojů pro řízení rizik v českém prostředí je vhodné zmínit také produkt RISKAN od společnosti T-SOFT a.s. Tento nástroj, implementovaný v prostředí Microsoft Excel, se zaměřuje především na kvantitativní a semi-kvantitativní analýzu rizik v oblastech jako havarijní plánování či ochrana obyvatelstva. Software operuje s koncepty aktiv, hrozeb a zranitelností, umožňující uživatelům identifikovat a kategorizovat aktiva, hodnotit hrozby a vypočítávat rizikové hodnoty. Jeho metodika vychází ze základního vzorce pro výpočet rizika, kde se kombinuje pravděpodobnost výskytu hrozby s potenciálním dopadem. Vzorec pro výpočet je součin Aktiva x Hrozby x Zranitelnost. [48]

Využití tohoto nástroje je dokumentováno zejména v akademické sféře a projektech veřejné správy. Příkladem může být jeho aplikace při analýze rizik pro město Zlín nebo při hodnocení bezpečnosti logistických skladů. Z hlediska legislativního souladu, RISKAN reflektuje požadavky vyhlášky o kybernetické bezpečnosti a normy ISO IEC 27001. Nicméně,

bezpečnosti, zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a implementuje požadavky směrnice NIS2. Tyto vlastnosti z něj činí vhodný nástroj pro organizace, které potřebují zajistit soulad s regulačními požadavky.[50]

Další klíčová vlastnost, je automatizace procesů spojených s řízením rizik. Systém je schopen generovat auditní dokumentaci a bezpečnostní reporty, což významně snižuje administrativní zátěž spojenou s řízením kybernetické bezpečnosti. Navíc nabízí vizualizační nástroje v podobě přehledných dashboardů, které usnadňují interpretaci dat jak pro manažery, tak pro technické týmy.[50]

Z hlediska praktického nasazení nachází tento software uplatnění v různých odvětvích, přičemž zvláště významné je jeho využití ve veřejné správě, zdravotnictví a velkých korporacích. Flexibilita nasazení je podpořena možností volby mezi cloudovým a on-premise řešením, což umožňuje organizacím zvolit model, který nejlépe odpovídá jejich specifickým potřebám a bezpečnostním požadavkům.[50]



Obrázek 21 Ukázka prostředí softwaru Risk*Guide

(zdroj:[50])

APTIEN

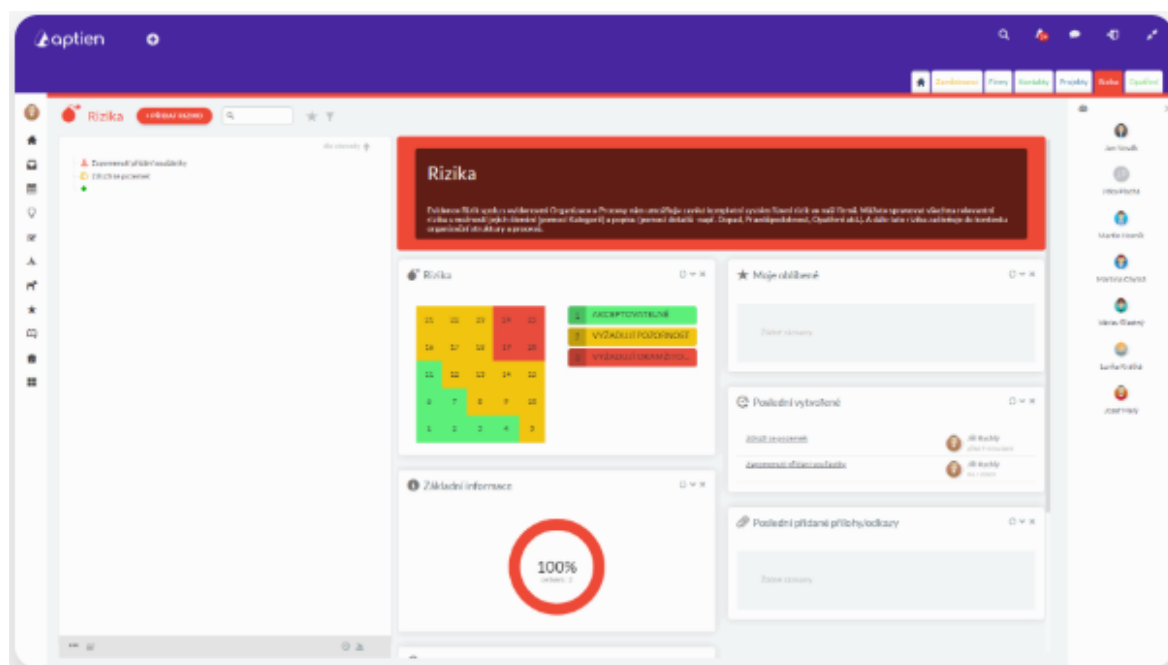
Aptien je moderní softwarové řešení zaměřené na efektivní řízení rizik v organizacích různých velikostí a odvětví. Jeho hlavním cílem je usnadnit správu rizik prostřednictvím centralizace dat, automatizace procesů a zajištění přehledné vizualizace klíčových informací. Tento nástroj umožňuje organizacím identifikovat, hodnotit a řídit rizika v souladu s jejich specifickými potřebami, což z něj činí univerzální platformu pro risk management.[51]

Centrálním prvkem je katalog rizik, který slouží jako komplexní databáze identifikovaných hrozeb. Každé riziko je detailně popsáno v rizikové kartě, obsahující informace o jeho zdroji, pravděpodobnosti výskytu, dopadu a navrhovaných opatřeních. Toto umožňuje systematické sledování a aktualizaci informací o rizicích.[51]

Důležitou součástí systému je mapa rizik, která vizuálně reprezentuje rizika podle jejich dopadu a pravděpodobnosti. Tato funkce pomáhá manažerům rychle identifikovat prioritní oblasti vyžadující okamžitou pozornost. Aptien také podporuje flexibilní kategorizaci rizik, což umožňuje přizpůsobení metodiky specifickým potřebám organizace.[52]

Systém dále umožňuje správu nápravných a preventivních opatření, včetně plánování a sledování jejich realizace. Součástí je také registr incidentů a procesů, které mohou být zdrojem potenciálních rizik. Tyto funkcionality společně přispívají k efektivnímu snižování identifikovaných hrozeb a celkovému zlepšení risk managementu v organizaci.[51]

Klíčovým prvkem je možnost integrace s dalšími aplikacemi prostřednictvím API rozhraní, což zajišťuje jeho snadné propojení s existujícími systémy organizace (plánování podnikových zdrojů nebo řízení vztahů se zákazníky). Tato vlastnost zvyšuje jeho použitelnost v různých provozních prostředích.[52]



Obrázek 22 Ukázka prostředí softwaru APTIEN

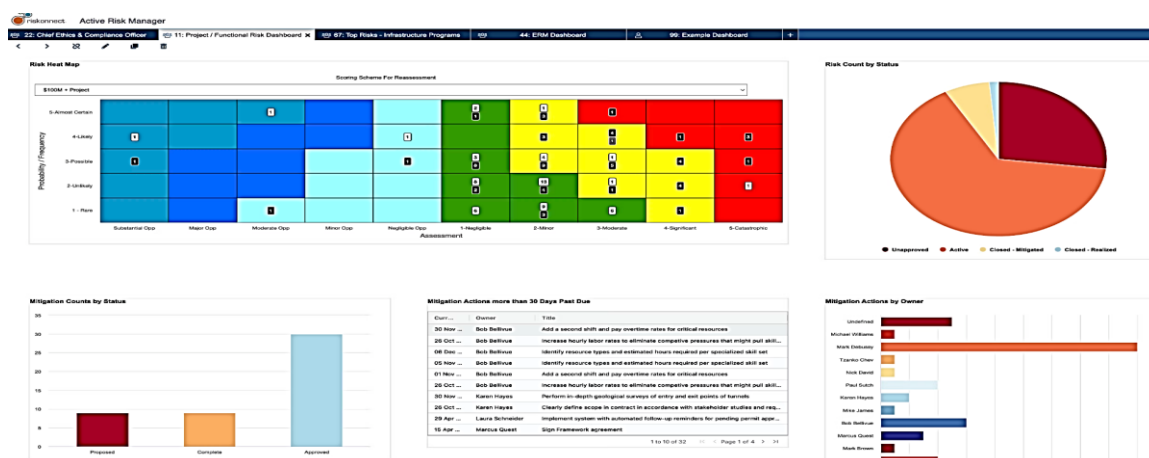
(zdroj:[52])

Active Risk Manager

Active Risk Manager je sofistikovaný softwarový nástroj vyvinutý společností Riskconnect, který se zaměřuje na řízení rizik v projektech, programech a na podnikové úrovni. Jeho hlavním cílem je identifikovat, hodnotit a řídit rizika s využitím pokročilých analytických nástrojů.[53]

Hlavní funkcionalita je založena na integraci dat z různých částí organizace, což umožňuje získat komplexní přehled o rizicích. Software nabízí vizualizační techniky, jako jsou teplotní mapy rizik a „Bow Tie“ analýza (grafické znázornění příčin a následků), které pomáhají pochopit souvislosti mezi riziky a jejich dopady. Důležitou funkcí je také simulace Monte Carlo, která modeluje různé scénáře vývoje projektů na základě pravděpodobnosti výskytu rizikových událostí.[53]

Mezi hlavní výhody patří jeho schopnost automatizovat celý proces řízení rizik, což umožňuje organizacím efektivně spravovat rizika bez nutnosti manuálního zásahu, čímž se výrazně snižuje časová náročnost a minimalizují chyby způsobené lidským faktorem. Software podporuje standardy jako ISO 31000 nebo COSO (standard pro hodnocení a řízení interních kontrol) [53]



Obrázek 23 Ukázka prostředí softwaru Active Risk Manager

(zdroj:[54])

Čtvrtá kapitola, se zabývá teoretickými základy analýzy rizik, jejími klíčovými pojmy (například riziko, scénář, pravděpodobnost, dopad, aktivum) a představuje hlavní mezinárodní normy v oblasti řízení rizik (ISO 31000, ISO/IEC 31010). Dále podrobně popisuje nejčastěji používané metody analýzy rizik a přehled dostupných softwarových nástrojů, které umožňují efektivní identifikaci, hodnocení a řízení rizik v organizacích.

II PRAKTICKÁ ČÁST

5 ZAVEDENÍ CERTIFIKACE TISAX

Myšlenka implementace toho standardu vznikla začátkem roku 2024, kdy společnost dostala nabídku na rozvoj nových projektů od dvou klíčových hráčů na trhu s brzdovými systémy a komponenty. Příchod těchto dvou nových zákazníků, a především dynamická situace v oblasti informační bezpečnosti tak byly hlavními důvody vzniku toho projektu, který měl za cíl implementovat standard TISAX tak, aby společnost mohla prokázat svou způsobilost působení v dodavatelském řetězci automobilového průmyslu. Druhým důvodem je skutečnost, že si stávající zákazníci začali vyžadovat platnost tohoto standardu a bez něj by společnost ztratila většinu svých velkých zákazníků a prakticky by nemohla dále fungovat.

5.1 Představení společnosti Lisi Automotive Form a.s.

Původní česká společnost byla založena v roce 1966, přičemž její výrobní program byl orientován na produkci kovových komponent, zejména pro automobilový průmysl. Výrobní proces byl realizován prostřednictvím vysoce specializované technologie tváření kovů za studena na českých tvářecích lisech. V roce 1970 došlo k rozšíření výrobních kapacit o druhý závod v Koryčanech, který se zaměřoval na kovoobrábění. V reakci na rostoucí požadavky automobilového průmyslu byl závod doplněn o sekci výstupní kontroly a expediční sklad.[55]

Zásadní transformace nastala v roce 2004, kdy většinový podíl společnosti odkoupila francouzská korporace Lisi Group. Česká společnost Form a.s. se tak stala součástí divize automotive této nadnárodní skupiny, která je organizačně rozdělena do tří hlavních divizí:

- Automotive (komponenty pro automobilový průmysl),
- Aerospace (komponenty pro letecký průmysl)
- Medical (chirurgické nástroje a ortopedické implantáty).[55]

V rámci restrukturalizace byla česká společnost rozdělena do tří lokalit. Vedení společnosti a administrativní zázemí sídlilo v Brně, lisovna a provoz fosfátovací linky byly umístěny v Čejči, zatímco obrobna, expedice a výstupní kontrola se nacházely v Koryčanech. Vzhledem k logistické náročnosti přesunů polotovarů mezi jednotlivými provozy bylo rozhodnuto o konsolidaci všech výrobních aktivit do jednoho místa. Tento proces byl zahájen v roce 2009 výstavbou nového areálu v Čejči, kam byla následně přesunuta veškerá výroba i administrativní zázemí. V roce 2018 došlo k dalšímu rozšíření prostor obrobny, výstupní kontroly a expedice.[55]

Současné produktové portfolio společnosti je primárně zaměřeno na výrobu vodících čepů pro brzdové systémy. Výrobní kapacity závodu v Čejči pokrývají přibližně 35 % celosvětové produkce těchto komponentů, které jsou dodávány prakticky všem významným automobilkám. Lze tedy konstatovat, že každý třetí automobil na světě obsahuje některý z produktů této společnosti.[55]



Obrázek 24 Závod společnosti Lisi automotive v Čejči

(zdroj:[23])



Obrázek 25 Ukázka stěžejního produktu

(zdroj:[23])

6 METODIKA PRO ZPRACOVÁNÍ PROJEKTU

Cílem této kapitoly, je zpracovat kompletní metodiku, která obsáhne všechny body zadání této diplomové práce a bude využitelná v praxi při řešení skutečného projektu, realizovaného v mém současném zaměstnání.

Na základě znalostí získaných ve svém zaměstnání a zároveň i využitých při psaní bakalářské práce, byl pro splnění hlavního cíle této diplomové práce zvolen přístup vycházející z projektového řízení a moderní metodologie Lean Six Sigma, která se používá pro zlepšení procesů a kvality výrobků zejména ve výrobních podnicích.

6.1 Východiska metodiky

Základní východiska této metodologie, se opírají o strukturovaný přístup, který k řešení konkrétních problémů nebo inovací procesu, přistupuje ve formě jednotlivých projektů, které jsou rozděleny na 5 fází, z nichž každá má jasně vytyčený obsah.

Konkrétní metoda, která se v rámci Lean Six Sigmy používá, se nazývá DMAIC a je složením ze slov: Define, Measure, Analyze, Improve a Control, kdy překlad těchto slov jasně udává záměr jednotlivých fází. Toto členění do jednotlivých fází poskytne základní rámec, do kterého budou implementovány všechny náležitosti požadované katalogem VDA ISA, které jsou nezbytné pro získání certifikace TISAX. V níže uvedené tabulce jsou stručně popsány jednotlivé kroky dle originální metodiky.

Tabulka 16 Popis kroků metody DMAIC

Fáze	Popis
Define (Definuj)	Definovat záměr a cíl projektu
Measure (Změř)	Sběr a analýza informací, stanovení ukazatelů pro měření účinnosti
Analyze (Analyzuj)	Analýza rizik a dat, na jejímž základě budou navrženy vhodné protiopatření.
Improve (Zlepši)	Implementace změn, nezbytných k dosažení stanovených cílů
Control (Kontroluj)	Nastavení kontrolních mechanismů pro stabilizaci nového stavu.

(zdroj:[23])

Shrnutí cílů metodiky

V průběhu tvorby této diplomové práce se postupně přidávali další a další cíle, proto pro ucelený přehled a orientaci, je v následující tabulce shrnutí hlavních cílů stanovených v zadání, a dílčích cílů, které musí vytvořená metodika splňovat. Cíle jsou řazeny chronologicky, dle předpokládaného naplnění spolu s fázemi projektu, která jim bude věnována.

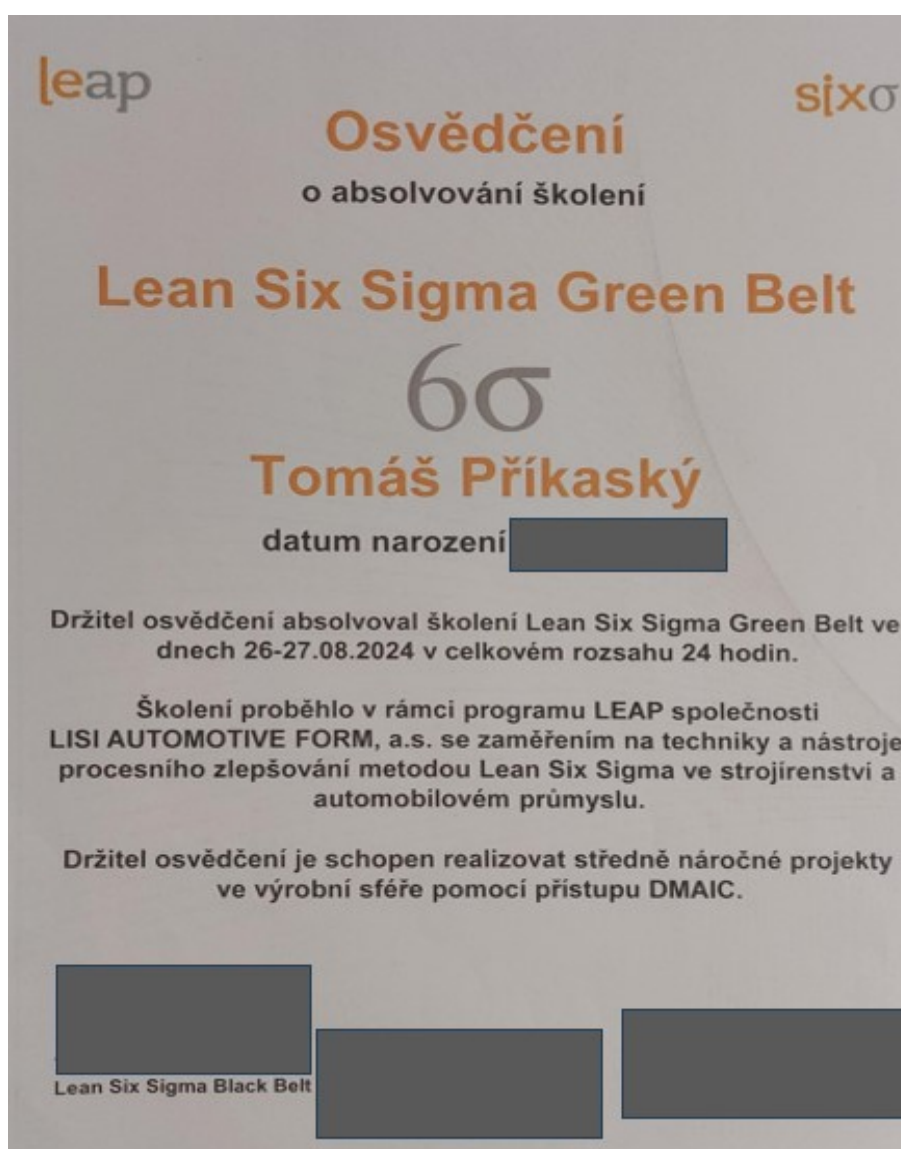
Tabulka 17 Shrnutí cílů metodiky

Cíl	Popis	Fáze
Zpracovat metodiku pro	Zpracovat postup, který je použitelný pro získání certifikace TISAX.	DMAIC (všechny)
Zpracovat analýzu rizik ve vybraném podniku	Analýza současného stavu, který musí být změněn, z důvodu splnění specifikací certifikace TISAX	Analyze
Zpracovat analýzu rizik související s implementací	Analýza rizik, které mohou ovlivnit průběh získání certifikace TISAX	Analyze
Navrhnout vhodná opatření	Navrhnout vhodné opatření, které budou řešit rizika a problémy	Improve
Výběr nejvhodnější varianty opatření pro zabezpečení informační bezpečnosti	Výběr nejvhodnější varianty s pomocí softwaru MC&S2 analyzer. Následně prověření související diplomové práce, a otestování nového softwaru vyvíjeného pro potřeby univerzity.	Improve
Prohloubení vědomostí získaných při zpracování bakalářské práce	Adaptace metodologie Lean Six sigma pro konkrétní problém a oblast informační bezpečnosti.	DMAIC (všechny)
Splnění podmínky získání profesní certifikace	Dokončení zaškolovacího procesu v rámci splnění podmínek nezbytných pro dokončení certifikace.	DMAIC (všechny)

(zdroj:[23])

Profesní certifikace Six Sigma

Proces certifikace obvykle zahrnuje teoretické školení a praktickou aplikaci metodologie na reálných projektech. Ačkoli formální certifikace není nutnou podmínkou pro využívání nástrojů Six Sigma, její získání poskytuje hlubší odborné znalosti a zvyšuje důvěryhodnost v profesním prostředí. Certifikace zahrnuje různé úrovně odbornosti rozlišované ve formě „pásů“: Bílý pás poskytuje základní přehled bez nutnosti předchozích zkušeností, žlutý pás je určen pro členy týmů podílejících se na zlepšování procesů, zelený pás připravuje projektové manažery na samostatné vedení optimalizačních projektů pomocí DMAIC a černý pás je určen pro experty řídící komplexní projekty a mentorující ostatní.[6]



Obrázek 26 Profesní certifikace Lean Six Sigma

(zdroj:[23])

6.2 Obsah metodiky

Hlavní metodika je rozdělena do 5 fází (etap), kterou jsou z originální metodologie adaptovány na problematiku související s tématem a cíli této diplomové práce. Jednotlivé fáze postupu jsou rozvedeny v následujících tabulkách.

Define

Tabulka 18 Popis I. etapy Define

Dílčí kroky	Popis
Stanovení cíle projektu	Určení cílů, kterých má projekt dosáhnout
Stanovení rozsahu projektu	Určení hranic projektu, aby nedošlo k jeho zacyklení
Stanovení projektového týmu	Určení členů projektového týmu a zájmových osob, kterých se tento projekt týká a bude si vyžadovat jejich zapojení
SWOT analýza	Analýza vnitřních a vnějších faktorů projektu
Validace vedením společnosti	Oficiální potvrzení z řad nejvyššího vedení společnosti, že projekt schválený a může začít samotná realizace

(zdroj:[23])

Measure

Tabulka 19 Popis II. etapy Measure

Dílčí kroky	Popis
Stanovení ukazatelů	Stanovení ukazatelů, které budou popisovat aktuální stav a na základě kterých bude možné posuzovat stav budoucí.
Stanovení cílové úrovně AL	Určení nezbytné úrovně certifikace TISAX, která je třeba dosáhnout, na základě těchto informací proběhne analýza rizik.

(zdroj:[23])

Analyze

Tabulka 20 Popis III. etapy Analyze

Dílčí kroky	Popis
Metodika pro analýzu rizik	Zpracování metodiky pro analýzu rizik v softwaru RISKAN. V rámci této metodiky bude přímo zpracována i analýza rizik, které by potenciálně mohli ohrozit průběh, realizaci a naplnění cílů projektu.
Analýza rizik v kontextu certifikace TISAX	Tato analýza bude vycházet z požadavků pro příslušnou úroveň AL, která byla stanovena v přechozím kroku „Measure“. Pro tuto analýzu bude použita metoda checklistu, který bude zpracován na základě požadavků, které vyplívají z příručky VDA ISA, jenž definuje podmínky, které je nezbytné splnit pro získání certifikace TISAX.
Vyhodnocení	Vyhodnocení výsledků provedených analýz

(zdroj:[23])

Improve

Tabulka 21 Popis IV. etapy Improve

Dílčí kroky	Popis
Návrh opatření	Návrh opatření, které budou řešit rizika vyláhané z analýz, realizovaných v předchozím kroku „Analyze“. Jednoduché opatření budou řešena přímým přístupem, u složitějších opatření, kde bude k dispozici vícero variant, bude využit software MC&S2 analyzer.
Metodika pro multikriteriální hodnocení	Zpracování metodiky pro multikriteriální hodnocení v softwaru MC&S2 analyzer
Aplikace metodiky	Vyhodnocení jednotlivých variant nápravných opatření.
Shrnutí nákladů projektu	Shrnutí nákladů projektu v kontextu stanovených kompromisních variant.

Implementace nápravných opatření	Určení harmonogramu realizace s pomocí Gantova diagramu
Ukázky z implementace	Fotodokumentace související s projektem

(zdroj:[23])

Control

Tabulka 22 Popis V. etapy Control

Dílčí kroky	Popis
Vyhodnocení přínosu	Na základě stanovených ukazatelů z etapy „Measure“, vyhodnotit přínos celého projektu.
Stabilizace nového stavu	Nastavení kontrolních opatření, nezbytných k udržení nového stavu.
Doporučení pro další rozvoj	Vyhodnocení možností, jakým způsobem by se projekt mohl rozvíjet do budoucna.

(zdroj:[23])

7 PROJEKT PŘÍPRAVY A IMPLEMENTACE CERTIFIKACE TISAX

Sedmá kapitola se zabývá již samotným projektem ve společnosti Lisi automotive Form a.s. a vychází z teoretických informací první částí diplomové práce a metodiky zpracované v šesté kapitole. Ta je postavena na základech metodologie Lean Six Sigma, požadavků VDA ISA v kontextu certifikace TISAX, vlastních zkušenostech, projektovém řízení, softwaru podporující analýzu rizik a multikriteriální hodnocení variant. V rámci projektu jsou zakomponovány i jednotlivé body oficiálního zadání diplomové práce.

7.1 Define

Define představuje první fázi metodologie DMAIC. Jejím cílem je přesně definovat problém, stanovit cíle projektu a vytvořit pevný základ pro jeho úspěšnou realizaci. V praxi jde o vypracování projektového záměru, který se v rámci metodologie nazývá projekt charter, který je vypracovaný v následující podkapitole.

7.1.1 Stanovení cílů a rozsahu projektu

Tabulka 23 Project Charter

Projekt Implementace standardu TISAX	
Datum zahájení	31.3.2024
Datum ukončení	31.3.2025
Cíle projektu	• Provést přípravu společnosti na certifikaci dle standardu TISAX. • Získat certifikaci a díky ní nové zákazníky • Zvýšit důvěryhodnost společnosti v dodavatelském řetězci • Získání je nezbytné, pro další působení společnosti v automobilovém průmyslu.
V rozsahu projektu (In scope)	• Změny v procesech v kontextu TISAXU • Školení zaměstnanců • Fyzické zabezpečení závodu v Čejči

Mimo rozsah projektu (Out of scope)	• Změny týkající se jiných certifikací • Změny IT struktury (realizovány a řízeny korporátním IT oddělením) • Procesy a aktivity, které nejsou součástí ISMS nebo nejsou relevantní pro TISAX požadavky
--	---

(zdroj:[23])

7.1.2 Určení projektového týmu a zainteresovaných osob

Určení zainteresovaných osob a projektového týmu je klíčovým krokem v rámci projektového řízení. Jasné vymezení těchto rolí zajišťuje, že každý účastník projektu zná své odpovědnosti, pravomoci a očekávání, což usnadňuje komunikaci, koordinaci a efektivní řešení problémů. Všichni účastníci svým podpisem stvrzují svou účast na projektu.[55]

Tabulka 24 Složení projektového týmu

Projektový tým		
Funkce	Jméno a příjmení	Seznámen s se svou účastí
Projektový manažer – black belt	Zaměstnanec A	Ano
Projektový manažer – green belt	Bc. Tomáš Příkaský	Ano
IT specialista Čejč	Zaměstnanec B	Ano
Manažer lidských zdrojů	Zaměstnanec C	Ano
Manažer logistiky	Zaměstnanec D	Ano
Manažer bezpečnosti a environmentu	Zaměstnanec E	Ano
Manažer APU Lisovna	Zaměstnanec F	Ano
Manažer APU Obrobna	Zaměstnanec G	Ano
Manažer APU kontrola	Bc. Tomáš Příkaský	Ano
Manažer financí	Zaměstnanec H	Ano
Obchodní ředitel	Zaměstnanec CH	Ano

Manažer technologie	Zaměstnanec I	Ano
IT manažer (korporátní)	Zaměstnanec J	Ano
IT team (korporátní)	Zaměstnanec K	Ano
Generální ředitel	Zaměstnanec L	Ano

(zdroj:[23])

Vzhledem k povaze a rozsahu projektu, jsou v projektovém týmu zahrnuti vedoucí pracovníci ze všech jednotlivých struktur společnosti. Tito zaměstnanci jsou zároveň tzv stakeholdery, tj. osoby, které jsou zapojeny do projektu, ovlivňují jeho průběh a mají zájem na splnění jeho dílčích cílů. Ze své podstaty, se informační bezpečnost dotýká každého zaměstnance společnosti.

7.1.3 SWOT analýza

Tabulka 25 SWOT analýza projektu

	Pozitivní	Negativní
Vnitřní faktory	Silné stránky • Silné korporátní zázemí • Interní IT specialisti • Platná certifikace ISO 27001	Slabé stránky • Nedostatečné zapojení zejména pracovníků ve výrobě • Náročnost na dokumentaci a důkazy
Vnější faktory	Příležitosti • Získat klíčové zákazníky • Udržet stávající zákazníky • Zvýšit hodnotu společnosti	Hrozby • Ztráta zákazníků a důvěry • Spolupráce mezi lokálními a korporátními specialisty • Nepřijetí zaměstnanci ve výrobě

(zdroj:[23])

7.2 Measure

Etapa Measure představuje druhou fázi projektu, která se soustředí na získávání informací a dat týkajících se procesů určených ke zlepšení. V této fázi je kladen důraz na shromáždění údajů nezbytných pro detailní pochopení fungování jednotlivých procesů ve společnosti, požadavků zákazníků, nebo specifikací od dodavatelů. Hlavním cílem této etapy bude v kontextu tématu diplomové práce vyhodnotit, jakou úroveň certifikace AL společnost potřebuje získat a následně zvolit vhodné ukazatele pomocí níž lze stávající úroveň procesu popsat a v poslední fázi Control vyhodnotit.

7.2.1 Stanovení cílové úrovně TISAX

Stanovení cílové úrovně certifikace je odvozeno z příručky VDA ISA. Prvním krokem je stanovení rozsahu hodnocení. Jsou zde rozlišeny tři základní moduly:

- Informační bezpečnost (relevantní pro všechny organizace)
- Ochrana prototypů (relevantní pro Subdodavatele vývojových dílů)
- Ochrana osobních údajů (pro zpracovatele osobních údajů dle článku 28 GDPR)[10]

Uchazeč o certifikaci si vybírá, v kterých modulech plánuje certifikaci získat. Moduly jsou rozčleněny do 12 oblastí uvedených v následující tabulce (1–6 informační bezpečnost, 7-10 ochrana prototypů, 11-12 ochrana osobních údajů). Modul týkající se informační bezpečnosti je povinný pro všechny žadatele, zbylé jsou doplňkové v závislosti na povaze výrobního procesu, nebo orientaci společnosti. Každá oblast hodnocení má uvedenou i požadovanou úroveň certifikace, které je potřeba dosáhnout AL2, nebo AL3.[10]

Tabulka 26 Moduly a dílčí oblasti hodnocení certifikace TISAX

	Oblast hodnocení	Popis	Úroveň hodnocení	
1	Info high	Nakládání s informacemi s vysokou potřebou ochrany	AL 2	
2	Info very high	Nakládání s informacemi s velmi vysokou potřebou ochrany		AL 3

3	Confidential	Nakládání s informacemi s vysokou potřebou ochrany v rámci zachování důvěrnosti (přístup k důvěrným informacím)	AL 2	
4	Strictly confidential	Nakládání s informacemi s velmi vysokou potřebou ochrany v rámci zachování důvěrnosti (přístup k přísně důvěrným informacím)		AL 3
5	High availability	Nakládání s informacemi s vysokou potřebou ochrany v rámci jejich dostupnosti (vysoká dostupnost informací)	AL 2	
6	Very high availability	Nakládání s informacemi s velmi vysokou potřebou ochrany v rámci jejich dostupnosti (velmi vysoká dostupnost informací)		AL 3
7	Proto parts	Ochrana prototypových dílů a součástí		AL 3
8	Proto vehicles	Ochrana prototypů vozidel		AL 3
9	Test vehicles	Manipulace se zkušebními vozidly		AL 3
10	Proto events	Ochrana prototypů při akcích a filmování nebo fotografování		AL 3
11	Data	Ochrana údajů podle článku 28 („zpracovatel“) obecného evropského nařízení o ochraně osobních údajů (GDPR)	AL 2	
12	Special data	Ochrana údajů podle článku 28 („zpracovatel“) obecného evropského nařízení o ochraně osobních údajů (GDPR) se zvláštními kategoriemi osobních údajů ve smyslu článku 9 GDPR		AL 3

(zdroj:[10])

Pro určení bylo nezbytné analyzovat související procesy v organizaci s využitím znalostí jednotlivých vlastníků procesu. Výstup této analýzy je následující matice:

Tabulka 27 Matice hodnocení Assessment level

Matice hodnocení úrovně AL v Čejči												
	1	2	3	4	5	6	7	8	9	10	11	12
AL2	ANO		ANO		ANO						ANO	
AL3		NE		NE		NE	NE	NE	NE	NE		NE

(zdroj:[23])

Z matice vyplývá, že požadovaná úroveň certifikace bude AL2. V případě že by jakákoliv oblast spadala do oblasti AL3, musel by celý certifikační proces směřován tímto směrem.

7.2.2 Stanovení vhodných ukazatelů KPI a PI

Cílem této podkapitoly je definovat klíčové ukazatele (KPI), které objektivně popisují aktuální úroveň informační bezpečnosti společnosti a umožní měřit pokrok v procesu přípravy na certifikaci TISAX. Výběr vhodných metrik musí reflektovat požadavky katalogu VDA ISA a zároveň být prakticky měřitelný v kontextu organizace. Ukazatele byly v kontextu tohoto projektu zvoleny následovně.

Počet nesplněných požadavků VDA ISA

Tento ukazatel bude vhodný pro udržení certifikace, která ze své podstaty počítá se splněním všech požadavků, aby mohla být společnosti udělena.

Absolvovaná školení na osobu/rok

Díky tomuto ukazateli, bude možné při recertifikačních auditech prokázat proškolení personálu v kontextu informační bezpečnosti. Aktuálně má společnost pouze 3 základní školení, které se pouze okrajově dotýkají zkoumané problematiky.

Počet kusů v knize objednávek

Počet objednaných kusů je klíčovým ukazatelem pro kalkulaci přínosu a případné návratnosti v projektu implementace standardu TISAX. Platí zde přímá úměra mezi objednanými kusy a z toho plynoucím ziskem společnosti.

Počet klíčových zákazníků

Ukazatel zaměřený na sledování získávání nových klíčových zákazníků, které implementace standardu přinese. Za klíčového zákazníka se považuje zákazník, který má zájem alespoň o dva nové projekty, s předpokládanou dobou trvání delší jak 3 roky, významně se podílí na tržbách a zisku a je významný z hlediska reference, nebo prestiže.

Počet projektů

Ukazatel, který sleduje počet nově získaných projektů, oproti výchozímu stavu před získáním certifikace.

Tabulka 28 Shrnutí ukazatelů stanovených pro sledování přínosu projektu

Ukazatel	Jednotka	Aktuální stav	Předpokládaný cílový stav
Počet nesplněných požadavků VDA ISA	Počet	N/A	0
Absolvovaná školení na osobu za kalendářní rok	Počet / rok	1	2
Počet kusů v knize objednávek na kalendářní rok	Počet kusů	98 526 300	102 526 300
Počet klíčových zákazníků	Počet celkem	8	10
Počet projektů	Počet celkem	105	112

(zdroj:[23])

7.3 Analýze

Třetí fáze Analýze, se zaměřuje na analytickou část projektu. Skládá se z třech dílčích kroků, kdy prvním krokem bude zpracovat metodiku pro analýzu rizik v softwarovém programu Riskan, kdy analýza bude zaměřena na rizika, které by potencionálně mohli ohrozit průběh implementace. V rámci zpracování metodiky, bude zároveň provedena i samotná analýza. Druhým krokem je provedení analýza rizik v kontextu certifikace TISAX, která bude realizována formou checklistu. Na základě výstupů z těchto dvou analýz, budou následně navrženy vhodná opatření.

7.3.1 Metodika Analýzy rizik

Metodika je obecně použitelná, a aplikovatelná i pro osoby, které nemají praktické zkušenosti.

1. Identifikace aktiv a hrozeb

Prvním krokem je identifikace aktiv a hrozeb, které jsou spojeny s konkrétním příkladem.

Tabulka 29 Souhrn aktiv a hrozeb, použitých v metodice analýzy rizik

Skupina	Dílčí aktivum	Hrozba
Lidské zdroje	Projektový tým	Odchod klíčového člena
	Vedení projektu	Nedostatečná podpora managementu
Dokumentace	Projektový plán	Nejednoznačnost plánu
Technologie	Nástroje pro řízení projektu	Ztráta dat
	Komunikační platformy	Kybernetický útok na platformy
Finance	Rozpočet	Překročení
	Finanční rezerva	Nemožnost získat další prostředky
Stakeholderi	Podpora a vedení	Neochota řešit eskalace
	Zákazníci a uživatelé	Odmítnutí výstupu projektu
Procesy	Metodika řízení projektu	Nedodržování postupu

	Kontrolní mechanismy	Opomenutí klíčových bodů
--	----------------------	--------------------------

(zdroj:[23])

2. Vytvoření nového subjektu

Pro tento subjekt budou v systému spravována data, především analýzy rizik, profily, aktiva, hrozby a další relevantní informace.

- V levém menu klikněte na tlačítko „Správa subjektů“.
- Stiskněte tlačítko „Nový“.
- Následně zadejte název a popis nového subjektu.

	Uložit	Tisk	Zavřít
Název	TISAX		
Popis			

Obrázek 27 Vytvoření subjektu

(zdroj:[23])

3. Vytvoření analýzy rizik

- V levém menu klikněte na tlačítko „Analýza rizik“.
- Stiskněte tlačítko Nová.
- Vyberte subjekt.
- Zadejte Název analýzy rizik a charakteristiku (popis, hranice, účel analýzy).

Analýza rizik
Na stránce byly provedeny změny, které nebyly uloženy.

	Uložit	Tisk	Zavřít
Subjekt	Implementace TISAXU		
Název	Analýza rizik DP Příkaský		
Charakteristika	Analýza rizik související s projektem implementace standardu TISAX		

Obrázek 28 Vytvoření analýzy rizik

(zdroj:[23])

4. Vytvoření profilu analýzy rizik

- V nově vytvořené analýze rizik, zvolte v sekci profilu „Nový“.
- Zadejte název a rozsahy hodnot aktiv, pravděpodobností hrozeb zranitelností, tyto rozsahy jsou editovatelné. Pro tento konkrétní případ byly zvoleny následující hodnoty rozsahu: aktiva zev (1-4), hrozby zev (1-4), zranitelnost zev (1-4).
- Seznamy aktiv a hrozeb prozatím zůstanou prázdné, budou vytvořeny v následující části metodiky na základě prvotní identifikace.
- Posledním krokem je zvolení maximální hodnoty, dolní meze červené hodnoty a dolní meze oranžové hodnoty. Maximum spočítejte na základě vzorce (max. hodnota aktiva * max. hodnota hrozby * max. hodnota zranitelnosti. V případě hodnot, které byly zvoleny v této metodice, je to $4*4*4 = 64$. Obě meze stanovuje uživatel subjektivně, na základě nich se budou podbarvovat výsledky.
- Poté klikněte na tlačítko „uložit“.[56]

Profil

Na stránce byly provedeny změny, které nebyly uloženy.

Uložit		Tisk	Zavřít
Analýza	* Analýza rizik DP Příkaský		
Název	* Profil TISAX		
Aktiva			
Hrozby			
Rozsah hodnot aktiv	* aktiva - Zev		
Rozsah pravděpodobností hrozeb	* hrozby - Zev		
Rozsah zranitelností	* zranitelnost - Zev		
Dílčí hodnoty aktiv			
Dílčí hodnoty hrozeb			
Maximální hodnota	* 64		
Dolní mez červené	* 42		
Dolní mez oranžové	* 21		

Obrázek 29 Vytvoření profilu analýzy rizik

(zdroj:[23])

5. Přiřazení Aktiv a Hrozeb

Přiřazení aktiv a hrozeb, které byly identifikovány v první kroku této metodiky se provádí opět na kartě analýzy rizik. Jako první označte checkbox s příslušným profilem analýzy. Pro přidání a editaci aktiv zvolíte tlačítko „Otevřít aktiva“, pro přidání a editaci hrozeb zvolíte tlačítko „Otevřít hrozby“. Postup a zákonitosti je stejný pro oba případy, proto bude dále popsán pouze na části týkající se aktiv.[56]

Analýza rizik

Obrázek 30 Nabídka panelu analýza rizik

(zdroj:[23])

Nyní je několik možností, jak jednotlivé prvky přidávat. První možností je přidávat jednotlivé prvky po jednom pomocí tlačítka „Editovat“. Jednotlivé prvky musí být číslovány od 1, pokud se jedná o rodiče. V případě že jde o potomka (podskupinu), je označení 1.1. Výhodnější je ovšem využít možnost „Textový editor“, která umožňuje sepsat jednotlivé prvky dohromady a pak je hromadně uložit.[56]

Přecházet	Uložit změny	Detail	Tisk	Zavřít
Editovatelný seznam:				
1.	Lidské zdroje			
2.	1.1 Projektový tým			
3.	1.2 Vedení projektu			
4.	Dokumentace			
5.	2.1 Projektový plán			
6.	Technologie			
7.	3.1 Nástroje pro řízení softwaru			
8.	3.2 Komunikační platformy			
9.	Finance			
10.	4.1 Rozpočet			
11.	4.2 Finanční rezerva			
12.	Stakeholdeři			
13.	5.1 Podpora a vedení			
14.	5.2 Zákazníci a uživatelé			
15.	Procesy			
16.	6.1 Metodika řízení projektu			
17.	6.2 Kontrolní mechanismy			

Obrázek 31 Seznam Aktiv

(zdroj:[23])

Editace seznamu hrozeb profilu "Analýza rizik DP Příkaský"

Přečíslovat	Uložit změny	Detail	Tisk	Zavřít
-------------	--------------	--------	------	--------

Editovatelný seznam:

1.	Odchod klíčového člena
2.	Nedostatečná podpora managementu
3.	Nejednoznačnost plánu
4.	Ztráta dat
5.	Kybernetický útok
6.	Překročení rozpočtu
7.	Nemožnost získat další prostředky
8.	Neochota řešit eskalace
9.	Odmítnutí výstupu projektu
10.	Nedodržování postupu
11.	Opomenutí klíčových bodů

Obrázek 32 Seznam hrozeb

(zdroj:[23])

6. Zadání hodnot do profilu

Zadání hodnot je posledním krokem v procesu analýzy rizik prostřednictvím softwarového nástroje Riskan. Jako první přejděte na bočním informačním panelu na záložku „Profily“, kde označíte příslušný profil a stisknete tlačítko „Otevřít profil“.

Riskan - Rizikový kalkulátor

Nový	Detail	Smazat	Excel
Export XML	Kopírovat profil	Otevřít aktiva	Otevřít hrozby
Otevřít profil	Tisk		

Profily

F	F	F
Analýza	Název profilu	Mezní hodnoty
☐ ANALÝZA POŽÁRNÍCH RIZIK PANELOVÝCH DOMŮ - Analýza rizik	ANALÝZA POŽÁRNÍCH RIZIK PANELOVÝCH DOMŮ - Profil	31 - 61 - 100
☒ Analýza rizik DP Příkaský	Analýza rizik DP Příkaský	21 - 42 - 64

Obrázek 33 Zadávání hodnot

(zdroj:[23])

Pro další postup je třeba zadat několik údajů: nejprve se určí hodnoty aktiv, které se zapisují do řádku označeného jako „hod.“ pod jednotlivými čísly aktiv. Dále je nutné vyplnit pravděpodobnost výskytu hrozeb, což se provádí ve sloupci „pra.“ napravo od názvů hrozeb. Nakonec se stanoví zranitelnost, která vyjadřuje vztah mezi konkrétním aktivem a hrozbou, a tato hodnota se zapisuje do pole, kde se protíná řádek dané hrozby se sloupcem příslušného aktiva. Po vyplnění uložte hodnoty tlačítkem „Uložit“.[56]

Vztahy mezi hrozbami a aktivy v projektovém řízení jsou často mnohvrstevnaté a překrývají se. Pro správné nastavení matice v nástroji Riskan je proto vhodné uvažovat, že:

- Většina hrozeb má dopad na více aktiv současně.
- Hodnoty zranitelnosti by měly být zadávány nejen pro „primární“ kombinace, ale i pro další relevantní propojení.
- Takový přístup zajistí realističtější a robustnější analýzu rizik, která lépe vystihuje skutečnou provázanost projektového prostředí.
- Příkladem může být odchod klíčového člena týmu. Tato skutečnost neohrozí pouze samotný projektový tým, ale může zásadně ovlivnit i vedení projektu, kvalitu projektové dokumentace, schopnost dodržovat metodiku nebo efektivitu kontrolních mechanismů.

Výsledkem je matice, zobrazená na následujícím obrázku.

		Akt.:																	
		Lid	Pro	Ved	Dok	Pro	Tec	Nás	Kom	Fin	Roz	Fin	Sta	Pod	Zák	Pro	Met	Kon	
		...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	
		1.	1.1	1.2	2.	2.1	3.	3.1	3.2	4.	4.1	4.2	5.	5.1	5.2	6.	6.1	6.2	
hod.:		2	2	1	2	2	1	1	1	2	2	0	3	2	3	2	0	2	
Hrozby		pra.:																	
1.	Odchod klíčového člena	2	3	3	1	1	1	0	0	0	0	0	0	0	0	1	1	1	
2.	Nedostatečná podpora mana ...	1	3	0	3	0	0	0	0	0	2	2	1	0	0	0	0	0	
3.	Nejednoznačnost plánu	1	0	0	0	3	3	0	0	0	0	0	0	0	0	2	2	0	
4.	Ztráta dat	1	0	0	0	0	0	3	3	0	0	0	0	0	0	0	0	0	
5.	Kybernetický útok	1	0	0	0	1	1	3	0	3	0	0	0	0	0	1	0	1	
6.	Překročení rozpočtu	1	0	0	0	0	0	0	0	0	3	3	0	0	0	0	0	0	
7.	Nemožnost získat další pr ...	0	2	2	1	0	0	0	0	0	3	0	3	0	0	1	1	0	
8.	Neochota řešit eskalace	2	3	3	2	0	0	0	0	0	1	1	0	3	3	0	1	1	0
9.	Odmítnutí výstupu projekt ...	3	0	0	0	0	0	0	0	0	0	0	0	3	0	3	0	0	0
10.	Nedodržování postupu	2	2	2	0	1	1	0	0	0	0	0	0	0	0	3	3	0	
11.	Opomenutí klíčových bodů	2	0	0	0	0	0	0	0	0	0	0	1	0	1	2	0	2	

Obrázek 34 Vyplněná matice pro výpočet rizika

(zdroj:[23])

Finální vizualizaci rizik provedete pomocí tlačítka „Výsledná rizika“. Riskan současně nabízí možnost stažení excelového souboru, z kterého je možné data vizualizovat ve formě grafů. Výsledky analýzy, který byla použita i jako vzor pro vypracování metodiku, budou

popsány v kapitole 7.3.3, který je zaměřena na vyhodnocení v rámci tohoto projektu. Celkem se jedná o 3 rizika.

		Akt.:																	
		Lid	Pro	Ved	Dok	Pro	Tec	Nás	Kom	Fin	Roz	Fin	Sta	Pod	Zák	Pro	Met	Kon	
		1.	1.1	1.2	2.	2.1	3.	3.1	3.2	4.	4.1	4.2	5.	5.1	5.2	6.	6.1	6.2	
		hod.:	2	2	1	2	2	1	1	1	2	2	0	3	2	3	2	0	2
Hrozby		pra.:																	
1.	Odchod klíčového člena	2	28	28	5	9	9	0	0	0	0	0	0	0	0	0	9	0	9
2.	Nedostatečná podpora mana ...	1	14	0	7	0	0	0	0	9	9	0	0	0	0	0	0	0	0
3.	Nejednoznačnost plánu	1	0	0	0	14	14	0	0	0	0	0	0	0	0	9	0	0	0
4.	Ztráta dat	1	0	0	0	0	0	7	7	0	0	0	0	0	0	0	0	0	0
5.	Kybernetický útok	1	0	0	0	5	5	7	0	7	0	0	0	0	0	5	0	5	0
6.	Překročení rozpočtu	1	0	0	0	0	0	0	0	14	14	0	0	0	0	0	0	0	0
7.	Nemožnost získat další pr ...	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8.	Neochota řešit eskalace	2	28	28	9	0	0	0	0	9	9	0	43	28	0	9	0	0	0
9.	Odmítnutí výstupu projekt ...	3	0	0	0	0	0	0	0	0	0	0	64	0	64	0	0	0	0
10.	Nedodržování postupu	2	19	19	0	9	9	0	0	0	0	0	0	0	0	28	0	0	0
11.	Opomenutí klíčových bodů	2	0	0	0	0	0	0	0	0	0	0	14	0	14	19	0	19	0

Obrázek 35 Výsledná rizika v softwaru Riskan

(zdroj:[23])

7.3.2 Analýza rizik TISAX

Tato kapitola řeší druhou část analýzy rizik, která je spjatá přímo s implementací TISAXU. Pro zpracování byla vybrána metoda checklistu, která byla podrobně popsána v teoretické části diplomové práce. Aby společnost mohla získat certifikaci, musí splňovat konkrétní kritéria. Checklist zabezpečí, že budou systematicky přezkoumány jednotlivé kategorie, které udává příručka VDA ISA.

Tabulka 30 Checklist pro kontrolu požadavků

Oblasti checklistu dle VDA ISA	Provedeno
Přípravná fáze a registrace	
Identifikace rozsahu ISMS (systému řízení bezpečnosti informací)	ANO
Definování hranic ISMS včetně všech relevantních systémů, procesů a lokalit	ANO
Výběr akreditovaného auditora/hodnotitele	ANO
Identifikace potřebných testovacích cílů (TISAX štítky)	ANO

Zpracování sebehodnocení pomocí dotazníku VDA ISA	ANO
Dokumentace ISMS a řízení rizik	
Dokumentovaná bezpečnostní politika organizace	ANO
Jasně definované bezpečnostní cíle informačního systému	ANO
Dokumentované role a odpovědnosti v rámci ISMS	ANO
Komplexní analýza rizik informační bezpečnosti	ANO
Plán zvládání rizik informační bezpečnosti	ANO
Definované a dokumentované bezpečnostní metriky a způsoby měření	ANO
Proces řízení incidentů informační bezpečnosti	ANO
Seznam informací vyžadujících ochranu včetně klasifikace	ANO
Implementace bezpečnostních opatření	
Bezpečnostní politiky a procedury	ANO
Organizace informační bezpečnosti	ANO
Bezpečnost lidských zdrojů	ANO
Správa aktiv	ANO
Řízení přístupu	ANO
Kryptografie	ANO
Fyzická bezpečnost a bezpečnost prostředí	ANO
Provozní bezpečnost	ANO
Bezpečnost komunikací	ANO
Vztahy s dodavateli	ANO
Řízení incidentů bezpečnosti informací	ANO
Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	ANO
Soulad s požadavky	ANO
Ochrana dat dle GDPR	
Implementace požadavků dle článku 28 GDPR (zpracování osobních údajů)	ANO
Dokumentované procesy pro ochranu osobních údajů	ANO
Technická a organizační opatření pro zajištění ochrany osobních údajů	ANO
Správa souhlasů se zpracováním osobních údajů	ANO

Specifické požadavky pro AL2	
Implementace opatření pro informace s vysokou potřebou ochrany	ANO
Opatření pro připojení třetích stran s vysokou potřebou ochrany (pokud relevantní)	ANO
Opatření pro ochranu osobních údajů dle článku 28 GDPR (pokud relevantní)	ANO

(zdroj:[23][10])

V rámci checklistu bylo nalezeno celkem 6 nálezů, které bude nutné řešit vhodnými protiopatřeními. Podrobný rozbor bude v následující podkapitole 7.3.3 spolu s riziky, které mohou ohrozit projekt implementace.

7.3.3 Vyhodnocení analýz rizik

V této kapitole jsou shrnuty rizika z analýzy rizik ohrožující proces implementace a analýzy rizik v kontextu získání certifikace. Jsou popsány v níže uvedené tabulce, spolu s číselným označením. Ke každému číslu bude zvoleno odpovídající nápravné opatření. V případě že se bude jednat o opatření, jehož řešení odpovídá definici složitého rozhodovacího problému (potřeba vyhodnocení vícero kritérií, která jsou často vzájemně konfliktní, a vyžadují strukturovaný přístup k nalezení optimálního řešení), bude realizováno pomocí softwaru MC&S2 analyzer. Ostatní opatření budou stanovena přímo hodnotitelem.

Tabulka 31 Shrnutí rizik

Rizika ohrožující proces implementace (Riskan)	Označení
Odmítnutí výstupu projektu zákazníky, nebo uživateli	I
Odchod klíčového člena projektu	II
Neochota řešit eskalace	III
Rizika ohrožující získání certifikace (Checklist)	
Nejednoznačné a nesourodé řízení přístupu do jednotlivých oblastí	IV
Chybějící certifikované skartovačky pro klasifikované dokumenty	V
Ve výrobě se vyskytují neaktuální dokumenty bez příslušné klasifikace	VI

Proces předávání a vracení hardwaru zaměstnancům	VII
Zabezpečení serverové místnosti	VIII
Zabezpečení přístupu z vnějšího prostředí	IX

(zdroj:[23])

Tyto rizika vyplívají z počáteční SWOT analýzy, analýzy rizik v softwaru Riskan a analýzy rizik zaměřené na získání nové certifikace. V další kapitole Improve, budou navrženy opatření k jejich eliminaci.

7.4 Improve

Čtvrtá fáze je zaměřena na implementaci změn, nezbytných k dosažení projektových cílů a opírá se o výstupy z přechozí kapitoly Analyze, která měla za cíl identifikovat rizika, ohrožující tento projekt.

7.4.1 Návrh opatření

Opatření se týkají rizik shrnutých v tabulce 31. K jednotlivým rizikům budou vybrána vhodná nápravná opatření

Tabulka 32 Seznam navrhovaných opatření

I	Odmítnutí výstupu projektu zákazníky, nebo uživateli
	U dodavatelů jde o riziko potencionální ztráty důvěryhodnosti, v případě neúspěšného absolvování certifikačního procesu (tj. nezískání certifikace). Nápravným opatřením je zpracování tohoto projektu, který byl realizován právě s cílem co nejlépe společnost připravit na získání certifikace.
	U uživatelů jde o zaměstnance společnosti, kteří by nemuseli tyto změny přijat a akceptovat, v nejhorším případě by mohli projekt dokonce i sabotovat.
	Nápravné opatření: Realizace školení zaměřeného na informační bezpečnost a význam certifikace pro zaměstnance a jejich zaměstnavatele.

	Školení musí být periodické minimálně 1x ročně pro stávající zaměstnance a pro nové zaměstnance při vzniku pracovního poměru. Hromadné školení bude realizováno externí společností před auditem TISAX a jednotlivý účastníci vyplní formulář J5120 (Prezenční listina), který lze použít jako důkaz o provedení, vstupní školení zajistí personální oddělení na základě materiálů poskytnutých externím dodavatel. Výběr externího dodavatele bude realizován prostřednictvím multikriteriální analýzy.
II	Odchod klíčového člena projektu
	Odchod klíčového člena projektu je rizikem u všech větších projektů. Problémem bývá zejména chybějící matice zastupitelnosti. V rámci tohoto projektu jsou všichni stakeholderi dlouholetými zaměstnanci společnosti, tudíž není riziko ukončení ve zkušební lhůtě. Nápravné opatření: Aktualizace stávajících matic zastupitelnosti (interní označení J4100) tak, aby každý stakeholder měl odpovídajícího zástupce. Revizi proveze provede projektový manažer.
III	Neochota řešit eskalace
	Společnost disponuje inovativním softwarovým systémem Fabrique, kde je možné eskalovat mezi jednotlivými úrovněmi (výroba, střední management, top management. Systém umožňuje delegovat konkrétní úkoly na konkrétní osoby spolu s časovým rozmezím pro splnění. Tento systém bude využit i v rámci tohoto projektu. Nápravné opatření: Hromadné online školení na správné používání vnitropodnikového systému. Toto školení musí obsahovat přesnou metodiku, jak eskalaci provádět, aby cílová osoba, ke které je případný problém eskalován byla včas a správně notifikována. Školení zabezpečí interní IT oddělení prostřednictvím metodiky distribuované přes platformu Outlook.
IV	Nejednoznačné a nesourodé řízení přístupu do jednotlivých oblastí

	Jednotlivé kanceláře a oddělení postrádají sledovatelnost přístupu. Chybí ucelená evidence, kde by bylo exaktně popsáno, kdo a do jakých prostor má přístup. Doposud byla distribuce přístupu v kompetenci příslušných vedoucích útvarů, nově toto zajistí manažer správy budov. Nápravné opatření: Výběr a implementace vhodného řešení pomocí multikriteriální analýzy. Výběr bude probíhat mezi dodavateli mechanického zabezpečení, nebo dodavateli řešení ve formě čipů a čteček. Zabezpečí projektový manažer.
V.	Chybějící certifikovaného skartovače pro klasifikované dokumenty Dle požadavků TISAX, musí organizace disponovat certifikovanými skartovacími zařízení, pro dokumenty klasifikované jako omezené nebo tajné. Nápravné opatření Bude realizováno výběrem vhodného řešení pomocí multikriteriální analýzy. Výběr bude probíhat mezi komerčními dodavateli. Zabezpečí projektový manažer.
	Ve výrobě se vyskytují neaktuální dokumenty bez příslušné klasifikace Při kontrole výrobních prostor bylo nalezeno množství staré dokumentace bez příslušné klasifikace, která je vyžadována v rámci ISMS a certifikace TISAX. Nápravné opatření Proběhne formou revize dokumentace. Cílem bude separovat a odstranit všechny dokumenty, které nenesou klasifikaci a zároveň revize všech stávajících dokumentů, které jsou zaneseny v systému pro sledování dokumentace (PALSTAT). Zodpovědnost za provedení tohoto nápravného opatření nesou stakeholderi, kdy každý z nich je povinen provést revizi na svých úsecích + v systému PALSTAT. Každý dokument musí být revidován a označen klasifikací (veřejný, interní, omezený, tajný).
VII.	Proces předávání a vrácení hardwaru zaměstnancům Při předání hardwaru novému zaměstnanci chybí doklad o převzetí příslušného zařízení. Dále chybí dokument, který celý tento proces popisuje. Základní struktura procesu musí být: Převzetí hardwaru (s podpisem), po vrácení je hardware uložen IT oddělením v uzamčeném prostoru, před předáním novému uživateli musí být

	reinstalován. Při likvidaci je disk daného zařízení odborně zlikvidován tak, aby z něj nešla vyčíst žádná metadata. Nápravné opatření: Oddělení lidských zdrojů zajistí vytvoření a zadání příslušné instrukce do systému sledování dokumentace, IT oddělení vyčlenění prostor pro skladování hardwaru a připraví proces reinstalace a likvidace (v součinnosti s centrálním IT oddělením).
VIII	Zabezpečení serverové místnosti
	Okno je zakryto pouze papírovým kartonem kvůli zabránění vizuálnímu přístupu zvenčí, což sice splňuje požadavky, nicméně jde o pouze prozatímní řešení Nápravné opatření: Implementovat neprůhlednou fólii na okno jako trvalé řešení. Zabezpečí HSE manažer.
IX	Zabezpečení přístupu z vnějšího prostředí
	Na dveřích určených pro zaměstnanecký vstup do objektu chybí mechanické, nebo elektronické systémy, které by upozornili na nedovření dveří, v případě nedovření hrozí riziko vstupu nepovolaných osob bez upozornění. Nápravné opatření: Implementace sirén, které při nedovření dveří spustí poplachový signál.

(zdroj:[23])

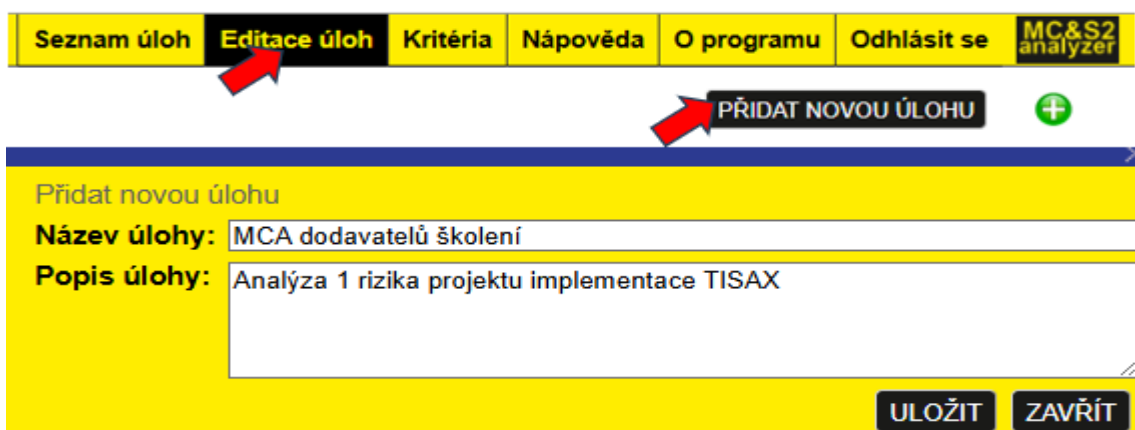
Z výše uvedených nápravných opatření, bude u opatření I, IV a V využita multikriteriální analýza, díky které bude zvolena kompromisní varianta, která bude realizována v rámci tohoto projektu. Ostatní varianty budou realizovány bez využití multikriteriální analýzy. Plán realizace všech opatření bude shrnut v kapitole 7.4.5 ve formě Gantova diagramu.

7.4.2 Metodika pro multikriteriální hodnocení

Cílem této kapitoly je zpracovat metodiku pro multikriteriální hodnocení (analýzu) v softwaru MC&S2 analyzer. Metodika je obecně použitelná, a aplikovatelná i pro osoby, které s multikriteriální analýzou nemají žádné zkušenosti.

1. Vytvoření nové úlohy

Prvním krokem je vytvoření nové úlohy, která reprezentuje konkrétní rozhodovací problém. Vytvoření je dostupné přes horní panel nabídky a kartu „Editace úloh“, následně klikněte na tlačítko „Přidat novou úlohu“. Poté zadejte název a popis úlohy a stiskněte tlačítko „Uložit“.

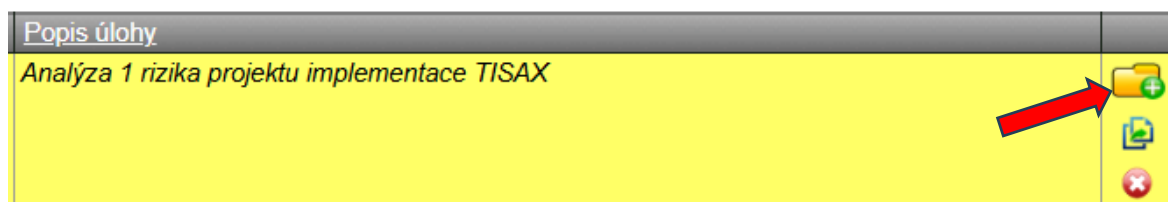


Obrázek 36 Vytvoření nové úlohy

(zdroj:[23])

2. Přidání variant

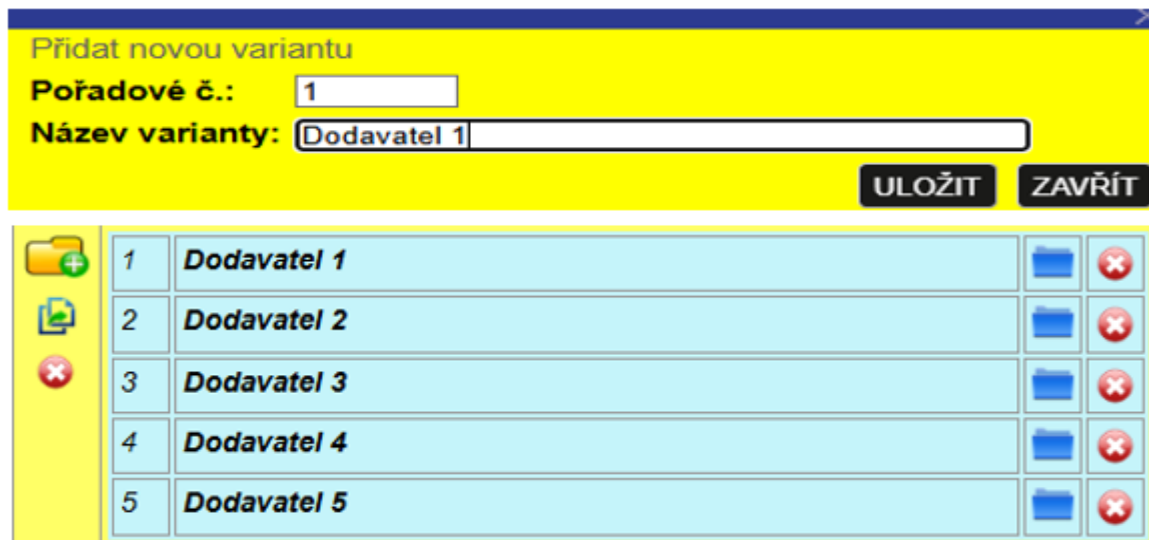
V druhém kroku je nezbytné nadefinovat varianty, z nichž má software najít kompromisní řešení. U nově vytvořené úlohy kliknete na tlačítko „Přidat novou variantu“.



Obrázek 37 Přidání nové varianty

(zdroj:[23])

Ke každé variantě je nezbytné definovat její pořadové číslo a název. Poté klikněte na tlačítko „Uložit“. Tento postup opakujete, dokud nemáte za definované všechny požadované varianty pro analýzu.



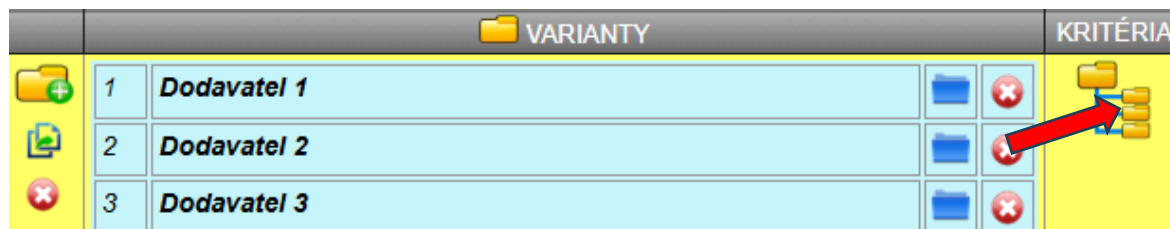
	Pořadové č.	Název varianty		
	1	Dodavatel 1		
	2	Dodavatel 2		
	3	Dodavatel 3		
	4	Dodavatel 4		
	5	Dodavatel 5		

Obrázek 38 Přidání všech variant

(zdroj:[23])

3. Přidání kritérií

Nyní je nezbytné provést výběr hodnotících kritérií. Při výběru berte v potaz, že kritéria musí být nastavena tak aby jimi bylo možné hodnotit všechny varianty. V příkladě výběru dodavatele školení jsou kritéria zvolena následovně: cena školení (Kč), rychlost realizace (kolik dnů dodavatel potřebuje na realizaci školení), reakční doba dodavatele školení (počet dnů), odbornost a zkušenosti (počet let působení v oboru) a průměrné hodnocení spokojenosti účastníků (v %). Pro přidání kritérií rozklikněte pravý boční panel vedle variant označený jako „Kritéria“.



VARIANTY					KRITÉRIA
	1	Dodavatel 1			
	2	Dodavatel 2			
	3	Dodavatel 3			

Obrázek 39 Vložení kritérií

(zdroj:[23])

Pokračujte přes tlačítko „Přidat kritérium“. Ke každému kritériu je nezbytné definovat: název, měrnou jednotku (lze zvolit pouze z nabízeného seznamu) a váhu. Výpočet pro váhu kritérií není v softwaru implementovaný, proto v tomto kroku musíte zvolit některou z metod, které byly popsány v kapitole 3.1, například Fullerovu metodu a spočítat jednotlivé váhy externě. Po zadání všech parametrů uložte tlačítkem „Uložit“. Tento proces opakujte, dokud nejsou zadány všechny kritéria.

Obrázek 40 Zadávání jednotlivých kritérií

(zdroj:[23])

Software umožňuje prioritizaci hodnot kritérií (větší hodnota je výhodnější, nebo menší hodnota je výhodnější). Nastavení je možné pomocí kliknutí na ikonu šipky vedle jednotlivých kritérií a zaškrtnutí checkboxu „Menší je výhodnější“. Výchozí nastavení je vždy ve smyslu, že větší hodnota je výhodnější.

Varianta 1: Dodavatel 1

1. Cena	120 000,00 Kč	0.3	↓
2. Rychlost realizace	10,00	0.2	↓
3. Reakční doba agentury	2,00 d	0.15	↓
4. Odbornost a zkušenosti	8,00 Rok	0.1	↑
5. Průměrné hodnocení spokojenosti	85,00 %	0.25	↑

Obrázek 41 Prioritizace hodnot kritérií

(zdroj:[23])

4. Výpočet a zobrazení výsledku

Pro výpočet hodnot zaklikněte checkbox „Přepočítat body“. Software následně na základě zadaných kritérií a jejich vah, bodově ohodnotí jednotlivá kritéria ve všech variantách. Pro zobrazení výsledku klikněte na checkbox „Výsledek“ a zobrazí se výsledné hodnocení variant. Pro zobrazení do formy grafů, přepněte v horním panelu na kartu „S2“. Zde můžete volit mezi celkovým hodnocením variant, nebo přehledem bodů, získaných v jednotlivých kategoriích.

Pořadové č.	Varianta	Body
1	Dodavatel 3	22,02
2	Dodavatel 4	20,72
3	Dodavatel 1	20,18
4	Dodavatel 5	18,98
5	Dodavatel 2	18,1

Obrázek 42 Zobrazení výsledků

(zdroj:[23])

7.4.3 Výběr nejlepších variant nápravných opatření

Na základě metodiky z kapitoly 7.4.2. budou stanoveny kompromisní varianty nápravných opatření na výstupy z analýzy rizik. Prvním krokem bude vždy určení vah pro kritéria pomocí bodovací metody, poté shrnutí vstupních dat a zadání do výpočetního softwaru. Ohodnocení variant při bodovací metodě proběhlo formou rozhodnutí na úrovni managementu.

Nápravné opatření I. Výběr dodavatele školení, zaměřeného na informační bezpečnost

Tabulka 33 Stanovení vah u nápravného opatření I

Počet bodů	Vyjádření	Kritéria	Body (k)	Váhy (V)
1	Nejhorší	Cena školení	5	0,33
2	Špatné	Rychlost realizace	2	0,13
3	Dobré	Reakční doba	1	0,07
4	Výborné	Odbornost a zkušenosti	4	0,27
5	Nejlepší	Hodnocení	3	0,20
Suma $\sum n$			15	1,00

(zdroj:[23])

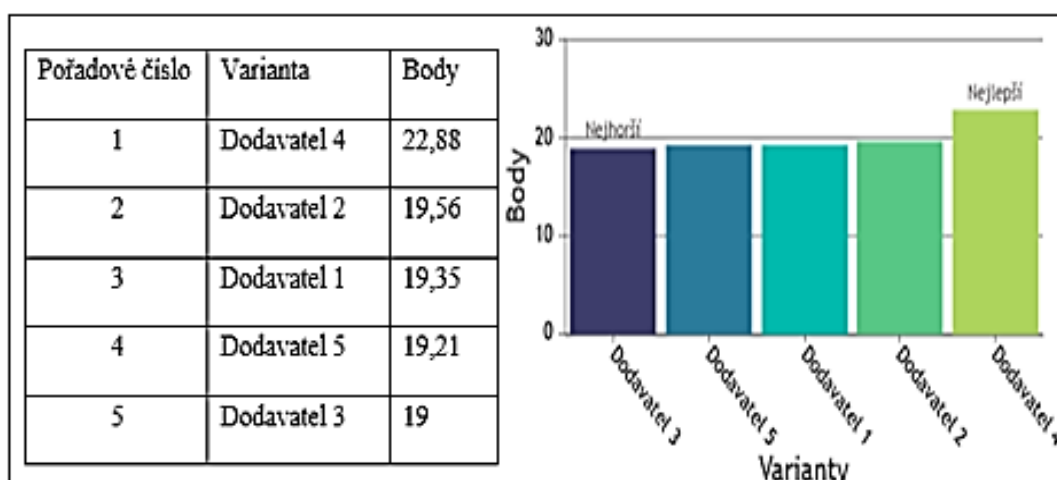
Shrnutí vstupních hodnot pro nápravné opatření a výpočet MC&S2 analyzerem

Tabulka 34 Shrnutí vstupních dat pro nápravné opatření I

Riziko		Nápravné opatření		Varianty	
Nepřijetí výstupu projektu		Periodické školení pro zaměstnance na téma Informační bezpečnost		5 variant možných dodavatelů	
Dodavatel	Cena školení (Kč)	Rychlost realizace (dny)	Reakční doba (dny)	Odbornost a zkušenosti (roky)	Průměrné hodnocení spokojenosti (%)
Váha kritéria	0,33	0,13	0,07	0,27	0,20
Dodavatel 1	120 000	10	2	8	85
Dodavatel 2	135 000	15	3	12	90
Dodavatel 3	110 000	12	1	5	80
Dodavatel 4	135 000	8	4	15	95
Dodavatel 5	130 000	14	2	10	88

(zdroj:[23])

Výsledné hodnocení



Obrázek 43 Výsledek hodnocení nápravného opatření I

(zdroj:[23])

V případě prvního nápravného opatření vyhodnotil jako kompromisní variantu dodavatele 4. Tento dodavatel je sice nejdražší, nicméně má dlouholeté zkušenosti a vysoké hodnocení spokojenosti.

Nápravné opatření IV. Výběr vhodného opatření v oblasti řízení fyzického přístupu

Tabulka 35 Stanovení vah u nápravného opatření IV

Počet bodů	Vyjádření	Kritéria	Body (k)	Váhy (V)
1	Nejhorší	Cena	5	0,33
2	Špatné	Rychlost realizace	2	0,13
3	Dobré	Reference dodavatele	1	0,07
4	Výborné	Potenciál rozvoje	4	0,27
5	Nejlepší	Udržitelnost	3	0,20
		Suma $\sum n$	15	1,00

(zdroj:[23])

Shrnutí vstupních hodnot pro nápravné opatření a výpočet MC&S2 analyzerem

Tabulka 36 Shrnutí vstupních dat pro nápravné opatření IV

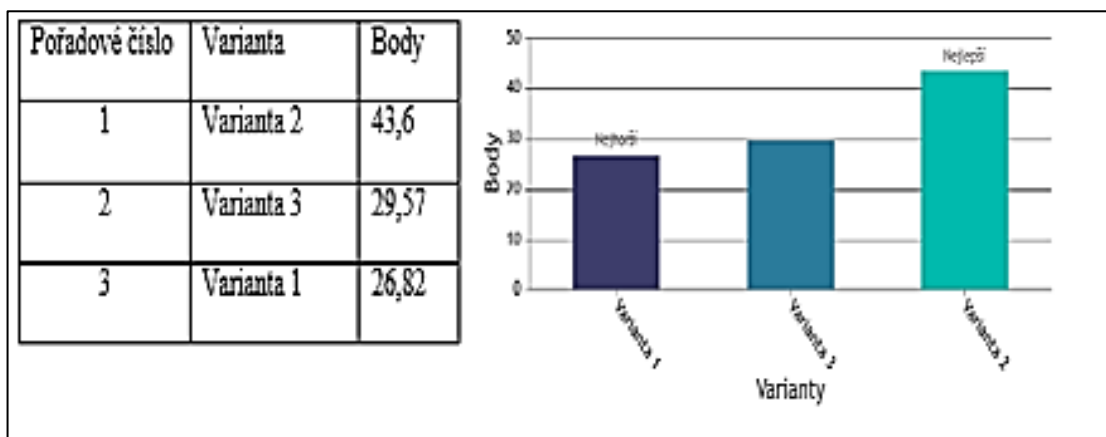
Riziko		Nápravné opatření		Varianty	
Neoprávněný přístup do jednotlivých prostor závodu		Implementace ACCESS systému		3 varianty možných řešení	
Varianta	Cena (Kč)	Rychlost realizace (dny)	Reference dodavatele (%)	Potenciál rozvoje (%)	Udržitelnost (%)
Váha kritéria	0,33	0,13	0,07	0,27	0,20
Varianta 1	1 300 000	20	95	75	80
Varianta 2	400 000	5	85	50	70
Varianta 3	1 450 000	20	85	95	95

(zdroj:[23])

Charakteristika variant

- Varianta 1 – Rozšíření stávajícího ACCESS systému, který funguje na bázi zaměstnaneckých čipů a čteček. Tento systém je implementovaný na hlavních vchodech do objektu společnosti a průchodu mezi administrativní a výrobní částí podniku, není však vůbec implementován na kancelářích, nebo laboratořích.
- Varianta 2 – Implementace mechanického MKS systému (Master Key System), který využívá cylindrických zámků a rozděluje dveře do zón s přiřazením konkrétních klíčů podle úrovně oprávnění.[57]
- Varianta 3 – Implementace nového ACCESS systému. Tato varianta využívá moderní bezdrátové přístupové zámků a čtečky, které lze instalovat přímo na dveře bez nutnosti rozsáhlých stavebních úprav a kabeláže. Systém podporuje více způsobů identifikace – mobilní telefon (Bluetooth/NFC), RFID karty/čipy, PIN kód, případně biometrické ověření (otisk prstu, obličeje). Správa přístupových práv probíhá centrálně, často v cloudovém rozhraní, a je možné ji snadno integrovat s HR, případně docházkovými systémy.

Výsledné hodnocení



Obrázek 44 Výsledek hodnocení nápravného opatření IV

(zdroj:[23])

U druhého nápravného opatření je kompromisní varianta číslo 2 na základě, které bude implementován MKS systém. Analýza ukazuje že rozhodujícím kritériem je cena, nicméně kdyby ne byla by kompromisní varianta 3, kde kombinace možného potenciálu rozvoje a udržitelnosti předčila i nejvyšší cenu.

Nápravné opatření V. Výběr certifikovaného skartovače

Tabulka 37 Stanovení vah u nápravného opatření V

Počet bodů	Vyjádření	Kritéria	Body (k)	Váhy (V)
1	Nejhorší	Cena	1	0,07
2	Špatné	Doba dodání	3	0,20
3	Dobré	Typ řezu (křížový)	5	0,33
4	Výborné	Skartace dalších médií	4	0,27
5	Nejlepší	Objem koše	2	0,13
		Suma $\sum n$	15	1,00

(zdroj:[23])

Shrnutí vstupních hodnot pro nápravné opatření a výpočet MC&S2 analyzerem

Tabulka 38 Shrnutí vstupních dat pro nápravné opatření V

Riziko		Nápravné opatření		Varianty	
Chybějící skartovače		Nákup nových zařízení		5 variant možných výrobků	
Varianta	Cena (Kč)	Doba dodání (dny)	Typ řezu (ANO / NE)	Skartace dalších médií (%)	Objem koše (litry)
Váha kritéria	0,07	0,20	0,33	0,27	0,13
Varianta 1	3489	3	ANO	50	23
Varianta 2	7390	3	ANO	100	23
Varianta 3	3649	2	ANO	75	23
Varianta 4	3790	5	ANO	75	19
Varianta 5	6290	4	ANO	75	20

(zdroj:[23])

Charakteristika variant

Varianta 1 - REXEL Momentum X410

- Rozměry (š, v, h): 356 × 423 × 238 mm
- Váha: 6,5 kg
- Barva: šedá
- Objem koše: 23 l / 225 listů A4
- Druh řezu, stupeň utajení: křížový řez, P4 / NNI 1 (vyhl. 13/2022 Sb.), odřezky o velikosti 4 × 28 mm
- Doba nepřetržitého provozu: 6 minut
- Hlučnost provozu: 62 dBA, univerzální motor
- Záruční doba: 2 roky (i na řezací mechanismus)

Obrázek 45 Specifikace REXEL Momentum X410

(zdroj:[58])

Varianta 2 - Fellowes 79 Ci

- Pokročilý stupeň bezpečnosti papír P-4 / karty T-4
- Křížový řez 3,9 × 38 mm
- **Skartace papíru, sponek, kreditních karet, CD**
- Skartovací kapacita až 16 listů 70 g/m2 papíru
- **Elektronický start / stop, funkce zpětného chodu**
- Šíře vstupu 230 mm
- 23litrový koš
- Kolečka pro snazší manipulaci
- Rychlost skartace 3,3 m/min.
- **100% JAM PROOF – funkce zabráňující uvíznutí papíru**
- Systém SafeSense – automatické zastavení skartovacího stroje při dotyku rukou v oblasti vstupního otvoru
- **SilentShred minimalizuje zatížení hlukem při skartování**
- Fellowes 79 Ci má systém úspory energie

Obrázek 46 Specifikace Fellowes 79 Ci

(zdroj:[59])

Varianta 3 - HP OneShred 12CC

- **Křížový řez skartuje listy papíru na částečky**
- **Skartovač HP disponuje košem o objemu 23 l**
- **Bezpečnostní stupeň utajení P-4 – částice do 160 mm²**
- **Umí skartovat papír, svorky a sponky, plastové karty**
- **Skartovač HP zvládne najednou skartovat 12 listů**
- **Navíc splňuje i GDPR požadavky**
- **Rozměry odpovídají 34,5 × 48,5 × 23,5 cm**

Obrázek 47 Specifikace HP OneShred 12CC

(zdroj:[60])

Varianta 4 - Fellowes LX 85

Klíčové vlastnosti skartovačky Fellowes LX 85

- Křížový řez zpracuje listy papíru na malé kousky
- Skartovač FELLOWES má ve výbavě koš o objemu 19 l
- Bezpečnostní stupeň utajení P-4 – částice do 160 mm²
- **Umí skartovat papír, svorky a sponky, plastové karty**
- Skartovač FELLOWES najednou skartuje 12 listů
- Navíc splňuje i GDPR požadavky
- Rozměry odpovídají 34 × 49,5 × 24,6 cm

Obrázek 48 Specifikace Fellowes LX 85

(zdroj:[61])

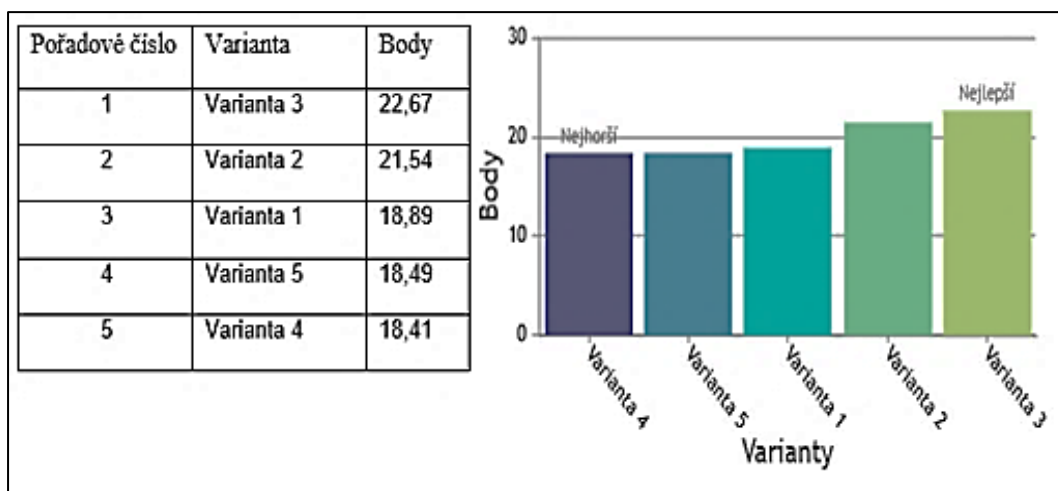
Varianta 5 - HP Pro Shredder 15CC

- Křížový řez nařeže dokumenty na kousky
- Skartovač HP má ve výbavě koš o objemu 20 l
- Stupeň utajení P-4 – částice do 160 mm²
- **Umí skartovat papír, svorky a sponky, plastové karty**
- Skartovač HP zvládne najednou skartovat 15 listů
- Naplňuje GDPR požadavky
- Rozměry jsou 35,4 × 53,5 × 24 cm

Obrázek 49 Specifikace HP Pro Shredder 15CC

(zdroj:[62])

Výsledné hodnocení



Obrázek 50 Výsledek hodnocení nápravného opatření V

(zdroj:[23])

Kompromisní volbou je produkt HP OneShred 12CC, který se sice řadí mezi cenově nejdostupnější v daném výběru, avšak vzhledem k tomu, že kritérium ceny mělo druhou nejnižší váhu, dosáhl tento model nejlepších výsledků v ostatních hodnocených parametrech.

Níže uvedená tabulka zobrazuje výsledky multikriteriální analýzy, realizované v rámci tohoto projektu.

Tabulka 39 Shrnutí výsledků multikriteriální analýzy

Nápravné opatření	Zvolená varianta na základě multikriteriální analýzy
I.	Školení dodá dodavatel 4.
IV.	Implementace MKS systému
V.	Nákup skartovače HP OneShred 12CC

(zdroj:[23])

7.4.4 Vyčíslení nákladů projektu

Náklady se týkají převážně externího prostředí. V rámci nákladů není zahrnutý čas a práce interních zaměstnanců a techniků, případně materiál, který byl k dispozici ve skladových zásobách společnosti a nebylo nutné jej nakoupit.

Tabulka 40 Shrnutí nákladů

Položka	Počet	Jednotková cena	Celkem
Školení informační bezpečnost	1	135000	135000
Implementace MKS systému	1	400000	400000
Skartovačka	3	3649	10947
Polachová siréna	4	1868	7472
Informační panely	2	4500	9000
Registrační poplatek	1	10125	10125
Provedení auditu na úroveň AL2	1	125000	125000

Instalace neprůhledné fólie do okna serverovny	1	1000	1000
Nákup uzamykatelné skříně na Hardware	1	24950	24950
Náklady celkem			723494

(zdroj:[23])

Náklady v kontextu tohoto projektu jsou marginální. Společnost tuto certifikaci musí získat pro udržení a rozvoj svého podnikání, nicméně i tak je dle interních předpisů nutné spočítat návratnost investice (ROI).

Výpočet ROI

Klíčovými daty pro tento výpočet je čistý zisk a celkové náklady investice. Aby bylo možné určit čistý zisk, bylo využito klíčového ukazatele – počet kusů v knize objednávek (dále již jen ODB). Díky rozdílu očekávaného stavu ODB a původního stavu ODB, byl stanoven přínos projektu v kusech, kdy díky jednotkové ceně bylo kalkulovat zisk v Kč.

Tabulka 41 Vstupní data pro výpočet ROI

Počet kusů v knize objednávek na kalendářní rok	
Původní stav ODB	98 526 300 Ks
Očekávaný stav ODB	102 526 300 Ks
Očekávaný přínos	+ 4 000 000 Ks
Čistý zisk / ks	9,5405 Kč
Předpokládaný zisk	38 162 000 Kč

(zdroj:[23])

Díky těmto datům je možné vypočítat hodnotu ROI, která se řídí vztahem:

$$ROI = \frac{\text{Čistý zisk} - \text{investice}}{\text{investice}} * 100\%$$

$$ROI = \frac{38162000 - 723494}{723494} * 100\% = 5175\%$$

Tato investice je i z matematického hlediska velmi výhodná. Výsledek lze interpretovat tak, že společnost z každé investované koruny vydělá 51,75 Kč.

7.4.5 Implementace nápravných opatření

Poslední částí etapy Improve je samotná implementace a realizace nápravných opatření. Jako nástroj pro sledování průběhu celého procesu implementace, byl zvolen Gantův diagram.

Jedná se o vizuální pomůcku, která se hojně využívá při řízení projektů. Jeho hlavním účelem je přehledně zobrazit, jaké úkoly je potřeba v projektu splnit, kdy mají začít a kdy skončit. Diagram je tvořen vodorovnou časovou osou, na které jsou jednotlivé úkoly znázorněny jako pruhy. Délka každého pruhu odpovídá době trvání konkrétní činnosti. Díky tomuto zobrazení je snadné vidět, které úkoly na sebe navazují, kde mohou vzniknout prodlévky nebo jaké činnosti lze provádět současně.[6]

Tento typ diagramu je velmi užitečný nejen při plánování, ale také při sledování postupu prací. Projektový tým i vedení mají díky Gantovu diagramu jasný přehled o tom, co už je hotové, co právě probíhá a co teprve přijde na řadu. Kromě toho pomáhá diagram odhalit úkoly, které jsou na sobě závislé, což je důležité pro správné načasování jednotlivých fází projektu. V praxi se Gantův diagram využívá v mnoha oborech – například ve stavebnictví, informačních technologiích nebo v oblasti výroby.[6]

Project: Implementace TISAX			Měsíc	LEDEN																
Sponzor: General manager			Den	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Etap	Akce	Zodpovědnost																		
D	Úvodní meeting	Projektový manažer																		
D	Stakeholderů a start projektu	Projektový manažer																		
D	Potvření stakeholderů	Projektový manažer																		
D	SWOT analýza projektů	Projektový manažer																		
M	Stanovení cílové úrovně TISAX	Projektový manažer																		
M	Konzultace s odborníkem	Projektový manažer																		
M	Stanovení ukazatelů	Projektový manažer																		

Obrázek 51 Ukázka části Gantova diagramu

(zdroj:[23])

V Ganttově diagramu byly reflektovány především klíčové aktivity a milníky daného projektu, které představují hlavní etapy postupu realizace. Pro efektivní sledování a rozdělování jednotlivých dílčích úkolů byl využit interní podnikový systém Fabrique. Tento systém umožňuje delegování konkrétních úkolů na příslušné zaměstnance, přesné vymezení

časového rámce pro jejich splnění, a také podporuje eskalaci úkolů mezi jednotlivými úrovněmi řízení ve společnosti (již zmiňovanou v souvislosti s nápravným opatřením VII.). Součástí funkcionality systému je rovněž možnost přikládat k úkolům relevantní dokumentaci a fotodokumentaci. Průběh plnění úkolů je pravidelně monitorován v rámci periodických porad. Každý splněný úkol je jednoznačně identifikován unikátním kódem a po jeho dokončení zůstává archivován v databázi jako důkazní materiál, který lze využít v případě interních či externích auditu. Na níže uvedeném obrázku je ukázka zadání jednotlivých úkolů v rámci vnitropodnikového informačního systému. Konkrétně se jedná o nápravné opatření II, popsané v kapitole 7.4.1.

TP Tomáš

15. 2.

LEAP

1 Priorita: Vysoká

Aktualizace matic zastupitelnosti

1 CEJC - Kontrola - PSM1

>

2 CEJC - Kontrola - PSM2

+

Štítky

AUDIT

+

Popis

V rámci přípravy na certifikační audit TISAX, jsou stakeholderi povinni aktualizovat své matice zastupitelnosti

+ Původní příčina

+ Jiné

0

+

7 / 9

+ Úkoly

Všechny úkoly

Řadit: Žádný

:

1	✓	Revize dokončených matic a potvrzení v Paistatu	TP Tomáš	15. 2.	:
2	✓	Aktualizace matice zastupitelnosti	LB	12. 2.	:
3	✓	Aktualizace matice zastupitelnosti	LR	12. 2.	:
4	✓	Aktualizace matice zastupitelnosti	LČ	12. 2.	:
5	✓	Aktualizace matice zastupitelnosti	RN	12. 2.	:
6	✓	Aktualizace matice zastupitelnosti	FI	12. 2.	:
7	✓	Aktualizace matice zastupitelnosti	MD	12. 2.	:

Obrázek 52 Ukázka zadání dílčích úkolů stakeholderům, u nápravného opatření II

(zdroj:[23])

Fotodokumentace z implementace



Obrázek 53 Zakoupené skartovače HP OneShred 12CC

(zdroj:[60])



Obrázek 54 Klíče od implementovaného systému MKS

(zdroj:[23])



Obrázek 55 Ukázka instalované sirény na zaměstnanecké vchody

(zdroj:[23])

lisi AUTOMOTIVE Přehled odebraných mate	
Internal Public	
Zkratka	Název
MBAEX00023	CARTON C40 + COVER C40
MBAEX00031	CARTON BOSCH 600x800mm
MBAEX00032	CARTON KRYCI 1200x800x300mm
MBAEX00035	PALETA 800x1200mm TEPELNE OŠ
MBAEX00044	CARTON 810x610x450mm
MBAEX00058	STOHOVATELNÝ KARTON 1205 X 805
MBAEX00061	PALETA 800 X 600MM OŠETRENÁ
MBAOS00013	SÁCEK ANTIK 0,06x300x200x320mm
MBAOS00015	SÁCEK ANTIK. 0,06X300X200X420M
MBAOS00016	FOLIE ANTIK. 0,1x1200x800mm
MBAOS00019	BRANO PAPIR 70g; 25x25cm

Obrázek 56 Ukázka aktualizovaných klasifikovaných dokumentů

(zdroj:[23])



Obrázek 57 Připomínkové informační tabule, na hlavní body školení

(zdroj:[23])

7.5 Control

Poslední etapa Control, se zaměřuje na zhodnocení dosažených výsledků v souvislosti s implementovanými změnami. Po aplikaci změnových a nápravných opatření popsanych v předchozích kapitolách, je nezbytné stanovit, zda a v jaké míře byly naplněny původní cíle a očekávání. Etapa Control představuje nejen završení celého procesu implementace, ale zároveň vytváří východisko pro budoucí organizační vývoj.

V rámci této kapitoly budou analyzovány přínosy realizovaných změn, identifikovány mechanismy pro stabilizaci nově zavedeného stavu a formulována konkrétní doporučení, která zajistí udržitelnost dosažených výsledků a napomohou dalšímu rozvoji organizace.

7.5.1 Vyhodnocení přínosu

Pro vyhodnocení přínosu budou použity zvolené výkonnostní ukazatele, stanovené v počáteční etapě projektu Measure. Srovnání je vypracováno v následující tabulce.

Tabulka 42 Vyhodnocení přínosu projektu

Ukazatel	Stav před implementací	Očekávaný stav před implementací	Reálný stav po implementaci
Počet nesplněných požadavků VDA ISA	N/A	0	0
Absolvovaná školení na osobu za kalendářní rok	1	2	2
Počet kusů v knize objednávek na kalendářní rok	98 526 300	102 526 300	102 526 300
Počet klíčových zákazníků	8	10	10
Počet projektů	105	112	109

(zdroj:[23])

Z tabulky vyplývá, že projekt, úspěšně naplnil 4 z 5 klíčových ukazatelů, které byly stanoveny v jeho počáteční etapě. Zajímavým zjištěním je, že i když se počet realizovaných projektů po implementaci zvýšil „pouze“ na 109 oproti očekávaným 112, celkový počet kusů v knize objednávek zůstal na plánované hodnotě 102 526 300. To znamená, že klíčový zákazníci sice nepoptali tolik projektů, kolik bylo původně v plánu, ale v těch projektech, které byly realizovány, naplnili předpokládaný objem objednávek. Tato skutečnost svědčí o stabilní poptávce a efektivním využití kapacit v rámci jednotlivých projektů.

Celkově lze tvrdit, že implementace přinesla naplnění nebo výrazné přiblížení se stanoveným cílům ve všech sledovaných oblastech, přičemž objem objednávek zůstal zachován i při mírně nižším počtu projektů. Dobrým důkazem je taktéž výpočet návratnosti investic ROI, který byl realizován již v rámci předchozí etapy, v podkapitole 7.4.4.

7.5.2 Stabilizace nového stavu

Pro udržení certifikace, doporučuje příručka VDA ISA celkem 39 ukazatelů, rozdělených do 17 oblastí. Tyto ukazatele nejsou povinné a slouží jako vzor pro nastavení vlastních metrik a kontrolních mechanismů. V souladu s příručkou byly zvoleny a upraveny následující ukazatele tak, aby naplňovali potřeby tohoto projektu.[63]

Tabulka 43 Stanovené ukazatele pro udržení stávajícího stavu

Oblast	Ukazatel	Cíl
Školení zaměstnanců	Procento zaměstnanců, prošlých školením v oblasti bezpečnosti informací	100 % každých 6 měsíců
Správa uživatelských účtů	Procent deaktivovaných účtů po ukončení pracovního poměru	100 % účtů do 72 hodin od odchodu zaměstnance
Ochrana před malwarem	Procento zařízení s antivirovou ochranou	100% zařízení má aktuální a aktualizovanou ochranu
Politiky a procedury	Revize aktuální bezpečnostní politiky	1 x za kalendářní rok
Správa mobilních zařízení	Procento firemních mobilních zařízení pod správou IT	100 % zařízení
Zabezpečení přístupu	Pravidelná revize nastavení systému MKS	1 x ročně

(zdroj:[63])

Pro udržení nového stavu, který je hodnocený jako pozitivní, byla zavedena periodická kontrola delegovanými zaměstnanci v rámci prostorů podniku a to zejména v kontextu „zlatých pravidel TISAX, které byly graficky znázorněny v kapitole 7.4.5.

- Žádné loginy, hesla, nebo jiné přihlašovací údaje nesmí být volně dostupné
- Jakákoliv externí osoba se nesmí pohybovat sama v prostorech společnosti. Vždy musí mít doprovod a viditelně umístěnou cedulku „Návštěvník“
- Osobní přístupové karty, nebo čipy nesmí být zapůjčeny jinému pracovníkovi
- Dodržování pořádku v kancelářích (čistý stůl, žádné volně položené dokumenty na stole, nebo v tiskárně, v době nepřítomnosti uživatele uzamčený počítač při odchodu z kanceláře)
- Kontrola systémů zajišťujících automatické uzavření dveří.
- Zajištění počítačů pomocí zámků

Záznam a vizualizace výsledků bude realizován prostřednictvím již zmíněného vnitro-podnikového systému Fabrique, který umožňuje plánování a vynucování auditů buď jednorázově, nebo prostřednictvím plánované řady událostí. Nastavení umožňuje to, aby delegovaný zaměstnanec nikdy nehodnotil své podřízené pracoviště a byla tak zachována nestranost kontroly. (Prostory výroby kontrolují pracovníci z administrativy a naopak). V případě negativního nálezu je negativně vyhodnocená oblast označena v systému a je k ní přiložena fotodokumentace nálezu.

Na základě těchto dat je následně vytvořen ticket směřující na vedoucího pracovníka daného pracoviště, který musí sjednat nápravu a tuto skutečnost taktéž potvrdit v systému. Revize výsledků probíhá na denní bázi v rámci běžných porad operativního a strategického managementu.

7.5.3 Doporučení pro další rozvoj

Přechod na úroveň AL3

V současné době je dosažená úroveň zabezpečení AL2 zcela dostačující a plně odpovídá aktuálnímu rozsahu výroby i požadavkům zákazníků. Pokud by však v budoucnu došlo k rozšíření výrobního portfolia o složitější komponenty pro automobilový průmysl, bylo by logickým a potřebným krokem usilovat o dosažení vyšší úrovně zabezpečení, konkrétně AL3.

Při přechodu na tuto vyšší úroveň by bylo možné využít stávající metodiku, která již byla v rámci společnosti implementována a ověřena v praxi. Nicméně samotný přechod by vyžadoval důkladnou revizi a aktualizaci všech nápravných opatření tak, aby odpovídala přísnějším požadavkům úrovně AL3. Zvláštní pozornost by přitom bylo nutné věnovat oblasti ochrany prototypů, kde se předpokládá zavedení pokročilejších bezpečnostních mechanismů, například implementace biometrických zabezpečovacích zařízení, která jsou na této úrovni standardem.

Rozšíření programu bezpečnostního povědomí

V praxi se ukazuje, že i při zavedení technických opatření zůstává lidský faktor často nejslabším článkem ochrany dat. Proto je vhodné navázat na dosavadní školení a vytvořit dlouhodobý program, který bude zaměstnance pravidelně seznamovat s aktuálními hrozbami a novými bezpečnostními postupy.

Doporučuje se například zavést roli tzv. „bezpečnostních ambasadorů“ v jednotlivých odděleních, kteří budou působit jako spojka mezi vedením a zaměstnanci a pomáhat šířit osvětu v každodenní praxi. Dále je možné využít interaktivní formy vzdělávání, například simulace phishingových útoků nebo krátké kvízy, které napomohou lepšímu zapamatování klíčových zásad. Pravidelné opakování a aktualizace těchto aktivit zajistí, že bezpečnostní povědomí zůstane vysoké i v době rychlých technologických změn.

Automatizace bezpečnostních procesů

Zavedení automatizovaných nástrojů do oblasti informační bezpečnosti přináší výrazné zvýšení efektivity a snižuje riziko lidské chyby. V kontextu společnosti Lisi Automotive Form a.s. lze doporučit například nasazení systému pro centralizovaný monitoring bezpečnostních událostí, který umožní včasnou detekci a reakci na incidenty.

Automatizace může zahrnovat také pravidelné kontroly souladu s požadavky TISAX a dalších standardů, čímž se minimalizuje administrativní zátěž a zvyšuje přesnost reportingu. Dalším krokem může být využití nástrojů pro automatické vyhledávání a klasifikaci citlivých dat v rámci podnikové infrastruktury, což usnadní jejich ochranu a správu. Celkově tak automatizace přispívá nejen ke zvýšení bezpečnosti, ale i k efektivnějšímu využití lidských zdrojů.

Posílení bezpečnosti cloud computingu

S rostoucím využíváním cloudových služeb v automobilovém průmyslu je nezbytné věnovat zvýšenou pozornost ochraně dat v těchto prostředích. Základem, by bylo vhodné stanovit jasná pravidla pro výběr a správu cloudových řešení, která budou zohledňovat jak požadavky TISAX, tak i specifika zpracovávaných dat.

Klíčové je zavedení více faktorového ověřování pro přístup do cloudových aplikací a důsledné šifrování dat během přenosu i uložení. Pravidelné bezpečnostní audity cloudových služeb by měly být samozřejmostí, stejně jako kontrola nastavení oprávnění a sledování přístupových logů.

ZÁVĚR

Diplomová práce se zabývá komplexní analýzou a návrhem opatření vedoucích k získání mezinárodní certifikace TISAX ve vybraném podniku automobilového průmyslu. Hlavním cílem bylo vyhodnotit aktuální stav informační bezpečnosti společnosti a navrhnout taková opatření, která umožní splnění požadavků certifikace TISAX s využitím metod multikriteriálního hodnocení a strukturovaného projektového řízení podle modelu DMAIC, upraveného v kontextu informační bezpečnosti.

V teoretické části byly podrobně rozebrány základní pojmy informační bezpečnosti, model CIA, systém řízení informační bezpečnosti (ISMS) a cyklus PDCA. Dále byla popsána certifikace TISAX, její význam, průběh a specifika v porovnání s normou ISO/IEC 27001. Součástí teoretického základu byla také analýza metod a softwarových nástrojů využitelných pro multikriteriální hodnocení a analýzu rizik, čímž byl vytvořen pevný základ pro praktickou aplikaci.

Praktická část byla zaměřena na aplikaci získaných poznatků na reálný podnikový případ. Pomocí metodiky DMAIC byly postupně definovány cíle projektu, provedena analýza současného stavu, identifikována klíčová rizika a navržena konkrétní nápravná opatření. Výběr optimálních opatření byl podpořen multikriteriální analýzou, která umožnila objektivní a transparentní rozhodování. Výsledkem bylo navržení uceleného postupu, který zahrnuje nejen samotnou implementaci požadovaných opatření, ale i nastavení mechanismů pro kontrolu a další rozvoj informační bezpečnosti ve společnosti.

Za hlavní přínos práce lze považovat propojení teoretických poznatků s praktickými nástroji a metodami, které jsou využitelné i v dalších organizacích usilujících o certifikaci TISAX. V rámci dalšího výzkumu by bylo vhodné zaměřit se na dlouhodobé sledování efektivity implementovaných opatření a rozšíření metodiky o nové trendy v oblasti informační bezpečnosti a kybernetické ochrany.

Závěrem mohu konstatovat, že stanoveného cíle práce bylo dosaženo a navržený postup může sloužit jako praktický návod pro podniky, které chtějí systematicky a efektivně přistoupit k získání certifikace a posílit tak svou informační bezpečnost v dynamickém prostředí automobilového průmyslu.

SEZNAM POUŽITÉ LITERATURY

- [1] CYBERSECURITY VENTURES. *Cybercrime Magazine*. Online. 2024. Dostupné z: <https://cybersecurityventures.com/cybersecurity-almanac-2024/>. [cit. 2025-02-04].
- [2] JAŠEK, Roman; MALANÍK, David a DAŇKOVÁ, Nicol. *Bezpečnost informačních systémů*. Online, UČEBNÍ MATERIÁL PŘEDMĚTU. Zlín: Univerzita Tomáš Bati, Fakulta aplikované informatiky, 2022. Dostupné z: <https://digilib.k.utb.cz/handle/10563/52082>. [cit. 2025-02-04].
- [3] JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-7318-456-7.
- [4] KOLOUCH, Jan a BAŠTA, Pavel. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7. Dostupné také z: <https://knihy.nic.cz/#cybersecurity>.
- [5] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Online. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6. Dostupné z: https://www.cybersecurity.cz/data/slovník_v310.pdf. [cit. 2025-02-06].
- [6] MILLER, Ivan. *Kapesní příručka Six Sigma*. 2. vyd. Praha: Interquality, 2011. ISBN 9788090277076.
- [7] CERTIFIKACE MANAŽERSKÝCH SYSTÉMŮ. *Cems.cz*. Online. 2017. Dostupné z: <https://www.cems-cz.com/clanok/231-pdca-cyklus>. [cit. 2025-02-06].
- [8] ENVSYS. *Logo TISAXU*. Online. 2024. Dostupné z: <https://www.envsys.cz/tisax-6-0/>. [cit. 2025-02-10].
- [9] BARTSCH, Christian. *Information Security Based on VDA ISA TISAX Automotive Strategies*. Amazon Digital Services LLC - Kdp, 2023. ISBN 9798865062653.
- [10] ENX. *Příručka pro účastníky TISAX*. Online. 2024. Dostupné z: <https://www.enx.com/handbook/tph-cz.html>. [cit. 2025-02-10].
- [11] CYBERELEMENTS. *Beyond Compliance: The Value of TISAX*. Online. 2024. Dostupné z: <https://cyberelements.io/beyond-compliance-the-value-of-tisax-in-the-automotive-industry/>. [cit. 2025-02-12].

- [12] PREVALENT. *TISAX and Cybersecurity Supply Chain Risk Management*. Online. 2024. Dostupné z: <https://www.prevalent.net/blog/tisax/>. [cit. 2025-02-12].
- [13] ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN EN ISO/IEC 27001, *Informační technologie – Techniky zabezpečení – Systémy managementu bezpečnosti informací – Požadavky*. Praha, 2023.
- [14] ČESKÁ AGENTURA PRO STANDARDIZACI. *Informace jsou cenné zboží. Norma ČSN EN ISO/IEC 27001 je pomůže ochránit*. Online. 2023. Dostupné z: <https://agenturacas.gov.cz/informace-jsou-cenne-zbozi-norma-csn-en-iso-iec-27001-je-pomuze-ochranit/>. [cit. 2025-02-16].
- [15] EURO-SYMBIOSE. *The differences between ISO 27001 and TISAX®*. Online. 2022. Dostupné z: <https://www.euro-symbiose.com/actuality-en/the-differences-between-iso-27001-and-tisax/>. [cit. 2025-02-17].
- [16] ENX. *Current TISAX Audit Providers*. Online. 2025. Dostupné z: <https://enx.com/en-US/TISAX/xap/?country=CZ>. [cit. 2025-02-18].
- [17] VDA. *Information security inside companies*. Online. 2024. Dostupné z: <https://www.vda.de/en/topics/digitization/data/information-security>. [cit. 2025-02-18].
- [18] WHITEHAT. *Why the automotive industry is a favourite of cyber criminals*. Online. 2023. Dostupné z: <https://whitehat.eu/the-ferrari-incident-and-why-the-automotive-industry-is-a-favourite-of-cyber-criminals/>. [cit. 2025-02-20].
- [19] ŽIVĚ.CZ. *Při ransomwarovém útoku na automobilku Ferrari unikla osobní data zákazníků*. Online. 2023. Dostupné z: <https://www.zive.cz/clanky/pri-ransomwarovem-utoku-na-automobilku-ferrari-unikla-osobni-data-zakazniku/sc-3-a-221346/default.aspx>. [cit. 2025-02-20].
- [20] CYBELLUM. *Massive Vehicle Breach Exposes Personal Data of 800,000 Volkswagen EV Owners*. Online. 2025. Dostupné z: <https://cybellum.com/blog/massive-vehicle-breach-exposes-personal-data-of-800000-volkswagen-ev-owners/>. [cit. 2025-02-20].
- [21] KONBRIEFING. *Major cyberattacks on the automotive industry 2023*. Online. 2024. Dostupné z: <https://konbriefing.com/en-topics/cyber-attacks-2023-ind-automotive.html>. [cit. 2025-02-20].

- [22] KIM, Shiko a SHRESTHA, Rakesh. *Automotive Cyber Security - Introduction, Challenges, and Standardization*. Springer Nature Singapore, 2020. ISBN 9789811580536.
- [23] Vlastní zdroj
- [24] CALS SERVIS. *O firmě*. Online. 2025. Dostupné z: <https://www.cals.cz/?pc=mAbout>. [cit. 2025-02-24].
- [25] SAZEČEK, Petr a BATURKO, Jurij. *Dokumentace MC&S2 analyzeru: O programu*. PDF. 2017.
- [26] EXPERTCHOICE. *HOW AHP WORKS*. Online. 2025. Dostupné z: <https://www.expertchoice.com/ahp-software>. [cit. 2025-02-24].
- [27] RESEARCH GATE. *Visual PROMETHEE User Manual*. Online. 2015. Dostupné z: https://www.researchgate.net/publication/275348613_Visual_PROMETHEE_User_Manual_including_tutorials. [cit. 2025-02-25].
- [28] INNOGET. *ELECTRE-H software package*. Online. 2006, 2020. Dostupné z: <https://www.innoget.com/technology-offers/4008/electre-h-software-package-a-tool-for-data-analysis-and-decision-aiding-with-hierarchical-criteria>. [cit. 2025-02-25].
- [29] 1000MINDS. *PAPRIKA method*. Online. 2006, 2025. Dostupné z: <https://www.1000minds.com/paprika>. [cit. 2025-02-25].
- [30] ONLINE OUTPUT. *TOPSIS software*. Online. 2023. Dostupné z: <https://onlineoutput.com/topsis-software/>. [cit. 2025-02-27].
- [31] ONLINE OUTPUT. *Guide for the SAW Online Software*. Online. 2023. Dostupné z: <https://onlineoutput.com/saw-help/>. [cit. 2025-02-27].
- [32] ŠAUR, David. *Informační podpora bezpečnostních systémů: Výukové materiály k přednáškám do předmětu Informační podpora bezpečnostních systémů*. PDF. Zlín. Dostupné také z: https://moodle.utb.cz/pluginfile.php/1139637/mod_resource/content/1/03_Anal%C3%BDza_rizik_MCA_metody_p%C5%99edn%C3%A1%C5%A1ky_AP8IP_%C5%A0aur.pdf.
- [33] FOTR, Jiří. *Vícekriteriální rozhodování za nejistoty*. Vysokoškolská skripta. Praha: Oeconomica, 2020. ISBN 978-80-245-2399-6.

- [34] ISHIZAKA, Alessio a NEMERY, Philippe. *Multi-criteria Decision Analysis, Methods and Software*. Wiley, 2013. ISBN 9781118644911.
- [35] *Structure of the AHP-model*. Online. 2001. Dostupné z: <https://www.researchgate.net/profile/Masood-Badri/publication/4916730/figure/fig1/AS:349419913400322@1460319607089/Structure-of-the-AHP-model.png>. [cit. 2025-03-12].
- [36] Using PROMETHEE Method for Multi-Criteria Decision Making: Applications and Procedures. Online. *Iris Journal of Economics & Business Management - IJEBM*. 2024, s. 7. ISSN 2993-8732. Dostupné z: <https://irispublishers.com/ijebm/fulltext/using-promethee-method-for-multi-criteria-decision-making-applications-and-procedures.ID.000502.php>. [cit. 2025-03-12].
- [37] MADANCHIAN, Mitra a TAHERDOOST, Hamed. A Comprehensive Overview of the ELECTRE Method in Multi Criteria Decision-Making. Online. *Journal of Management Science & Engineering research*. 2023, roč. 6, č. 2, s. 16. Dostupné z: <https://doi.org/10.30564/jmsr.v6i2.5637>. [cit. 2025-03-12].
- [38] ŁATUSZYŃSKA, Anna. MULTIPLE-CRITERIA DECISION ANALYSIS USING TOPSIS METHOD. Online. *Folia Oeconomica Stetinensia*. 2014, s. 76. Dostupné z: <https://doi.org/10.2478/fofi-2013-0015>. [cit. 2025-03-13].
- [39] PROCHÁZKOVÁ, Dana. *Analýza a řízení rizik*. Praha: České vysoké učení technické v Praze, 2011. ISBN 978-80-01-04841-2.
- [40] VALOUCH, Jan a HROMADA, Martin. *BEZPEČNOSTNÍ FUTUROLOGIE*. Online. 2. Zlín: Univerzita Tomáše Bati, 2016. ISBN 9788074546211. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/36771/Bezpecnostni_futurologie_2016.pdf?sequence=1&isAllowed=n. [cit. 2025-03-17].
- [41] APTIEN. *Co jsou dopady a důsledky rizik*. Online. 2023. Dostupné z: <https://aptien.com/cs/kb/articles/what-are-risk-impacts>. [cit. 2025-03-19].
- [42] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ. ČSN ISO 31000, *Management rizik*. 2 vydání. Praha, 2018.
- [43] KAMENICKÝ, Jan. Analýza a řízení rizika. Online. In: . 2016, s. 23. Dostupné z: https://www.csq.cz/fileadmin/user_upload/Clenstvi/Centra/Sborniky_spolehlivost/192_62Sbornik_n.pdf. [cit. 2025-03-19].

- [44] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ. ČSN EN 31010, *Management rizik - Techniky posuzování rizik*. 2 vydání. Praha, 2020. Dostupné také z: <http://csnonline.agentura-cas.cz/>.
- [45] PANJAITAN, Muhammad Iqbal. Simple Additive Weighting (SAW) method in Determining Beneficiaries of Foundation Benefits. Online. *Jurnal Teknologi Komputer*. 2019, roč. 13, č. 1, s. 25. ISSN 2723-8695. Dostupné z: <https://media.neliti.com/media/publications/326766-simple-additive-weighting-saw-method-in-f8f093e8.pdf>. [cit. 2025-03-14].
- [46] SMEJKAL, Vladimír a RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Expert. Praha: Grada, 2013. ISBN 978-80-247-4644-9.
- [47] *Co to je FTA*. Online. 2007, 2025. Dostupné z: https://www.volko.cz/w_co_je_to_FTA.php. [cit. 2025-03-24].
- [48] ŠAUR, David. Využití informační podpory pro krizové řízení. Online. *Trilobit*. 2014. ISSN 1804-1795. Dostupné z: <https://trilobit.fai.utb.cz/vyuziti-informacni-podpory-pro-krizove-rizeni>. [cit. 2025-03-26].
- [49] KYBEZ. *Začněte rok 2025 s CSA*. Online. 2025. Dostupné z: <https://kybez.cz/zacnete-rok-2025-s-csa-7-duvodu-proc-je-tento-nastroj-klicovy-pro-kybernetickou-bezpecnost/>. [cit. 2025-03-26].
- [50] ICZ. *ICZ Risk*Guide, pro řízení a analýzu rizik kybernetické bezpečnosti*. Online. 2025. Dostupné z: <https://www.iczgroup.com/risk-guide-pro-velke-organizace/>. [cit. 2025-03-26].
- [51] APTIEN. *Risk Management*. Online. 2024. Dostupné z: <https://aptien.com/en/kb/articles/risk-management>. [cit. 2025-03-26].
- [52] APTIEN. *Manažer rizik*. Online. 2024. Dostupné z: <https://aptien.com/cs/software-pro-manazery-rizik>. [cit. 2025-03-26].
- [53] RISKONNECT. *Active Risk Manager Brochure*. Online. 2024. Dostupné z: <https://riskonnect.com/solutions/active-risk-manager/>. [cit. 2025-03-31].
- [54] CAPTERRA. *Riskonnect Active Risk Manager*. Online. 2024. Dostupné z: <https://www.capterra.com.au/software/59568/active-risk-manager>. [cit. 2025-03-31].

- [55] PŘÍKASKÝ, Tomáš. *Implementace výrobního informačního systému*. Online, Bakalářská práce. Zlín: Univerzita Tomáš Bati, Fakulta aplikované informatiky, 2022. Dostupné z: <https://digilib.k.utb.cz/handle/10563/53936>. [cit. 2025-04-14].
- [56] FRÖHLICH, Tomáš. *RISKAN: Metodický manuál použití nástroje*. PDF. 2. 2018.
- [57] DOM SECURITY. *Master key system*. Online. 2024. Dostupné z: <https://www.dom-security.com/si/en/professionals/building-owners/master-keying#:~:text=clear%20and%20well%20defined%20structures>. [cit. 2025-04-23].
- [58] ALZA. *Specifikace REXEL Momentum X410*. Online. 1994, 2025. Dostupné z: <https://www.alza.cz/rexel-momentum-x410-d5630486.htm?o=1>. [cit. 2025-04-24].
- [59] ALZA. *Specifikace Fellowes 79 Ci*. Online. 1994, 2025. Dostupné z: https://www.alza.cz/fellowes-79ci-d434777.htm?evt=ac&pos=1&sqid=LuigisBox_1f124d0c-a289-43a6-b053-1504c8f23695. [cit. 2025-04-24].
- [60] ALZA. *Specifikace HP OneShred 12CC*. Online. 1994, 2025. Dostupné z: https://www.alza.cz/hp-oneshred-12cc-d7706925.htm?evt=ac&pos=1&sqid=LuigisBox_ad9bd9e2-7b03-426b-9f69-59ba816a74f1. [cit. 2025-04-24].
- [61] ALZA. *Specifikace Fellowes LX 85*. Online. 1994, 2025. Dostupné z: <https://www.alza.cz/fellowes-lx-85-d7016394.htm?o=1>. [cit. 2025-04-24].
- [62] ALZA. *Specifikace HP Pro Shredder 15CC*. Online. 1994, 2025. Dostupné z: <https://www.alza.cz/hp-pro-shredder-15cc-d7706929.htm>. [cit. 2025-04-24].
- [63] VDA. *VDA ISA Catalogue*. Online. 2022, 2024. Dostupné z: <https://www.vda.de/en/news/publications/publication/vda-isa-catalogue-version-5.1#publication-title>. [cit. 2025-04-26].
- [64] LEAN SIX SIGMA EXPERTS. *PDCA CYCLE*. Online. 2024. Dostupné z: <https://sixsigmaonlinetraining.com.au/pdca-cycle-what-is-it-and-what-can-it-do/>. [cit. 2025-05-14].

SEZNAM OBRÁZKŮ

Obrázek 1 Rozšířená triáda CIA	17
Obrázek 2 Komparace metod PDCA a DMAIC	22
Obrázek 3 Oficiální logo certifikace	23
Obrázek 4 Popis jednotlivých úrovní modelu CMM	32
Obrázek 5 Proces implementace	33
Obrázek 6 Analýza měsíců, kdy došlo k nejvíce narušením IB	36
Obrázek 7 Analýza zemí, kde došlo k nejvyššímu počtu narušení IB	36
Obrázek 8 Ukázka struktury AHP	43
Obrázek 9 Ukázka prostředí MC&S2 analyzeru	53
Obrázek 10 Ukázka uživatelského prostředí Expert Choice	54
Obrázek 11 Ukázka uživatelského prostředí Visual PROMETHEE	55
Obrázek 12 Ukázka uživatelského prostředí ELECTRE-H	56
Obrázek 13 Ukázka uživatelského prostředí 1000minds	57
Obrázek 14 Ukázka uživatelského prostředí TOPSIS	58
Obrázek 15 Ukázka uživatelského prostředí SAW	59
Obrázek 16 Proces managementu rizik, dle ČSN ISO 31000	62
Obrázek 17 Vizualizace procesu posuzování rizik dle ČSN EN IEC 31010	64
Obrázek 18 Ukázka metody modifikované metody FMEA	68
Obrázek 19 Ukázka struktury FTA analýzy	70
Obrázek 20 Ukázka prostředí softwaru RISKAN	72
Obrázek 21 Ukázka prostředí softwaru Risk*Guide	73
Obrázek 22 Ukázka prostředí softwaru APTIEN	74
Obrázek 23 Ukázka prostředí softwaru Active Risk Manager	75
Obrázek 24 Závod společnosti Lisi automotive v Čejči	78
Obrázek 25 Ukázka stěžejního produktu	78
Obrázek 26 Profesní certifikace Lean Six Sigma	81
Obrázek 27 Vytvoření subjektu	93
Obrázek 28 Vytvoření analýzy rizik	93
Obrázek 29 Vytvoření profilu analýzy rizik	94
Obrázek 30 Nabídka panelu analýza rizik	95
Obrázek 31 Seznam Aktiv	95
Obrázek 32 Seznam hrozeb	96
Obrázek 33 Zadávání hodnot	96
Obrázek 34 Vyplněná matice pro výpočet rizika	97

Obrázek 35 Výsledná rizika v softwaru Riskan.....	98
Obrázek 36 Vytvoření nové úlohy	105
Obrázek 37 Přidání nové varianty.....	105
Obrázek 38 Přidání všech variant	106
Obrázek 39 Vložení kritérií.....	106
Obrázek 40 Zadávání jednotlivých kritérií	107
Obrázek 41 Prioritizace hodnot kritérií.....	107
Obrázek 42 Zobrazení výsledků	108
Obrázek 43 Výsledek hodnocení nápravného opatření I	109
Obrázek 44 Výsledek hodnocení nápravného opatření IV	111
Obrázek 45 Specifikace REXEL Momentum X410	113
Obrázek 46 Specifikace Fellowes 79 Ci	113
Obrázek 47 Specifikace HP OneShred 12CC	113
Obrázek 48 Specifikace Fellowes LX 85.....	114
Obrázek 49 Specifikace HP Pro Shredder 15CC	114
Obrázek 50 Výsledek hodnocení nápravného opatření V	114
Obrázek 51 Ukázka části Gantova diagramu	117
Obrázek 52 Ukázka zadání dílčích úkolů stakeholderům, u nápravného opatření II	118
Obrázek 53 Zakoupené skartovače HP OneShred 12CC.....	119
Obrázek 54 Klíče od implementovaného systému MKS	119
Obrázek 55 Ukázka instalované sirény na zaměstnanecké vchody	120
Obrázek 56 Ukázka aktualizovaných klasifikovaných dokumentů	120
Obrázek 57 Připomínkové informační tabule, na hlavní body školení.....	121

SEZNAM TABULEK

Tabulka 1 Základní odlišnosti mezi informační a kybernetickou bezpečností.....	15
Tabulka 2 Charakteristiky a specifické požadavky úrovně ochrany	25
Tabulka 3 Příklady kybernetických hrozeb a nápravných opatření.....	26
Tabulka 4 Popis ustanovení první části u normy ISO/IEC 27001	29
Tabulka 5 Shrnutí kategorií obsažených v dodatku, včetně příkladů opatření	30
Tabulka 6 Rozdíly mezi normou ISO/IEC 27001 a TISAXEM	30
Tabulka 7 Ukázka postupu bodovací metody	38
Tabulka 8 Ukázka postupu metody pořadí	39
Tabulka 9 Ukázka postupu Fullerovi metody	40
Tabulka 10 Ukázka postupu Saatyho metody.....	41
Tabulka 11 Výhody a nevýhody konkrétních metod pro stanovení vah	42
Tabulka 12 Typy metody PROMETHEE	43
Tabulka 13 Typy metody ELECTRE	45
Tabulka 14 Shrnutí jednotlivých metod multikriteriálního hodnocení.....	51
Tabulka 15 Rámec managementu rizik dle ISO 31000	62
Tabulka 16 Popis kroků metody DMAIC	79
Tabulka 17 Shrnutí cílů metodiky	80
Tabulka 18 Popis I. etapy Define.....	82
Tabulka 19 Popis II. etapy Measure	82
Tabulka 20 Popis III. etapy Analyze	83
Tabulka 21 Popis IV. etapy Improve	83
Tabulka 22 Popis V. etapy Control.....	84
Tabulka 23 Project Charter	85
Tabulka 24 Složení projektového týmu	86
Tabulka 25 SWOT analýza projektu	87
Tabulka 26 Moduly a dílčí oblasti hodnocení certifikace TISAX.....	88
Tabulka 27 Matice hodnocení Assessment level	90
Tabulka 28 Shrnutí ukazatelů stanovených pro sledování přínosu projektu	91
Tabulka 29 Souhrn aktiv a hrozeb, použitých v metodice analýzy rizik.....	92
Tabulka 30 Checklist pro kontrolu požadavků	98
Tabulka 31 Shrnutí rizik	100
Tabulka 32 Seznam navrhovaných opatření	101
Tabulka 33 Stanovení vah u nápravného opatření I	108
Tabulka 34 Shrnutí vstupních dat pro nápravné opatření I.....	109

Tabulka 35 Stanovení vah u nápravného opatření IV	110
Tabulka 36 Shrnutí vstupních dat pro nápravné opatření IV	110
Tabulka 37 Stanovení vah u nápravného opatření V	112
Tabulka 38 Shrnutí vstupních dat pro nápravné opatření V	112
Tabulka 39 Shrnutí výsledků multikriteriální analýzy	115
Tabulka 40 Shrnutí nákladů	115
Tabulka 41 Vstupní data pro výpočet ROI	116
Tabulka 42 Vyhodnocení přínosu projektu	122
Tabulka 43 Stanovené ukazatele pro udržení stávajícího stavu	123

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

TISAX	Trusted Information Security Assessment eXchange, certifikát využívaný pro standardizované hodnocení informační bezpečnosti v automobilovém průmyslu
ICT	Information and Communication Technologies, informační a komunikační technologie
AI	Artificial Intelligence, umělá inteligence
ISMS	Information Security Management System, systém řízení informační bezpečnosti
IT	Information Technologies, informační technologie
PDCA	Plan-Do-Check-Act, cyklus plánuj-dělej-kontroluj-jednej
VDA	Verband der Automobilindustrie, německá asociace automobilového průmyslu
ENX	European Network Exchange, evropská asociace výrobců automobilů
ISA	Information Security Assessment, posouzení bezpečnosti informací
AL	Assessment Level, úroveň hodnocení
CI	Continuous Improvement, neustálé zlepšování
ISO	International Organization for Standardization, mezinárodní organizace pro normalizaci
IEC	International Electrotechnical Commission, mezinárodní elektrotechnická komise
KPMG	Klynveld-Peat-Marwick-Goerdeler, zkratka vzniklá z jmen zakladatelů celosvětové sítě poradenských společností
TÜV NORD	Technischer Überwachungs Verein, technické kontrolní sdružení
OEM	Original Equipment Manufacturer, původní výrobce zařízení.
GB	Giga Byte, zkratka jednotky vyjadřující množství dat
CALS	Continuous Acquisition & Life-cycle Support, Řízení životního cyklu produktu

GPT	Generative Pre-trained Transformer, jazykový model umělé inteligence
AHP	Analyticko-hierarchický proces, metoda multikriteriálního hodnocení
PROMETHE	Preference Ranking Organization Method for Enrichment Evaluation, metoda organizace preferenčního pořadí pro hodnocení obohacení
ELECTRE	Elimination Et Choix Traduisant la Realité, metoda eliminace a volby odrážející realitu
PAPRIKA	Potentially All Pairwise RanKings of all possible Alternatives, metoda hodnocení všech potenciálně párových, možných alternativ
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution, technika pro určení pořadí preferencí podle podobnosti s ideálním řešením
WSM	Weighted Sum Model, metoda váženého součtu
SAW	Simple Additive Weighting, metoda jednoduchého aditivního vážení
WLC	Weighted Linear Combination, metoda vážené, lineární kombinace
MACBETH	Measuring Attractiveness by a Categorical Based Evaluation Technique, metoda měření atraktivity pomocí kategoriální hodnotící techniky
SWOT	Strengths-Weaknesses-Opportunities-Threats, metoda využívaná k hodnocení vnitřních a vnějších faktorů
FMEA	Failure Mode and Effects Analysis, analýza způsobů a důsledků poruch
FTA	Fault tree analysis, analýza stromu poruch
NASA	National Aeronautics and Space Administration, národní úřad pro letectví a vesmír
CCA	Cause Consequence Analysis, analýza příčin a následků
NIS2	Network and Information Security 2, celoevropská směrnice zabývající se kybernetickou bezpečností
COSO	Committee of Sponsoring Organization, standard pro hodnocení a řízení interních kontrol
DMAIC	Define-Measure-Analyze-Improve-Control, metoda používaná v rámci přístupu Six Sigma

APU	Autonomous Production Unit, manažer výrobní divize.
ACCESS	Systém řízení přístupu
MKS	Master Key System, mechanický systém řízení přístupu
KČ	Koruna česká, měna
ROI	Return on Investment, návratnost investice
HR	Human Resources, lidské zdroje
KPI	Key Performance Indicator, Klíčové ukazatele výkonnosti

SEZNAM PŘÍLOH

Příloha P I: Techniky a metody dle normy ISO/IEC 31010

PŘÍLOHA P I: TECHNIKY A METODY DLE NORMY ISO/IEC 31010

	Název techniky	Stručný popis	Oblast využití
1	Brainstorming	Skupinová kreativní metoda generování nápadů	Identifikace rizik
2	Strukturované nebo polostrukturované rozhovory	Systematický sběr informací od expertů formou rozhovorů	Identifikace a analýza rizik
3	Metoda Delphi	Iterativní metoda získávání konsenzu expertů pomocí dotazníků	Identifikace, analýza a hodnocení rizik
4	Kontrolní seznamy (Checklist)	Seznam kontrolních otázek pro ověření identifikace rizik	Identifikace rizik
5	Předběžná analýza nebezpečí	Včasná identifikace potenciálních nebezpečí v systémech nebo procesech	Identifikace rizik
6	Studie nebezpečí a provozuschopnosti (HAZOP)	Systematická analýza procesů k identifikaci odchylek a jejich následků	Identifikace a analýza rizik
7	Analýza nebezpečí a kritických kontrolních bodů (HACCP)	Identifikace kritických bodů v procesech, zejména potravinářství a výrobě léčiv	Identifikace a řízení kritických bodů
8	Hodnocení toxicity	Hodnocení toxických účinků látek na zdraví lidí nebo životní prostředí	Analýza dopadů na zdraví a životní prostředí
9	Strukturovaná technika "Co když" (SWIFT)	Systematická analýza scénářů pomocí otázek "Co když?" za účelem identifikace rizikových situací	Identifikace scénářů a dopadů

10	Analýza scénářů	Vývoj popisných modelů možných událostí k pochopení jejich dopadů a pravděpodobností výskytu	Analýza dopadů, plánování opatření
11	Analýza dopadů na podnikání (BIA)	Hodnocení dopadu narušení klíčových procesů organizace na její cíle a provozuschopnost	Kontinuita podnikání
12	Analýza prvotních příčin (RCA)	Zjišťování základních příčin problémů či selhání za účelem prevence opakování v budoucnu	Analýza příčin incidentů
13	Analýza způsobů a důsledků poruch (FMEA)	Systematická analýza možných poruch systému, jejich příčin a důsledků s cílem prevence selhání systému či procesu.	Prevence selhání systémů
14	Analýza stromu poruch (FTA)	Grafická metoda analýzy příčin nežádoucích událostí pomocí logických vazeb	Analýza příčin, pravděpodobností
15	Analýza stromu událostí (ETA)	Grafická metoda znázorňující možné následky iniciační události formou větvení scénářů	Analýza následků, pravděpodobností
16	Analýza příčin a následků (CCA)	Kombinovaná metoda spojující strom poruch a strom událostí pro komplexní pochopení vztahu mezi příčinami a následky nežádoucích událostí.	Komplexní analýza příčin i následků
17	Diagram příčin a následků	Grafické znázornění vztahů mezi problémem a jeho potenciálními příčinami.	Identifikace příčin problémů
18	Analýza ochranných vrstev (LOPA)	Semikvantitativní hodnocení účinnosti jednotlivých vrstev ochrany před nežádoucími událostmi.	Hodnocení bezpečnostních opatření
19	Rozhodovací strom	Grafická metoda znázorňující rozhodovací alternativy, možné výsledky rozhodování za nejistoty	Podpora rozhodování za nejistoty

		hodnutí a jejich pravděpodobnosti. Pomáhá při výběru optimální varianty rozhodnutí za nejistoty.	
20	Analýza lidské spolehlivosti (HRA)	Hodnocení pravděpodobnosti lidských chyb v systémech či procesech. Zaměřuje se na snížení vlivu lidského faktoru na vznik incidentů.	Hodnocení vlivu lidského faktoru
21	Bow Tie analýza	Spojuje možné příčiny incidentu s jeho důsledky prostřednictvím preventivních opatření. Poskytuje komplexní přehled o řízení konkrétního rizika.	Komplexní vizualizace řízení rizika
22	Údržba zaměřená na bezporuchovost (RCM)	Optimalizace údržby zařízení s cílem minimalizovat pravděpodobnost selhání systému.	Řízení údržby systémů
23	Analýza parazitních obvodů	Identifikace skrytých návrhových chyb v elektronických systémech či obvodech.	Bezpečnost elektronických systémů
24	Markovova analýza	Pravděpodobnostní modelování systémů s různými stavy pro predikci budoucích stavů systému.	Modelování spolehlivosti systémů
25	Simulace Monte Carlo	Statistická simulační metoda pro kvantitativní hodnocení rizik pomocí náhodných vzorkování vstupních proměnných.	Kvantitativní analýza nejistot
26	Bayesovská statistika a Bayesovské sítě	Pravděpodobnostní modelování založené na podmíněných pravděpodobnostech událostí. Pomáhá aktualizovat odhady rizik dle nových informací.	Kvantitativní hodnocení pravděpodobností
27	FN křivka	Vizualizace závažnosti dopad	

28	Index rizika	Polokvantitativní vyjádření úrovně rizika pomocí indexu.	Prioritizace rizik
29	Matice rizik	Kvalitativní nebo semikvantitativní vizualizace úrovně rizika dle pravděpodobnosti výskytu a závažnosti dopadu.	Prioritizace rizik
30	Cost-benefit analýza	Porovnání nákladů na opatření vůči přínosům snížení rizika.	Ekonomické hodnocení opatření
31	Vícekriteriální rozhodovací analýza (MCA)	Vyhodnocení alternativ podle více kritérií současně.	Podpora komplexního rozhodování

(zdroj:[44])