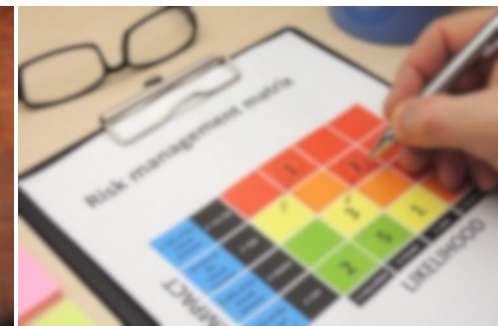




KONFERENCIA

RIADENIE RIZÍK V INFORMATICKOM A KYBERNETICKOM PRIESTORE

Vybrané techniky posudzovania rizík

Podľa normy IEC 31010:2019 pre rizikovú analýzu organizácie v oblasti ISO 37301:2021 „Compliance Management Systems“

Ing. Vladimíra Duníková, ACCIA, s.r.o.

dunikova@accia.sk

14.09.2021 Hotel Color Bratislava (virtuálna konferencia)

Čo sa dnes dozviete ?

...a čo vám chcem povedať...



...myslenie založené na rizikách sa stáva **integrálnou súčasťou** všetkých **procesov** organizácie – každý proces je **dotknutý** rizikom alebo môže vyvolávať riziko... ale aj **príležitosť** 😊...



Novinky v oblasti ISO štandardov

- Novinky v ISO/TC 262 Risk Management
- Novinky ÚNMS SR - odbor technickej normalizácie

Čo je nové ?

ISO/TC 262 Risk Management



TC

STANDARDS BY ISO/TC 262

Risk management

Zdroj: ISO - ISO/TC 262 - Risk management

Filter: ☒ Published standards ☐ Standards under development ☐ Withdrawn standards ☐ Projects deleted

Filter the list

STANDARD AND/OR PROJECT UNDER THE DIRECT RESPONSIBILITY OF ISO/TC 262 SECRETARIAT (5) ↓

	STAGE	ICS
IWA 31:2020 Risk management — Guidelines on using ISO 31000 in management systems	60.60	03.100.01
ISO 31000:2018 Risk management — Guidelines	60.60	03.100.01
ISO/TR 31004:2013 Risk management — Guidance for the implementation of ISO 31000	60.60	03.100.01
IEC 31010:2019 Risk management — Risk assessment techniques	60.60	03.100.01
ISO 31022:2020 Risk management — Guidelines for the management of legal risk	60.60	03.100.01

Čo je nové ?

ISO/TC 262 Risk Management



TC STANDARDS BY ISO/TC 262 • Risk management

Zdroj: ISO - ISO/TC 262 - Risk management

Filter: ☐ Published standards ☒ Standards under development ☐ Withdrawn standards ☐ Projects deleted

Filter the list

STANDARD AND/OR PROJECT UNDER THE DIRECT RESPONSIBILITY OF ISO/TC 262 SECRETARIAT (3) ↓

ISO 31030

Travel risk management — Guidance for organizations

STAGE

60.00

ICS

03.100.01

ISO/WD 31050

Guidance for managing emerging risks to enhance resilience

20.20

03.100.01

ISO/DIS 31073

Risk management – Vocabulary

40.60

01.040.03
03.100.01



Čo je nové ?

ÚNMS SR – odbor technickej normalizácie



STN EN IEC 31010

Zdroj: STN EN IEC 31010 | SUTN (unms.sk)



Pridať tlačенú formu normy do košíka:

[pridať do košíka](#)



Pridať elektronickú formu normy do košíka:

[pridať do košíka](#)

Označenie:	STN EN IEC 31010
Slovenský názov:	Manažérstvo rizika. Techniky posudzovania rizík
Anglický názov:	Risk management. Risk assessment techniques
Pôvodné označenie:	
Dátum vydania:	1. 8. 2021
Dátum zrušenia:	
Jazyk:	 SK
ICS:	03.100.01
Triediaci znak:	01 0380
Úroveň zapracovania:	idt IEC 31010:2019, idt EN IEC 31010:2019
Vestník:	07/21
Poplatok:	Tlačená verzia: 35,00 €

Elektronická verzia

- Bez možnosti tlače, prenosu textu a obrázkov: 31.50 €
- Bez možnosti tlače, s prenosom textu a obrázkov: 35.00 €
- S možnosťou tlače, prenosu textu a obrázkov: 45.50 €



Manažérstvo rizika

- IEC 31010:2019
- STN EN IEC 31010:2021 ☺ ☺ ☺

Proces manažérstva rizika

Norma ISO 31000:2018



Figure 1 — Process

The risk management process should be an integral part of management and decision-making and integrated into the structures, operations and processes of the organisation. It can be applied at strategic, operational, programme or project levels.

There can be many applications of the risk management process within an organisation, determined by its objectives, and its use the internal and external context in which they are applied.

The dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process.

Although the risk management process is often presented as sequential in practice it is iterative.

6.2 Communication and consultation

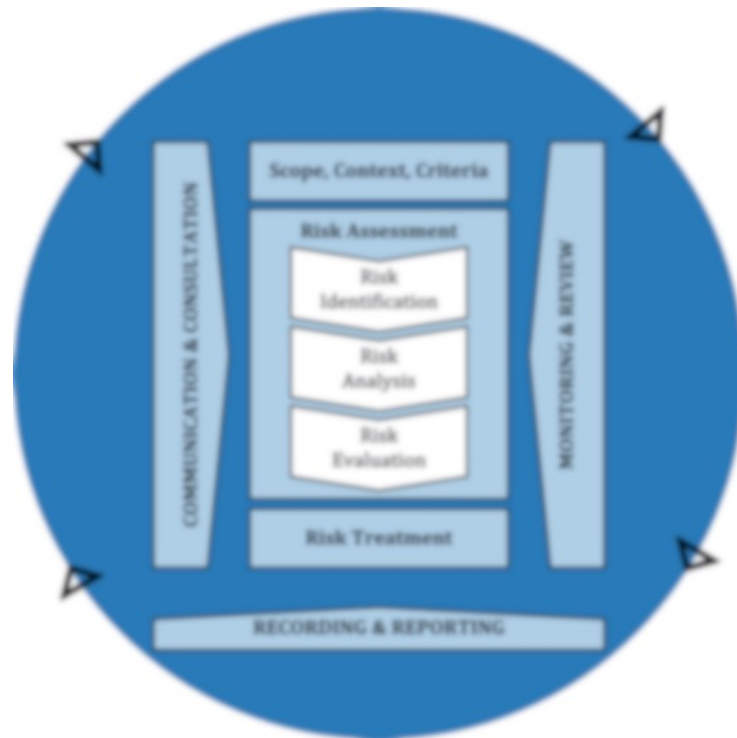
The process of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication aims to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Close coordination between the two should facilitate timely, relevant, accurate and understandable exchange of information, helping to ensure the confidentiality and integrity of information as well as the privacy rights of individuals.

Communication and consultation with appropriate internal and external stakeholders should take place within and throughout all stages of the risk management process.

Communication and consultation activities

- bring different areas of expertise together for each step of the risk management process
- ensure that different views are appropriately considered when defining risk criteria and when evaluating risks
- provide sufficient information to facilitate risk analysis and decision-making

ISO 31000 — 01/2018



Zdroj: ISO - ISO 31000:2018 - Risk management — Guidelines

Riziko

...účinnok neistoty na ciele...



Účinnok je odchýlka od očakávania

Môže byť **pozitívna**, **negatívna** alebo **oboje** a môže riešiť, vytvárať alebo vyústiť do **príležitostí** a **hrozieb**.

Riziko sa zvyčajne vyjadruje z hľadiska

zdrojov rizika, potenciálnych **udalostí**, ich **následkov** a ich **pravdepodobnosti**

Nástroje a techniky pre posudzovanie rizík

Norma STN EN IEC 31010:2021



ICS 03.100.01 SLOVENSKÁ TECHNICKÁ NORMA August 2021

STN	Manažérstvo rizika Techniky posudzovania rizík (IEC 31010: 2019)	STN EN IEC 31010
		01 0380

idI IEC 31010: 2019

Risk management
Risk assessment techniques
Management du risque
Techniques d'évaluation du risque
Risikomanagement
Verfahren zur Risikobewertung

Táto norma je slovenskou verziou európskej normy EN IEC 31010: 2019, ktorá bola vypracovaná Úradom pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky. Táto norma má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN IEC 31010: 2019. It was translated by Slovak Office of Standards, Metrology and Testing. It has the same status as the official versions.

Nahradenie predchádzajúcich noriem

Táto norma nahrádza anglickú verziu STN EN IEC 31010 z decembra 2019, ktorá od 01. 12. 2019 nahrádza STN EN 31010 z decembra 2010 v celom rozsahu.

STN EN 31010 z decembra 2010 sa môže súbežne s touto normou používať do 18. 7. 2022.

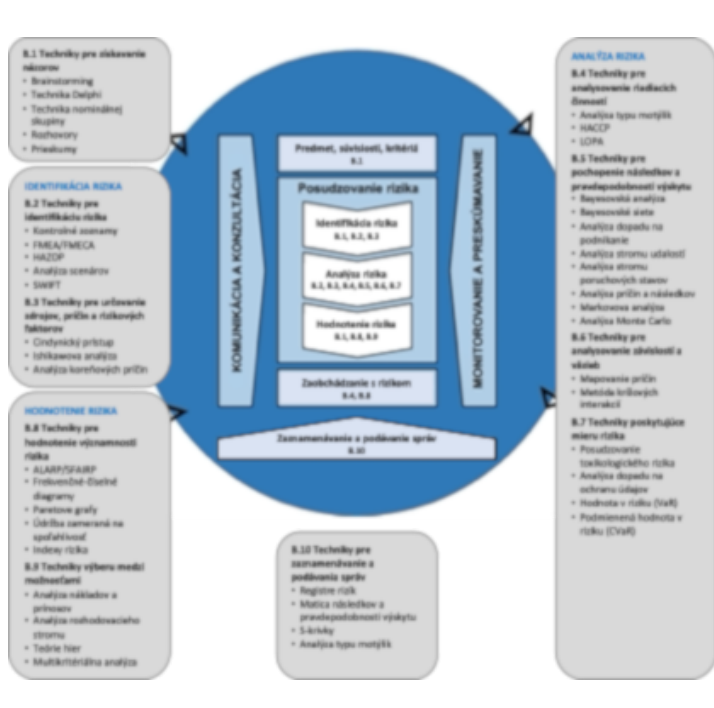
123848

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2021
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii.



Manažérstvo rizika – techniky posudzovania rizika

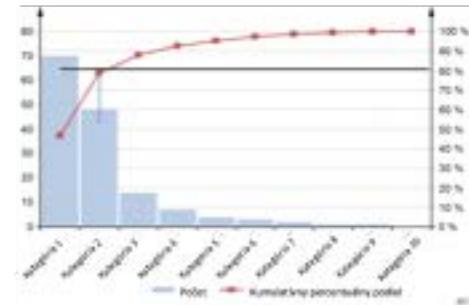
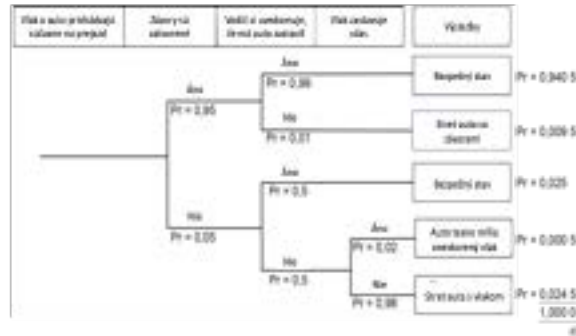
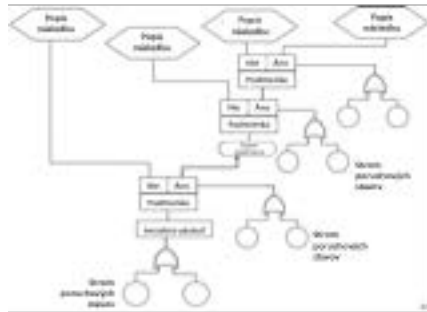
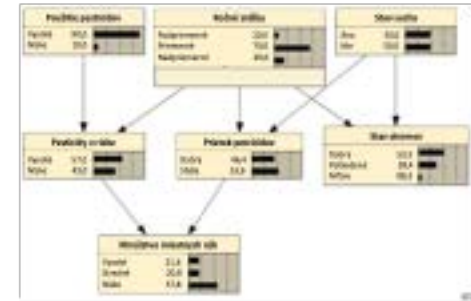
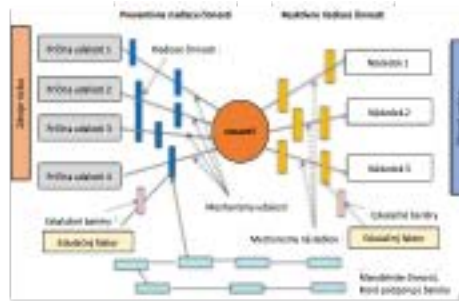
Ako vybrať správnu techniku pre posúdenie rizika ?



Tabuľka A.1 – Charakteristiky techník

Charakteristika	Opis	Podrobnosti (napr. indikátory funkcií)
Aplikácia	Ako sa technika používa pri posudzovaní rizika (pozri názvy kapitol S.1 až S.10).	Získať názory, identifikovať, analyzovať príčinu, analyzovať radiace činnosti rizika, atď.
Oblasť použitia	Týka sa rizika na úrovni organizácie, oddelenia alebo projektu alebo na úrovni jednotlivých procesov alebo zariadení.	Organizácia Projekt/oddelenie Zariadenia/proces
Časový horizont	Zahŕňa krátkodobé, strednodobé alebo dlhodobé riziko alebo je uplatniteľné v akomkoľvek časovom horizonte.	Krátkodobý, strednodobý, dlhodobý, akákoľvek
Úroveň rozhodovania	Týka sa rizika na strategickú, taktickú alebo prevádzkovú/operatívnu úroveň.	Strategická, taktická, prevádzková/operatívna
Zaťažiteľnosť potrebných informácií/údajov	Úroveň potrebných zaťažiteľných informácií alebo údajov.	Vysoká, stredná, nízka
Odborné poznatky	Úroveň odbornosti požadovaná na správne použitie.	Nízka: intuitívna alebo jednoduchá až dvojzložková príprava. Príkladom: prípravný kurz trvá ako dva dni. Vysoká: vyžaduje značnú prípravu alebo odborné poznatky.
Kvalitatívna – kvantitatívna	Či je metóda kvalitatívna, semikvantitatívna alebo kvantitatívna.	Kvantitatívna Kvalitatívna Semikvantitatívna Môže sa použiť kvantitatívna alebo kvalitatívna (jedna alebo druhá).
Vynaložené úsilie	Na použité techniky sú potrebné čas a náklady.	Vysoká, stredná, nízka

Norma STN EN IEC 31010:2021



Nástroje a techniky	Proces používania rizika					Číslo
	Identifikácia rizika	Analýza rizika			Hodnotenie rizika	
		Následok	Pravdepodob- nosť výskytu	Úroveň rizika		
ALARP, ALARA a SFAIRP	NA	NA	NA	NA	SA	B.2.2
Bayesovská analýza (angl. Bayesian analysis)	NA	NA	SA	NA	NA	B.5.2
Bayesovská sieť (angl. Bayesian network)	NA	NA	SA	NA	SA	B.5.3
Analýza typu mozítk (angl. Bow tie analysis)	A	SA	A	A	A	B.4.2
Brainstorming	SA	A	NA	NA	NA	B.1.2
Analýza dopadu na podnikanie (angl. Business impact analysis)	A	SA	NA	NA	NA	B.5.4
Mapovanie príčin (angl. Causal mapping)	A	A	NA	NA	NA	B.6.1
Analýza príčin a následkov (angl. Cause-consequence analysis)	A	SA	SA	A	A	B.5.5
Kontrolné zoznamy, klasifikácie a taxonomie (angl. Checklists, classifications and taxonomies)	SA	NA	NA	NA	NA	B.2.2
Condynický prístup (angl. Condynic approach)	SA	NA	NA	NA	NA	B.3.2
Matrica následkov/pravdepodobnosť výskytu (angl. Consequence/likelihood matrix)	NA	A	A	SA	A	B.10.3
Analýza nákladov a prínosov (angl. Cost/benefit analysis)	NA	SA	NA	NA	SA	B.9.2
Analýza krízových vplyvov (angl. Crisis impact analysis)	NA	NA	SA	NA	NA	B.6.2
Analýza rozhodovacieho stromu (angl. Decision tree analysis)	NA	SA	SA	A	A	B.9.3
Technika Delphi (angl. Delphi technique)	SA	NA	NA	NA	NA	B.1.3
Analýza stromu udalostí (angl. Event tree analysis)	NA	SA	A	A	A	B.5.6
Spôsob porúch a analýza vplyvov (angl. Failure modes and effects analysis)	SA	SA	NA	NA	NA	B.2.3
Spôsob vplyvov porúch a analýza kritickosti (angl. Failure modes and effects and criticality analysis)	SA	SA	SA	SA	SA	B.2.3
Analýza stromu porúch (angl. Fault tree analysis)	A	NA	SA	A	A	B.5.7
Frekvénčnô/časové diagramy (angl. F-N diagrams)	A	SA	SA	A	SA	B.8.3
Teória hier (angl. Game theory)	A	SA	NA	NA	SA	B.9.4

Použitelnosť techník

v procese riadenia rizík podľa normy ISO 31000:2018



Číslo	Technika	Opis	Aplikácia	Úroveň použitia	Časový horizont	Úroveň rozhodovania	Zachovaná potrebnosť informácií/údajov	Odberaná personália	Kvalitatívna/kvantitatívna/semikvantitatívna	Vynáhodné zisky
B.2	ALARP/SPARP	Kritériá na rozhodovanie o výnámennosti rizika a prostriedky na hodnotenie tolerovateľnosti rizika	hodnotí riziko	organizácia	aplikovať	strategická/technická	vysoká	vysoká	kvalitatívna/kvantitatívna	vysoká
B.3.2	Bayesovská analýza (angl. Bayesian analysis)	Nástroj na vyhodnotenie logického vzťahu o parametroch modelu pomocou Bayesovskej vety, ktorý má schopnosť zachovávať empirické údaje do predchádzajúcich vplyvov pravdepodobnosti	analýza/analýza/analýza	akumulovať	aplikovať	akumulovať	stredná	vysoká	kvantitatívna	stredná
B.3.3	Bayesovská sieť/Diagramy vplyvov (angl. Bayesian network/Influence diagrams)	Grafický model premenlivých a ich vplyvov príčin a následkov vzájomnej pomoci pravdepodobnosti. Základná Bayesovská sieť má premenlivé predstavujúce nastavenie. Rozšírená sieť, ktorá ako diagram vplyvov, obsahuje premenlivé predstavujúce nastavenie, následky a vplyvy.	identifikovať vplyvy/analýza/analýza	akumulovať	aplikovať	akumulovať	stredná	vysoká	kvantitatívna	stredná/vysoká
B.4.2	Analýza typu mozík (angl. Bow tie analysis)	Schematický spôsob opisu vzťahu príčin rizika a vplyvov rizika v rozhodovaní a predikovaní následkov škodlivých rizika.	analýza/analýza/analýza	projekt/organizácia	kritická/analýza	akumulovať	nízka	nízka/prestředná	kvalitatívna/semikvantitatívna	nízka
B.1.2	Brainstorming	Technika používaná na generovanie/identifikáciu na podporu tvorby systému.	analýza/analýza	akumulovať	aplikovať	akumulovať	nízka	nízka/prestředná	kvalitatívna	nízka
B.5.4	Analýza dopadu na podnikanie (angl. Business impact analysis)	Proces BIA analyzuje následky rušivých incidentov na organizáciu, ktorý určuje priority obnovy produktov a služieb organizácie, a typ a priority škodlivých a závažných, ktoré ich dodávajú.	analýza/analýza/analýza	organizácia	kritická/analýza	technická	stredná	nízka	kvalitatívna	stredná

A: použitelná (angl. applicable); SA: veľmi dobre použitelná (angl. strongly applicable); NA: nepoužitelná (angl. not applicable).



ISO 37301:2021

- Čo je norma ISO 37301:2021
- Požiadavky normy ISO 37301:2021 v oblasti riadenia rizík

Systemy manažérstva súladu (zhody)

Norma ISO 37301:2021



FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/FDIS
37301

ISO/TC 309
Secretariat: BSI
Voting begins on:
2021-01-01
Voting terminates on:
2021-02-26

**Compliance management systems —
Requirements with guidance for use**

*Systèmes de management de la conformité — Exigences et
recommandations pour la mise en oeuvre*

TC

STANDARDS BY ISO/TC 309

Governance of organizations

Filter: ☒ Published standards ☐ Standards under development ☐ Withdrawn standards ☐ Projects deleted

Filter the list

STANDARD AND/OR PROJECT UNDER THE DIRECT RESPONSIBILITY OF ISO/TC 309 SECRETARIAT (3) ↓

STAGE

ICS

ISO 37001:2016

Anti-bribery management systems — Requirements with guidance for use

60.60

03.100.01
03.100.02
03.100.70

ISO 37002:2021

Whistleblowing management systems — Guidelines

60.60

03.100.01
03.100.02
03.100.70

ISO 37301:2021

Compliance management systems — Requirements with guidance for use

60.60

03.100.01
03.100.02
03.100.70



Hlavný zámer a predmet normy

ISO 37301:2021



Zámer, použiteľnosť

- Norma špecifikuje **požiadavky** a poskytuje pokyny na návrh, vývoj, implementáciu, hodnotenie, udržiavanie a zlepšovanie efektívneho systému manažérstva súladu (zhody) v rámci organizácie.
- Je použiteľná pre **všetky typy** organizácií bez ohľadu na **typ, veľkosť** a **povahu** činnosti, ako aj na to, či je organizácia z verejného, súkromného alebo neziskového sektora.



Riadiaci orgán vs. Vrcholový manažment

- Všetky požiadavky uvedené v norme, ktoré sa týkajú riadiaceho orgánu, **sa vzťahujú** na vrcholový manažment v prípadoch, keď organizácia nemá riadiaci orgán ako samostatnú funkciu.



Kultúra, súlad, správanie

- Organizácie, ktorých cieľom je byť dlhodobo úspešné, musia vytvoriť a udržiavať **kultúru dodržiavania predpisov**, berúc do úvahy **potreby a očakávania zainteresovaných strán**.
- „Compliance“ je preto nielen základom, ale aj **príležitosťou** pre úspešnú a udržateľnú organizáciu. Compliance je neustály proces a **výsledok organizácie, ktorá si plní svoje povinnosti**.
- Udržiavanie súladu je možné tým, že sa **začlení do kultúry organizácie** a do **správania a prístupu ľudí**, ktorí pre ňu pracujú.



Integrácia a záväzky

- V rámci zachovania **nezávislosti** je vhodné, aby bol manažment súladu **integrovaný s inými procesmi riadenia organizácie** a jej prevádzkovými požiadavkami a postupmi.
- Efektívny systém manažérstva súladu v rámci celej organizácie umožňuje organizácii **preukázať svoj záväzok** dodržiavať príslušné zákony, regulačné požiadavky, priemyselné kódexy a organizačné normy, ako aj štandardy dobrej správy, všeobecne uznávané najlepšie postupy, etiku a očakávania komunity.



Riziká

- Uplatnenie **súladu v správaní ľudí** pracujúcich pre organizáciu závisí predovšetkým **od vedenia na všetkých úrovniach** a od **jasných hodnôt** organizácie, ako aj od uznania a implementácie opatrení na podporu kompatibilného správania.
- **Ak to tak nie je vo všetkých úrovniach organizácie, existuje riziko nedodržania.**



Zodpovednosť

- V mnohých jurisdikciách súdy **pri určovaní pokuty**, ktorá sa má uložiť **za porušenie príslušných zákonov**, zväžili záväzok organizácie **dodržiavať pravidlá** prostredníctvom **systému manažérstva súladu**.
- Regulačné a súdne orgány preto môžu z normy tiež ťažiť.

Systémy manažérstva súladu a riadenie rizík

Norma ISO 37301:2021



- Organizácie sú čoraz viac presvedčené, že **použitím záväzných hodnôt a vhodného manažmentu dodržiavania predpisov** môžu **zaistiť ich integritu** a **vyhnúť sa** alebo **minimalizovať** nedodržiavanie povinností organizácie týkajúcich sa dodržiavania súladu.



Jedným z cieľov normy ISO 37301 je pomôcť organizáciám rozvíjať a **široť pozitívnu kultúru dodržiavania predpisov**, pričom sa domnieva, že **účinné a správne riadenie rizík** spojených s **dodržiavaním predpisov** by sa malo považovať **za príležitosť**, ktorú je potrebné sledovať a brať vzhľadom na niekoľko výhod, ktoré poskytuje organizácii, ako napríklad:

- zlepšovanie **podnikateľských príležitostí** a **udržateľnosti**;
- ochrana a posilnenie **reputácie** a **dôveryhodnosti** organizácie;
- zohľadnenie **očakávaní** zainteresovaných strán;
- preukázanie **záväzku** organizácie **efektívne a účinne riadiť riziká** súvisiace s dodržiavaním predpisov;
- zvýšenie **dôvery** tretích strán v schopnosť organizácie dosiahnuť trvalý úspech;
- **minimalizácia rizika**, že dôjde k rozporom s tým spojenými nákladmi a **poškodením** dobrej povesti.

Vybrané termíny a definície

Norma ISO 37301:2021



RIZIKO

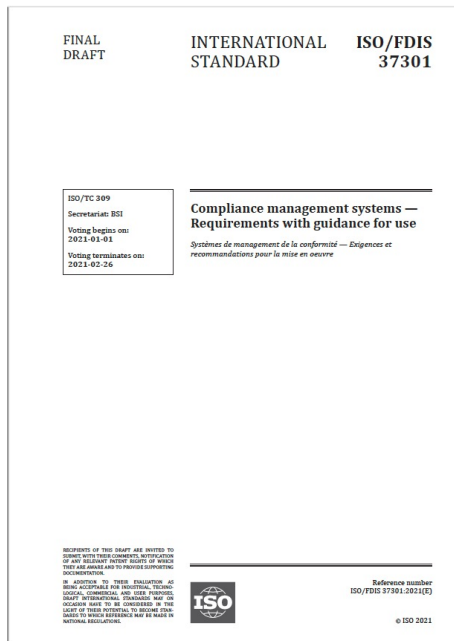
účinok neistoty na ciele.



- **Riziko súladu (compliance risk)**
pravdepodobnosť výskytu a následky nedodržania povinností organizácie v súvislosti so súladom (zhodou).
- **Povinnosti súladu (compliance obligations)**
požiadavky, ktoré musí organizácia povinne spĺňať, ako aj tie, ktoré sa organizácia dobrovoľne rozhodne splniť.
- **Súlad (compliance)**
splnenie všetkých povinností organizácie o dodržiavaní predpisov.
- **Nesúlad (noncompliance)**
nedodržanie neplnenie povinností týkajúcich sa súladu.

Systémy manažérstva súladu (zhody)

Norma ISO 37301:2021 - Požiadavky



4.4 Systémy manažérstva súladu

- Systém musí **zohľadniť** hodnoty, ciele, stratégiu a **riziká súladu organizácie** s prihliadnutím na kontext organizácie.

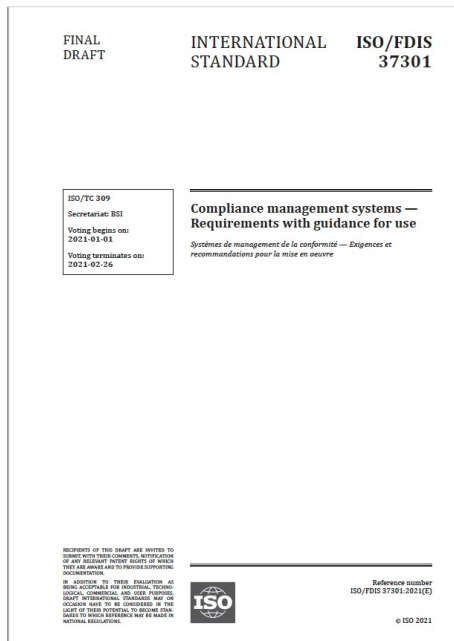


4.6 Posudzovanie rizík súladu s požiadavkami

- Organizácia musí **identifikovať**, **analyzovať** a **hodnotiť** svoje **riziká súladu** na základe posúdenia rizika súladu.
- Organizácia musí identifikovať **riziká** súvisiace s **dodržiavaním súladu** so svojimi **povinnosťami** v oblasti súladu so svojimi **činnosťami, produktami, službami** a príslušnými aspektmi svojich činností.
- Organizácia musí posúdiť **riziká** súvisiace s dodržiavaním predpisov súvisiace s **outsourcovanými procesmi** a **procesmi tretích strán**.
- **Riziká** súladu sa musia hodnotiť **pravidelne** a vždy, keď dôjde k **podstatným zmenám okolností** alebo organizačného kontextu.
- Organizácia musí uchovávať **zdokumentované informácie** o hodnotení **rizika** súladu a o opatreniach na riešenie svojich rizík súladu.

Systemy manažérstva súladu (zhody)

Norma ISO 37301:2021 - Požiadavky



6.1 Opatrenia na riešenie rizík a príležitostí

- Pri plánovaní systému manažérstva súladu musí organizácia vziať do úvahy vplyvy uvedené v bode 4.1 a požiadavky uvedené v bode 4.2 a **určiť riziká a príležitosti**, ktoré je potrebné riešiť, aby sa:
 - poskytla záruka, že systém manažérstva súladu môže dosiahnuť zamýšľané výsledky;
 - predchádzalo alebo znižovalo nežiaduce účinky;
 - dosiahlo neustále zlepšovanie.
- Pri plánovaní systému manažérstva súladu musí organizácia vziať do úvahy: ciele (6.2); identifikované povinnosti (4.4); výsledky posudzovania rizika (4.5).
- Organizácia musí naplánovať:
 - a) opatrenia na riešenie týchto rizík a príležitostí;
 - b) ako: 1) integrovať a implementovať opatrenia do svojich procesov systému manažérstva súladu; 2) vyhodnotiť účinnosť týchto opatrení.

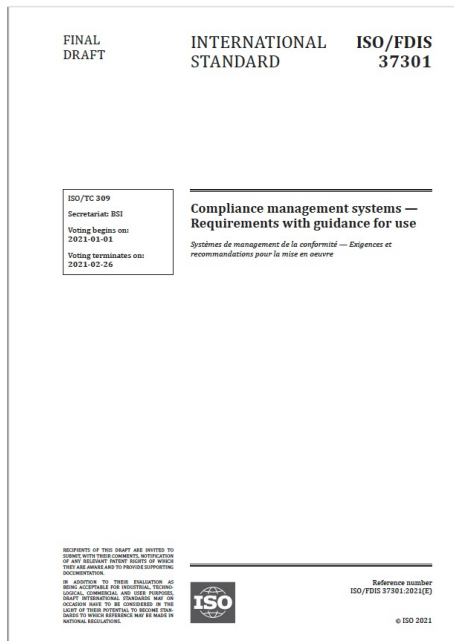


8.1 Plánovanie a riadenie prevádzky

- Organizácia musí plánovať, implementovať a riadiť procesy potrebné na splnenie požiadaviek a implementovať **opatrenia** uvedené v článku 6.

Systemy manažérstva súladu (zhody)

Norma ISO 37301:2021 - Požiadavky



8.2 Určenie riadenia a postupov



- Organizácia musí implementovať riadiace činnosti na zaistenie svojich povinností v oblasti dodržiavania súladu a **súvisiacich rizík** v súvislosti s dodržiavaním predpisov. Tieto kontroly sa musia udržiavať, pravidelne kontrolovať a testovať, aby sa zaistila ich nepretržitá účinnosť.

9.1.2 Spätná väzba



- Organizácia musí zaviesť, implementovať, hodnotiť a udržiavať procesy na hľadanie a prijímanie spätnej väzby o svojich výkonoch v oblasti dodržiavania súladu z rôznych zdrojov. Informácie sa analyzujú a kriticky vyhodnotia, aby sa zistili **hlavné príčiny** nedodržiavania predpisov, aby sa zabezpečilo **prijatie vhodných opatrení** a aby sa tieto informácie premietli do **pravidelného hodnotenia rizika** požadovaného v bode 4.5.

9.3 Preskúmanie manažmentom



- V rámci preskúmania manažmentom musí byť zohľadnená primeranosť posudzovania rizík súvisiacich s dodržiavaním súladu.



Analýza typu „motýlik“

- Metodika analýzy
- Použitelnost analýzy v rámci plnění požadavků normy ISO 37301:2021

Nástroje a techniky pre posudzovanie rizík

Norma STN EN IEC 31010:2021



Zdroj: STN EN IEC 31010 | SUTN (unms.sk)

B.4 Techniky na analyzovanie radiacích činností

Techniky sa môžu použiť na kontrolu vhodnosti a adekvátnosti radiacích činností.

Analýza typu motýlik identifikuje bariéry medzi zdrojom rizika a jeho možnými následkami a možno ich použiť na kontrolu dostatočnosti týchto bariér.

Analýza typu motýlik

- Je grafické znázornenie ciest od príčin udalosti k jej následkom. Zobrazuje radiace činnosti, ktoré modifikujú pravdepodobnosť výskytu udalosti, a tie, ktoré modifikujú následky, ak sa udalosť stane.
- Diagram typu motýlik možno zostaviť na základe stromu porúch a stromu udalostí, ale častejšie ich kreslí tím priamo podľa scenára workshopu.
- Analýza sa spracováva v grafickej podobe ako diagram typu motýlik.
- Výhodou diagramu je jeho prehľadnosť a zrozumiteľnosť, znázorňuje možné preventívne a reaktívne opatrenia na zmiernenie následkov rizika.
- Diagram je vhodný na vysvetlenie podstaty rizika a vhodnosti navrhovaných opatrení na zvládanie rizika a pre tímovú diskusiu o navrhovaných opatreniach.
- Cieľom analýzy nie je detailná technická analýza a prepočet pravdepodobnosti výskytu, ale jednoduché znázornenie mechanizmu vzniku a následkov rizika, doplnené o:
 - preventívne pôsobiace bariéry, resp. radiace akcie, ktoré by mohli zabrániť vzniku rizika.
 - reaktívne radiace akcie na zabránenie, resp. zmiernenie následkov rizika a obnovu funkcií systému, resp. prevádzky, v prípade ak riziko nastane.

Analýza typu motýlik

Norma STN EN IEC 31010:2021 – Diagram typu motýlik (BTA - Bow Tie Analysis)



Diagram typu motýlik sa kreslí takto:

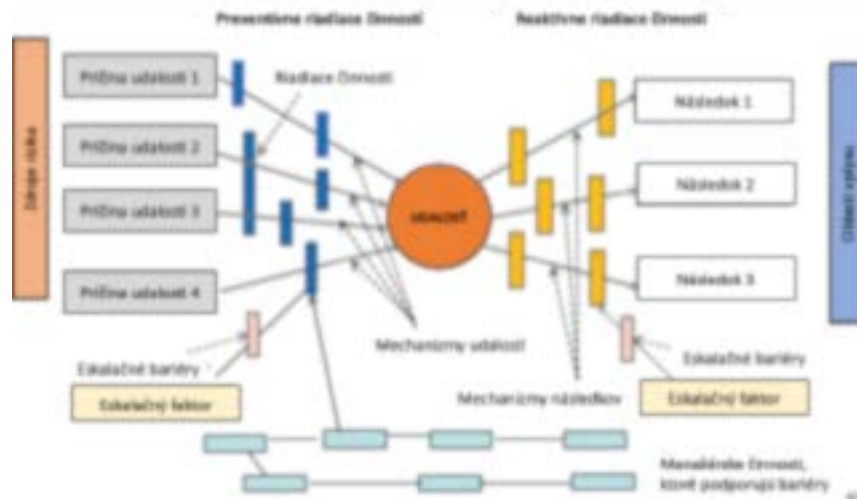
- **Udalosť**, ktorá je predmetom analýzy, predstavuje **stredový uzol** motýlika.
- **Zdroje rizika** sú uvedené na **ľavej strane** uzla a sú **spojené s uzlom** lúčovitými čiarami predstavujúcimi rôzne mechanizmy, pomocou ktorých môžu zdroje rizika viesť k udalosti.
- **Bariéry** alebo **radiace činnosti** pre každý mechanizmus sú zobrazené ako **zvislé čiar** cez lúčovité čiar.
- Na pravej strane od stredového uzla sú nakreslené lúčovité čiar, ktoré **smerujú od udalosti do každého potenciálneho následku**.
- Zvislé pruhy za udalosťou predstavujú **reaktívne radiace činnosti** alebo **bariéry**, ktoré **modifikujú následky**.
- **Faktory**, ktoré môžu spôsobiť **zlyhanie radiacích činností** (eskalačné faktory), pridávajú sa spolu s radiaciami činnosťami pre **eskalačné faktory**.
- **Manažérske funkcie**, ktoré **podporujú radiace činnosti** (ako sú školenia a dozor), môžu byť zobrazené pod motýlikom a spojené s príslušnou radiacou činnosťou.

Určitá úroveň kvantifikácie diagramu typu motýlik je možná, ak sú cesty nezávislé, je známa pravdepodobnosť konkrétneho následku alebo výsledku a ak možno odhadnúť pravdepodobnosť zlyhania radiacej činnosti. V mnohých situáciách však cesty a bariéry nie sú nezávislé a radiace činnosti môžu byť procedurálne a ich efektívnosť nieistá. Kvantifikácia sa často vhodnejšie vykonáva pomocou analýzy stromu poruchových stavov a analýzy stromu udalostí alebo LOPA (Analýza ochranných vrstiev).



Zdroj: STN EN IEC 31010 | SUTN (unms.sk)

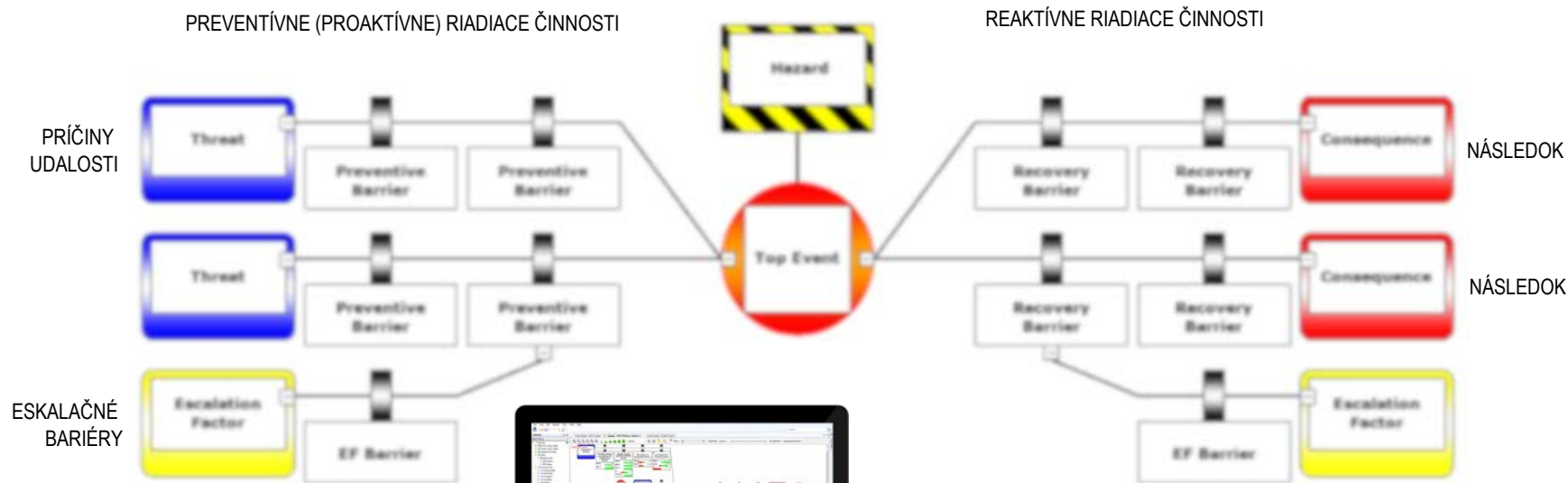
Základný nástroj

[illegible]

Zdroj: STN EN IEC 31010 | SUTN (unms.sk)

Postup tvorby diagramu typu motýlik

Myšlienková mapa



ZDROJ: BowTieXP - Bowtie Software - CGE Risk

- "Bowtie" je diagram, ktorý **vizualizuje riziko**, s ktorým sa zaoberáte len v **jednom**, ľahko pochopiteľnom obrázku.
- Diagram je tvarovaný ako motýlik, čo vytvára **jasnú diferenciáciu medzi proaktívnym a reaktívnym riadením rizík**.
- Sila diagramu spočíva v tom, že poskytuje prehľad o **viacerých pravdepodobných scenároch** v jednom obrázku.
- Stručne povedané, poskytuje jednoduché vizuálne vysvetlenie rizika, ktoré by bolo oveľa ťažšie vysvetliť inak.

Myšlienková mapa



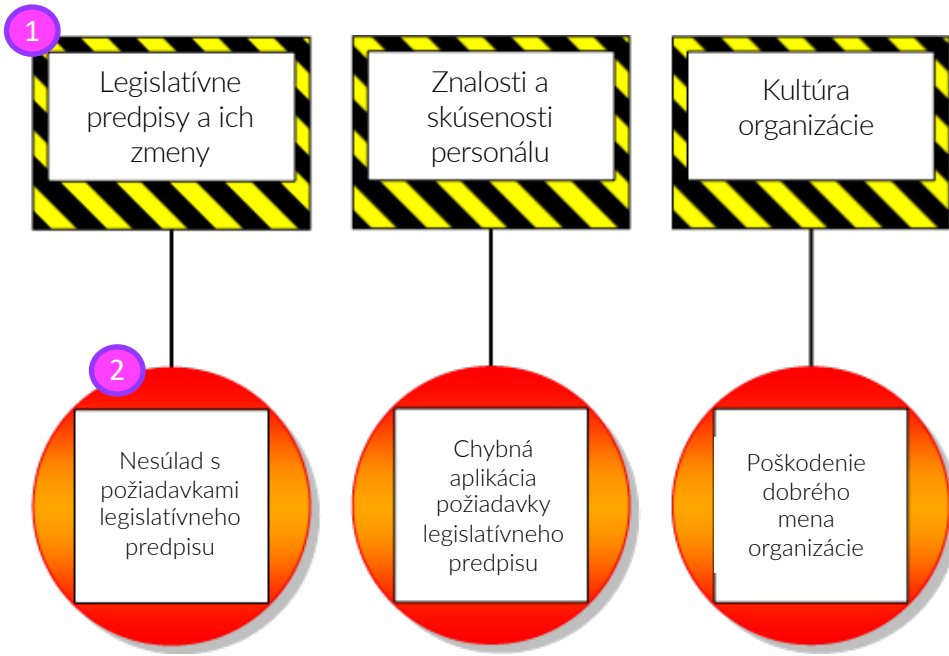
Postup tvorby diagramu

1. a 2. krok: Určite zdroj a udalosť



ZDROJ

UDALOSŤ



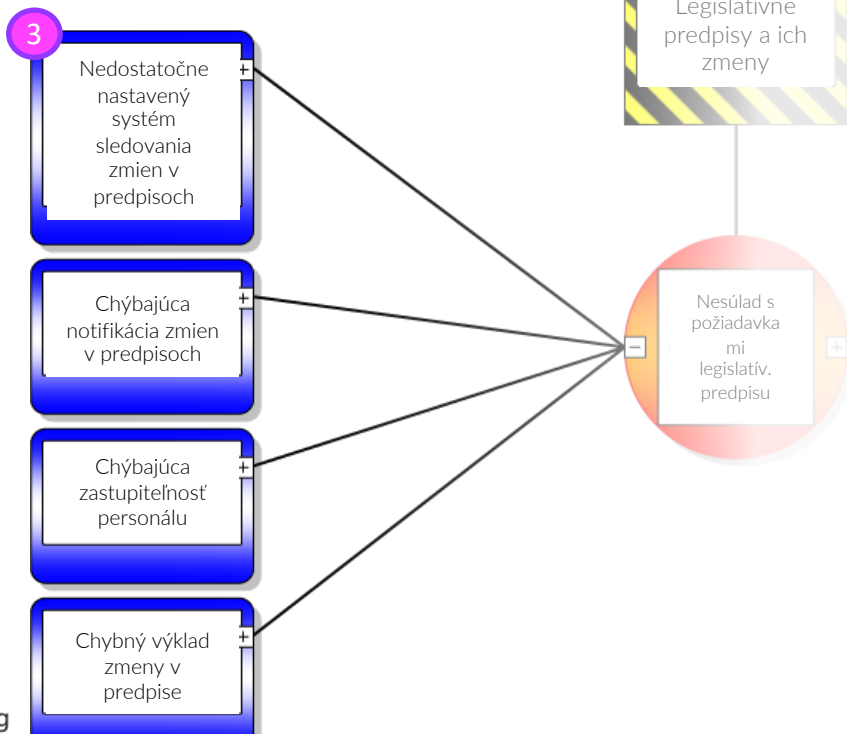
- Začiatok každého „motýlika“ je **ZDROJ**. Zdroj je niečo v organizácii, v jej okolí alebo v jej časti, čo má **potenciál spôsobiť škodu**. Zámerom je nájsť oblasti (aspekty), ktoré sú súčasťou organizácie a mohli by mať **negatívny vplyv**, ak sa stratí kontrola nad týmto aspektom. Bowties sa vytvárajú len pre tie zdroje, ktoré majú **vysoký potenciál spôsobiť rozsiahle škody**. Za normálnych okolností je **5 až 10 zdrojov** dobrým východiskovým bodom.
- Po určení ZDROJA je ďalším krokom definovanie kľúčovej **UDALOSTI**. Toto je okamih, keď sa **stratí kontrola nad zdrojom**. Zatiaľ **nie sú žiadne škody ani negatívne vplyvy**, ale je to možné. To znamená, že udalosť sa určuje **predtým**, ako by mohla **začať** spôsobovať skutočné škody. Udalosť je však voľbou, aký je presný okamih, kedy sa kontrola stratí? Je to do veľkej miery **subjektívna a pragmatická voľba**. Vrcholná udalosť je často **preformulovaná** po dokončení zvyšku motýlika.

Postup tvorby diagramu

3. krok – Určite príčiny



PRÍČINY UDALOSTI



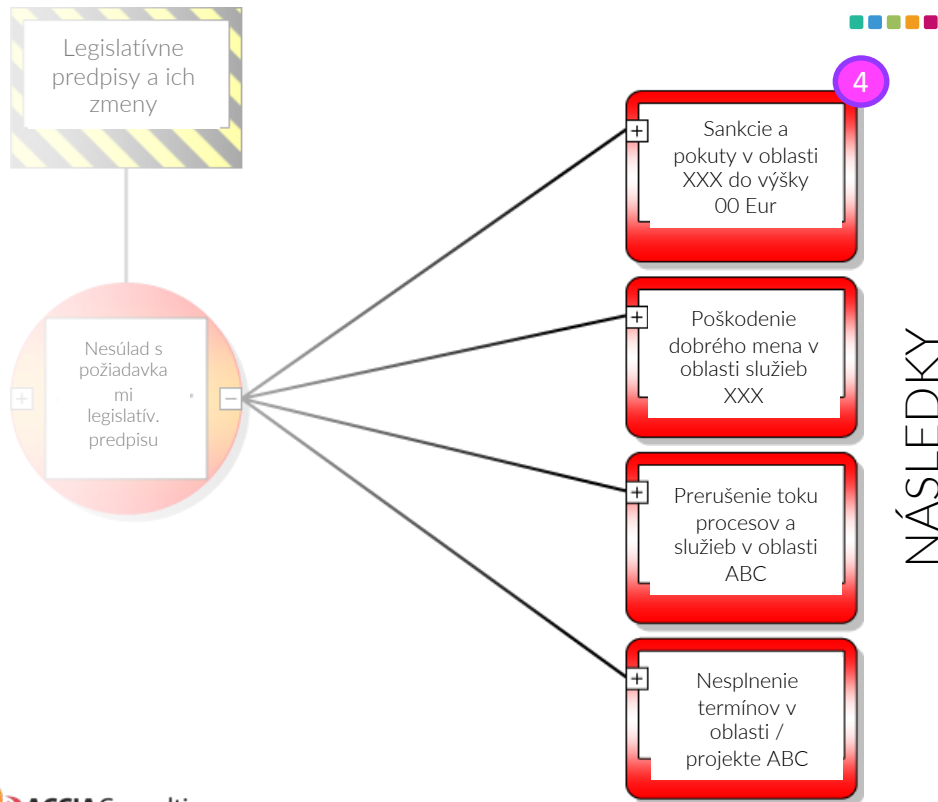
PRÍČINY sú to, čo spôsobuje kľúčovú udalosť. Môže byť identifikovaných viacero PRÍČIN. Je potrebné sa vyhnúť všeobecným formuláciám, ako je "ľudská chyba", "nedostatok informácií" alebo "zle nastavený systém".

Je potrebné si pomôcť **doplňujúcimi otázkami**: Čo vlastne človek robí, aby spôsobil kľúčovú udalosť? Aké informácie sú dôležité? Aké požiadavky majú vplyv na systém?

Je potrebné **byť konkrétny** a pomôcť si **doplňujúcou analýzou**, napr. Analýza koreňových príčin (RCA).

Postup tvorby diagramu

4. krok – Určite následky



NÁSLEDKY sú **výsledkom** kľúčovej udalosti. Udalosť môže mať viac ako jeden následok.

Rovnako ako v prípade príčin, ľudia majú tendenciu zamerať sa **na všeobecné konštatovania** namiesto opisu konkrétnych následkov.

Snažte sa nezameriavať sa napr. na všeobecné konštatovania ako „sankcie a pokuty“, „poškodenie mena“, „finančná strata“. Ide skôr o **širšie kategórie škôd než opisy konkrétnych následkov udalosti**.

Konkrétne určenie následkov okrem toho, že obsahujete **podrobnejšie informácie**, pomáha myslieť konkrétnejšie **pri riešení bariér**. Už teraz premýšľajte o tom, ako chcete zabrániť napr. „sankciám a pokutám“.

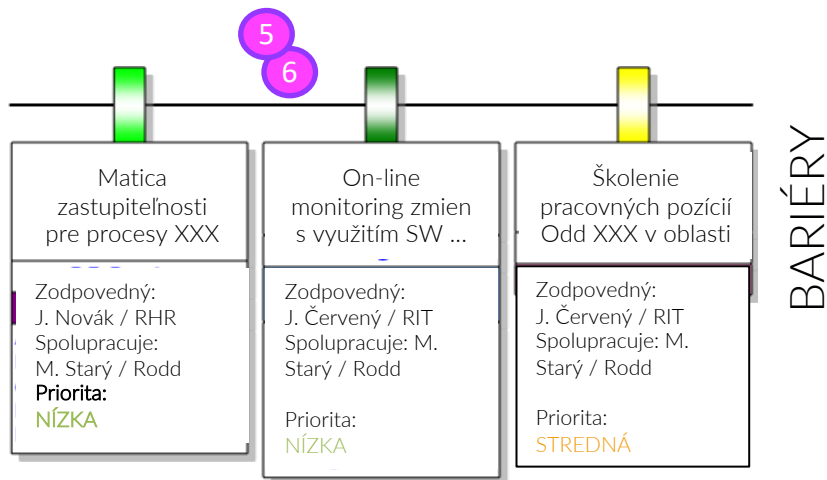
Druhým je skutočný scenár, ktorý uľahčuje vymýšľanie konkrétnych prekážok.

V tejto fáze máme **jasné pochopenie rizika** a toho, **čo je potrebné kontrolovať**. Zdroj, udalosť, príčiny a následky nám poskytujú **prehľad** o všetkom, čo nechceme aby nastalo v súvislosti s identifikovanou udalosťou.

Každý riadok motýlika predstavuje iný potenciálny incident. Okrem toho, že obsahuje scenáre incidentov, ktoré sa už mohli vyskytnúť, časť sily motýlika spočíva v tom, že existuje aj priestor pre scenáre, ktoré sa ešte nestali. To z neho robí veľmi proaktívny prístup.

Postup tvorby diagramu

5. a 6. krok – Určite bariéry (kontrola neželaných scenárov)



BARIÉRY (riadiace činnosti) v motýliku sa objavujú na oboch stranách kľúčovej udalosti.

Bariéry na **ľavej strane** „prerušujú“ scenár tak, aby sa príčiny nevyskytovali, a ak áno, nemali za následok **stratu kontroly**.

Bariéry na **pravej strane** zabezpečujú, že ak **nastane kľúčová udalosť**, scenár sa nevystupňuje do **reálneho následku** (vplyvu) a/alebo zmierňujú následok (vplyv).

Existujú **rôzne typy bariér**, ktoré sú kombináciou ľudského správania, SW/HW, informácií, postupov, riadiacich mechanizmov a pod.

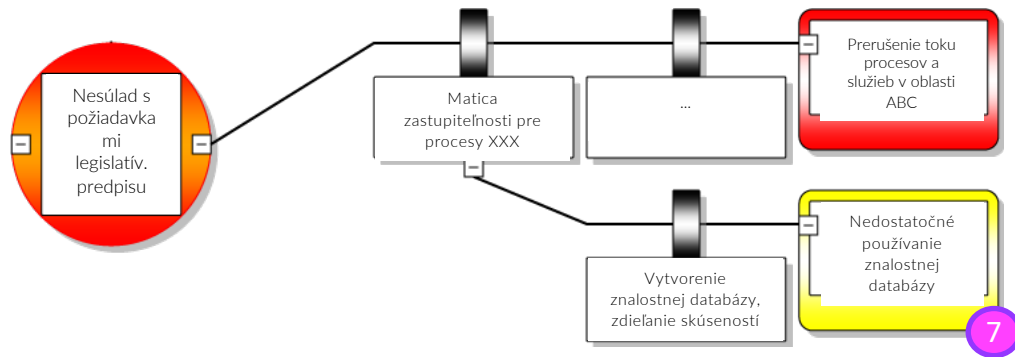
Akonáhle sú bariéry identifikované, máte **základné pochopenie toho, ako sa riadia riziká**. Môžete ďalej stavať na tejto základnej „bariérovej“ štruktúre, aby ste **prehľadli svoje chápanie toho, kde sú silné a slabé stránky**.

Je možné testovať účinnosť bariéry. To umožňuje posúdiť, ako dobre bariéra funguje alebo sa očakáva, že bude fungovať, na základe dostupných údajov a/alebo je možné sa spoliehať sa na odborný úsudok. Okrem toho môžete určiť, **kto je zodpovedný za bariéru a posúdiť kritickosť bariéry v kontexte všetkých ostatných súvisiacich informácií**. To sú všetko veci, ktoré je možné urobiť, aby sa zlepšilo chápanie bariér.

V konečnom dôsledku prepojenie a vizualizácia všetkých týchto informácií o bariére poskytuje holistický prehľad o bezpečnostných opatreniach s relevantnými meta údajmi v kontexte rizikových scenárov.

Postup tvorby diagramu

5. a 6. krok – Určite bariéry (kontrola neželaných scenárov)



ESKALAČNÉ FAKTORY

Bariéry nie sú nikdy dokonalé...

Dokonca aj najlepšia bariéra môže zlyhať.

Vzhľadom na túto skutočnosť, čo potrebujete vedieť je, **prečo bariéra zlyhá**. To sa vykonáva pomocou **"ESKALAČNÉHO FAKTORA"**. Všetko, čo môže spôsobiť zlyhanie bariéry, sa dá opísať prostredníctvom eskalačného faktora.

Napríklad Matica zastupiteľnosti, môžu zlyhať, ak dôjde k výpadku zastupujúceho personálu z dôvodu choroby, štrajku, hromadného prepúšťania, rozsiahlej organizačnej zmeny a pod.

Upozornenie:

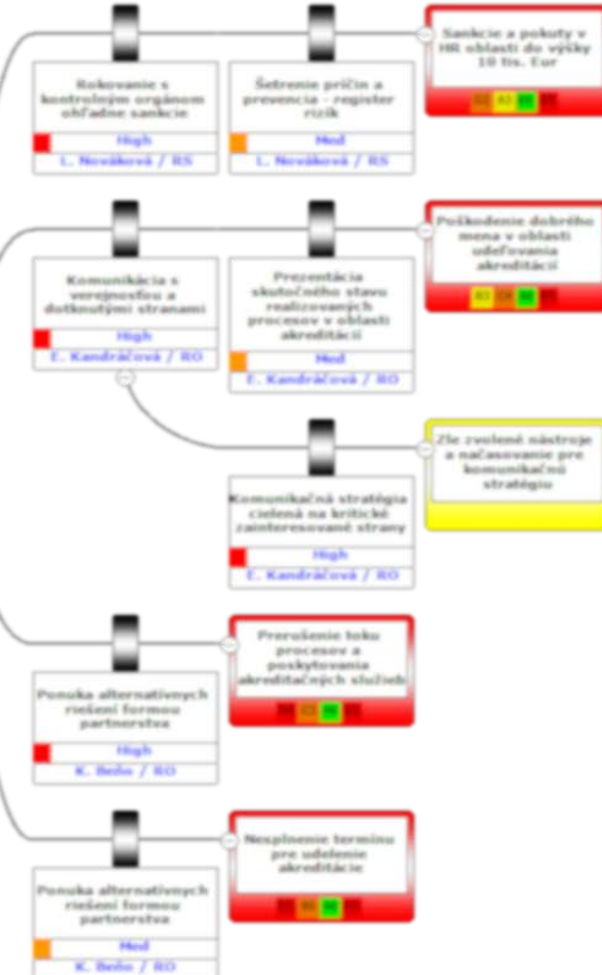
Dávajte si pozor na eskalačné faktory. Neopisujete všetky potenciálne režimy zlyhania. Popíšte len **skutočné nedostatky vášho kontrolného rámca** a ako to chcete zvládnuť.

Logickým ďalším krokom k riadeniu eskalačných faktorov je vytvorenie bariér pre eskalačné faktory, nazývané aj "bariéry eskalačného faktora". V tomto to má byť chápané ako „záložný generátor“.

PREVENTÍVNE RIADIACE ČINNOSTI



REAKTÍVNE RIADIACE ČINNOSTI



Analýza typu motýlik

Norma STN EN IEC 31010:2021 – Zhrnutie



Použitie

- Analýza typu motýlik sa používa na **zobrazenie a komunikáciu informácií o rizikách** v situáciách, keď má udalosť má **mnoho** možných príčin a následkov. Môže sa použiť na **podrobné preskúmanie príčin a následkov udalostí**, ktoré sa zaznamenávajú **jednoduchou formou do registra rizík**. Používa sa najmä na **analýzu udalostí so závažnejšími následkami**.
- Analýza typu motýlik sa používa na **preskúmavanie radiacích činností** na **kontrolu** toho, či každá cesta od príčiny k udalosti a od udalosti k následku má **účinné radiace činnosti** a či sú **rozpoznané faktory**, ktoré by **mohli spôsobiť zlyhanie radiacích činností** (vrátane zlyhaní systémov manažérstva). Môže sa použiť ako základ prostriedku na zaznamenanie informácií o riziku, pre ktoré sa **nehodí jednoduché lineárne znázornenie registra rizík**. Je možné ju proaktívne použiť na zvažovanie potenciálnych udalostí a tiež spätne na modelovanie udalostí, ktoré už nastali.
- Analýza typu motýlik sa používa, keď situácia **nezaručuje** zložitost' úplnej analýzy stromu poruchových stavov a analýzy stromu udalostí, ale je zložitejšia, ako ju možno predstaviť pomocou jedinej cesty príčina-udalosť-následok.
- V niektorých situáciách môžu byť vyvinuté **kaskádovité analýzy typu motýlik**, v ktorých sa **následky jednej udalosti stanú príčinou ďalšej udalosti**.

Vstupy

Vstupy zahŕňajú informácie o **príčinách** a **následkoch** vopred definovanej **udalosti** a o **radiacích činnostiach**, ktoré ju môžu modifikovať. Tieto informácie môžu byť **prevzaté z výstupov techník** na identifikáciu rizík a radiacích činností alebo zo skúseností jednotlivcov.

Výstupy

Výstupom je **jednoduchý diagram znázorňujúci hlavné cesty rizika, zavedené radiace činnosti a faktory, ktoré by mohli viesť k zlyhaniu radiacích činností**. Ukazuje tiež potenciálne následky a opatrenia, ktoré možno prijať na ich modifikáciu, ak udalosť nastane.

Silné a slabé stránky

Medzi silné stránky analýzy typu motýlik patria tieto okolnosti:

- Je **ľahko pochopiteľná** a poskytuje **jasné grafické znázornenie** udalosti, jej príčin a následkov.
- Zameriava pozornosť na radiace činnosti, ktoré sa majú zaviesť, a na ich efektívnosť.
- Môže sa použiť pre želané aj neželané následky.
- Na použitie **nepotrebuje vysokú úroveň odbornosti**.

Slabé stránky zahŕňajú tieto okolnosti:

- Analýza typu motýlik nemôže zobrazovať situáciu, keď cesty od príčin k udalosti nie sú nezávislé (t. j., kde by v strome poruchových stavov bol logický uzol „A“).
- Môže príliš zjednodušiť zložité situácie, najmä keď sa pokúša o kvantifikáciu.

**Be nice.
Be cool.
Be happy.
Everyday!
Forever!**



■ ADRESA

ACCIA, s.r.o.

Armádna 1655/5 I 911 01 Trenčín I Slovenská republika

IČO: 474 081 97, DIČ: 202 387 2268

IČDPH: SK 202 387 2268

■ TELEFÓN, EMAIL & WEB

+421 32 390 4132

accia@accia.sk, www.accia.sk

www.revizia9000.sk, www.rizika31000.sk

■ NÁJDETE NÁS AJ NA

<http://www.facebook.com/revizia.iso.9001>

<http://plus.google.com/+Revizia-iso9001Sk/posts>

<http://www.youtube.com/user/reviziais9001>

<https://www.twitter.com/AcciaConsulting/>

