



KONFERENCIA

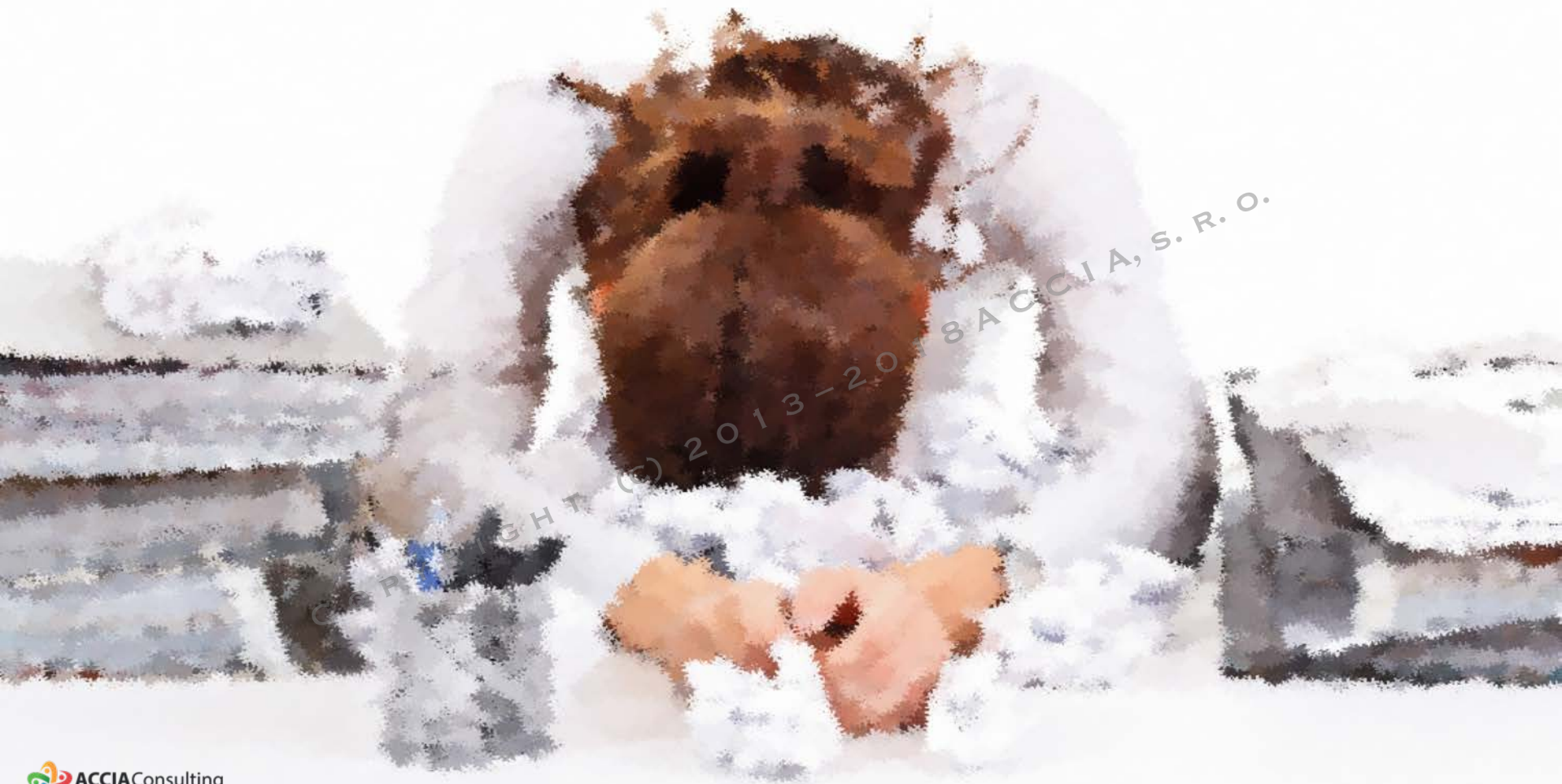
Riziká a ich manažment v kybernetickom priestore a
v podnikovej IT infraštruktúre

Nová norma ISO 31000:2018 Manažérstvo rizika a jej využitie v riadení IT rizík

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

dunikova@accia.sk

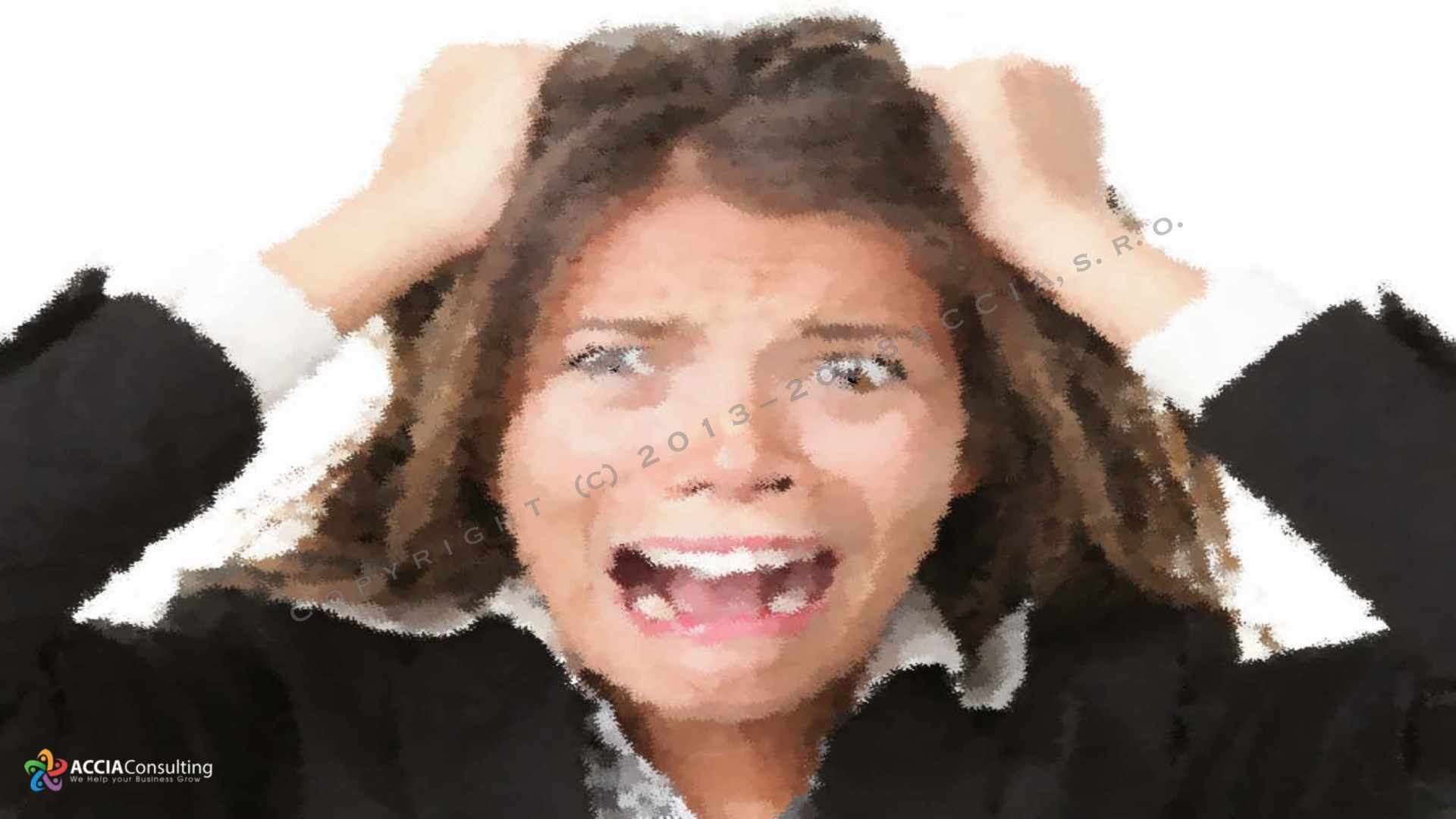
19.09.2018 Bratislava



COPYRIGHT (C) 2013-2018 ACCIA, S.R.O.

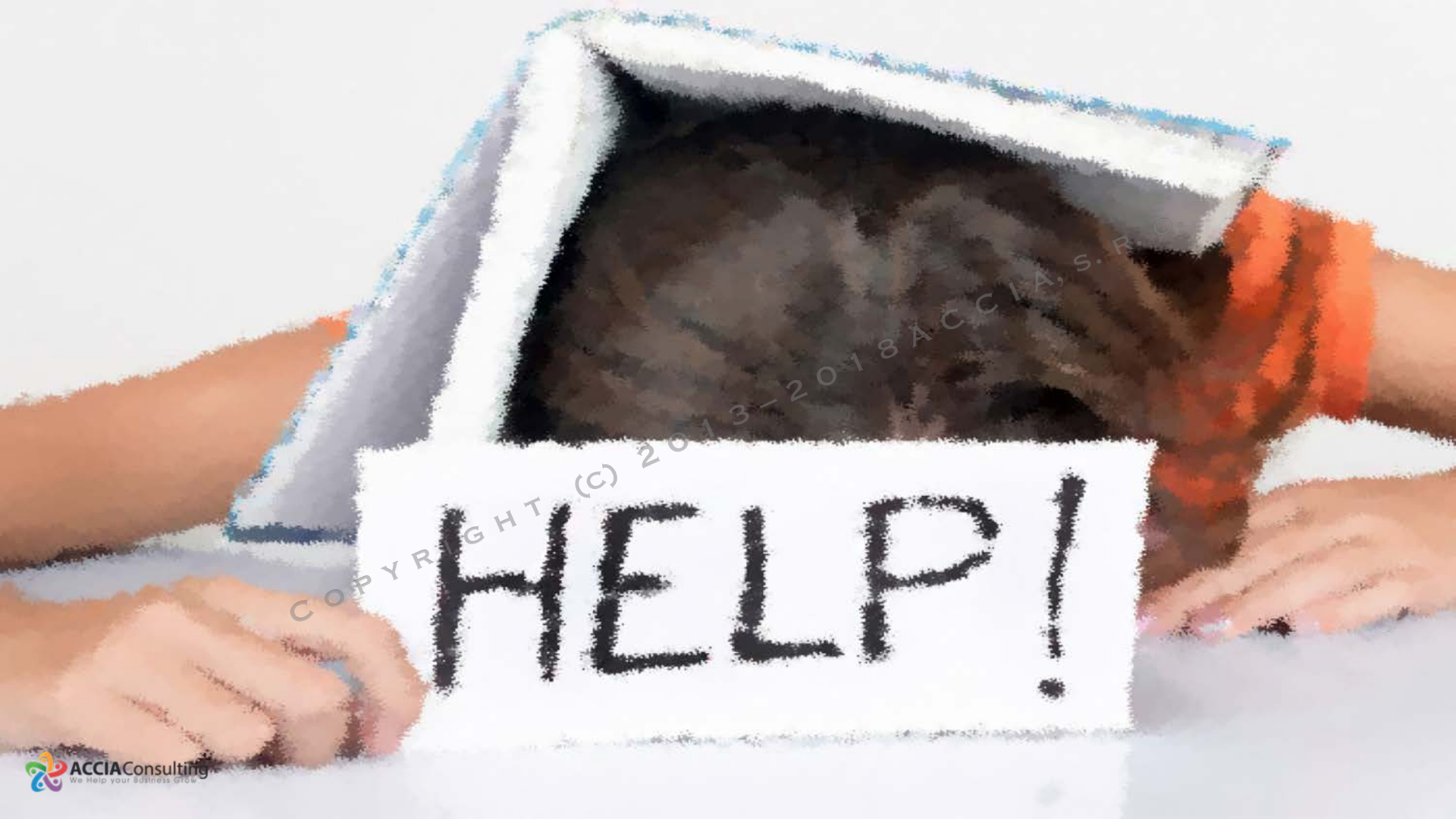


COPYRIGHT (C) 2013-2018 ACCIA, S.R.O.



COPYRIGHT (C) 2013-2018 ACCIA, S.R.O.

COPYRIGHT (C) 2013-2018 ACCIA, S. R. O.



COPYRIGHT (C) 2013-2018 ACCIA, S.R.L.

HELP!



COPYRIGHT (C) 2013-2018 ACCIA, S.R.O.



COPYRIGHT (C) 2013-2018 ACCIA, S. R. O.



ISO/TC 262 Risk Management

ISO/TC 262 Risk Management

Slovensko zastúpené TK 22 Kvalita



Manažérstvo rizika

Termíny a definície v oblasti manažérstva rizika, Návod na manažérstvo rizika, Nástroje a techniky pre posudzovanie rizík, atď.



Technická komisia

Viac ako 55 participujúcich krajín

Viac ako 18 pozorovateľov



ISO/TC 262
Risk management

zdroj: <https://www.iso.org/committee/629121.html>

Filters: ☒ Published standards ☒ Standards under development ☐ Withdrawn standards ☐ Projects deleted

Standard and/or project under the direct responsibility of ISO/TC 262 Secretariat (x)	Stage	ICS
☒ NP IWA 31 [Under development] Using ISO 31000 guidance on risk management in management systems	10.99	
☒ 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 31010:2009 Risk management -- Risk assessment techniques	90.92	03.100.01
☒ IEC/DIS 31010 [Under development] Risk management -- Risk assessment techniques	40.60	03.100.01
☒ ISO/WD 31022 [Under development] Risk management -- Guidelines for the management of legal risk	20.20	
☒ ISO/AWI 31030 [Under development] Risk management -- Managing travel risks -- Guidance for organizations	20.00	
☒ ISO/NP 31050 [Under development] Guidance for managing emerging risks to enhance resilience	10.99	

Web stránka

ISO/TC 262 Risk Management



Informácie

Manažérstvo rizika

Publikované a vydané normy, pripravované normy,
Case Study, prieskumy, rozhovory, atď.



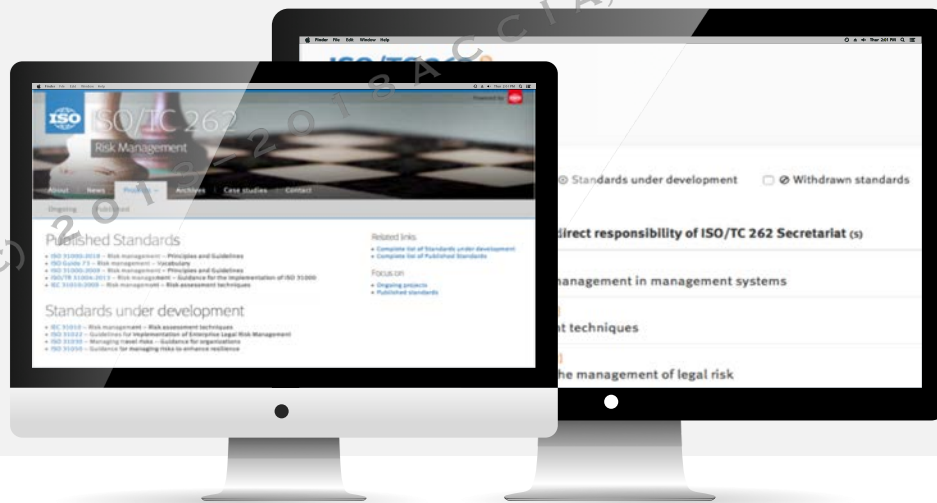
Novinky



Projekty



Prieskumy



zdroj: <https://committee.iso.org/home/tc262>

Normy radu ISO 31000

Aktuálny stav



ISO Guide 73:2009

Risk management – Vocabulary
(TNI 01 0350)

ISO 31000:2018

Manažérstvo rizika – Návod
(publikovaná 14.02.2018)

ISO/TR 31004:2013

Risk management – Guidance for
the implementation of ISO 31000

IEC 31010:2009

Risk management – Risk assessment
techniques (v revízii IEC/DIS 31010)

NP IWA 31

Using ISO 31000 guidance on risk
management in management
systems

Čo je nové ?

Pripravované normy v oblasti riadenia rizík



5

Nových noriem
pre riadenie rizík



ISO 31022 Návod na riadenie legislatívnych rizík v organizáciách

Riadenie legislatívnych rizík je dôležitou súčasťou celkového riadenia rizík



ISO 31050 Návod na riadenie novovznikajúcich rizík za účelom zvýšenia odolnosti

Nové prístupy na zvýšenie odolnosti organizácií pri riešení nových výziev, zvýšenie miery dôvery v riadení rizika



ISO 31030 Návod na riadenie rizík súvisiacich s cestovaním

Riadení rizík spojených s cestovaním, ktorým čelia organizácie



IEC 31010 Techniky pre posudzovanie rizík

Návod na výber a aplikáciu techník systematického posudzovania rizika.

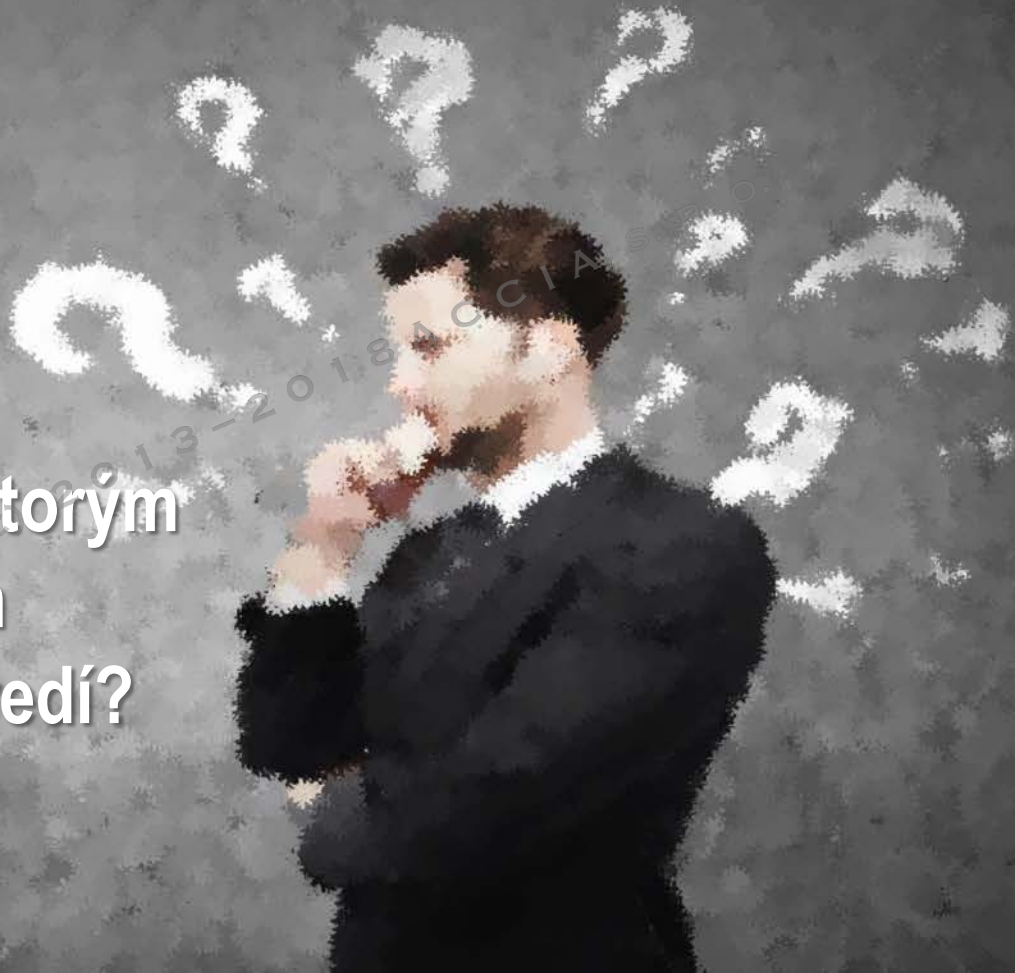


NP IWA 31

Návod na riadenie rizík v systémoch manažérstva

ČO MYSLÍTE,

ktoré riziká patria do
skupiny **TOP 10 rizík**, ktorým
čelia firmy v súčasnom
podnikateľskom prostredí?



Top 10 rizík

Kategórie rizík s najvyššou úrovňou rizikovosti



1. miesto

Poškodenie dobrého
mena spoločnosti



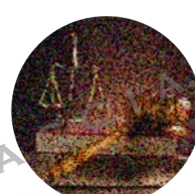
2. miesto

Spomalenie
hospodárskeho rastu



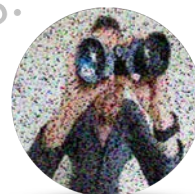
3. miesto

Nárast
konkurencie



4. miesto

Zmena zákonných a
iných požiadaviek



5. miesto

Počítačová kriminalita
(hacking, vírusy, škodlivé kódy)



6. miesto

Neschopnosť inovovať
včas produkty a služby



7. miesto

Neschopnosť prilákať a
udržať najväčšie talenty



8. miesto

„Business Interruption“
(Business Continuity)



9. miesto

Politická situácia a
neistota



10. miesto

Plnenie záväzkov voči
tretím stranám

Introduction

This document is for use by people who create, make decisions, control and deliver products and services.

Organizations of all types and sizes have many reasons whether they will achieve their objectives.

Managing risk is essential and enables organizations to achieve their objectives.

Managing risk is part of governance and leadership at all levels. It contributes to the organization's success.

Managing risk is part of all activities, including the organization's core business.

Managing risk considers the internal and external context and the organization's culture and values.

Managing risk is based on the principles, as described in [Figure 1](#). These principles are fundamental; they might need to be adapted to the organization.



Figure 1 — Principles

INTERNATIONAL STANDARD

ISO
31000

Second edition
2017-01

Risk management — Guidelines

Management de risque — Lignes directrices



Reference number
ISO 31000:2017

ISO 31000

COPYRIGHT (C) 2013-2017 ACCIA CONSULTING

...nikdy sa na 100 %
nedá vyhnúť riziku...

Norma ISO 31000:2018 vs. ISO 31000:2009

Manažerstvo rizika – Zásady a návod



ISO 31000:2009

Zdroj: www.iso.org



ISO 31000:2018

Zdroj: www.iso.org

Najväčšie zmeny

Norma ISO 31000:2018



Zásady

Preskúmanie zásad manažérstva rizika, ktoré sú kľúčovými kritériami pre jeho úspech



Vodcovstvo

Zdôraznenie vodcovstva vrcholového manažmentu a integrácie manažérstva rizika v rámci organizácie



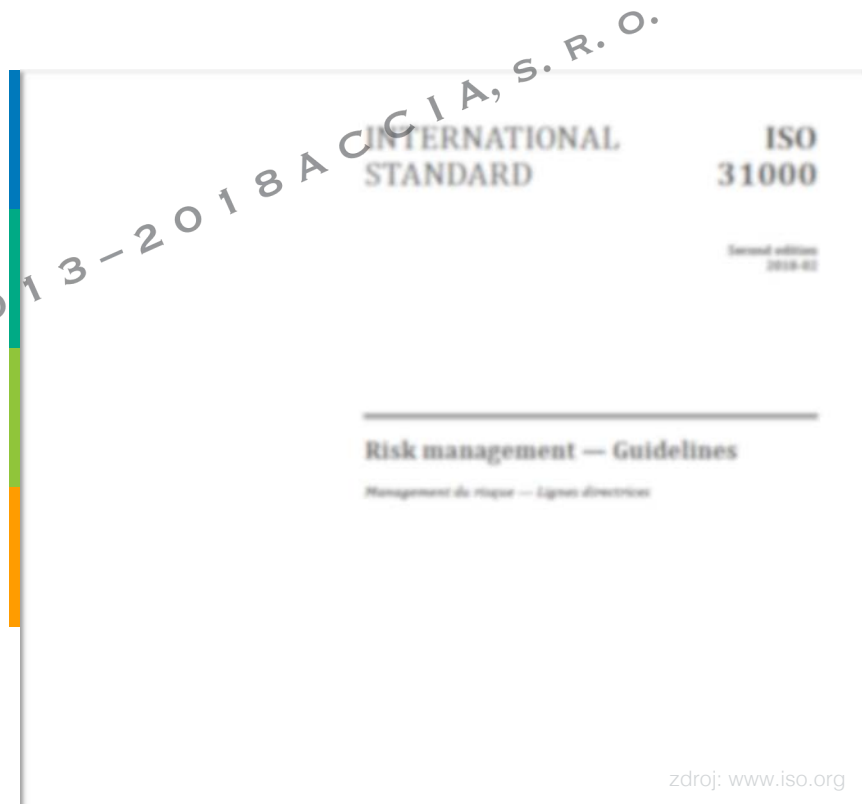
Opakovateľnosť

Väčší dôraz na opakujúci sa charakter manažérstva rizika, nové skúsenosti, poznatky a analýzy môžu v každej fáze procesu viesť k revízii procesných prvkov, činností a riadenia



Zjednodušenie

Zjednodušenie obsahu so zvýšeným zameraním sa na udržanie modelu otvorených systémov tak, aby vyhovoval viacerým potrebám a súvislostiam



Zásady

Norma ISO 31000:2018



Od čoho závisí úspešnosť
riadenia rizík ???



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**.



Zdroj: www.iso.org

Termíny a definície

ISO 31000:2018



Zníženie počtu termínov a definícií. Norma ISO Guide 73:2009 Risk management – Vocabulary

1

Riziko

účinnok neistoty na ciele

2

Manažérstvo rizika

koordinované činnosti riadenia a kontroly organizácie s ohľadom na riziko

3

Zúčastnená strana

osoba alebo organizácia, ktorá môže ovplyvniť, byť ovplyvnená alebo sa cíti byť ovplyvnená rozhodnutím alebo činnosťou

4

Zdroj rizika

prvok, ktorý sám alebo v kombinácii môže spôsobiť riziko

5

Udalosť

výskyt alebo zmena konkrétneho súboru okolností

6

Následok

výsledok udalosti ovplyvňujúci ciele

7

Vierohodnosť

možnosť, že sa niečo stane

8

riadenie / riadiaca činnosť

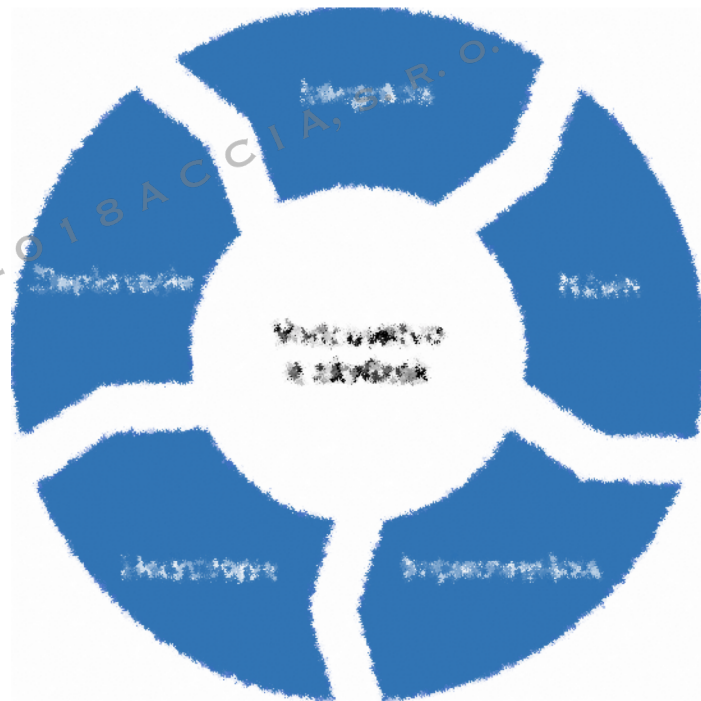
opatrenie, ktoré udržiava a/alebo modifikuje riziko

V terminológii manažérstva rizika sa slovo „**vierohodnosť**“ používa na označenie možnosti, že sa **niečo môže stať**, či už definované, merané alebo určené objektívne alebo subjektívne, kvalitatívne alebo kvantitatívne, a opísané pomocou všeobecných pojmov alebo matematicky (napríklad pravdepodobnosť alebo frekvencia počas daného časového obdobia).

Anglický pojem „**vierohodnosť**“ nemá v niektorých jazykoch priamy ekvivalent; namiesto toho sa často používa ekvivalent pojmu „**pravdepodobnosť**“. Avšak v angličtine je „pravdepodobnosť“ často užšie interpretovaná ako matematický pojem. Preto sa v terminológii manažérstva rizika používa „vierohodnosť“ s úmyslom, že má rovnaký široký výklad, aký má termín „pravdepodobnosť“ v mnohých jazykoch iných ako angličtina.

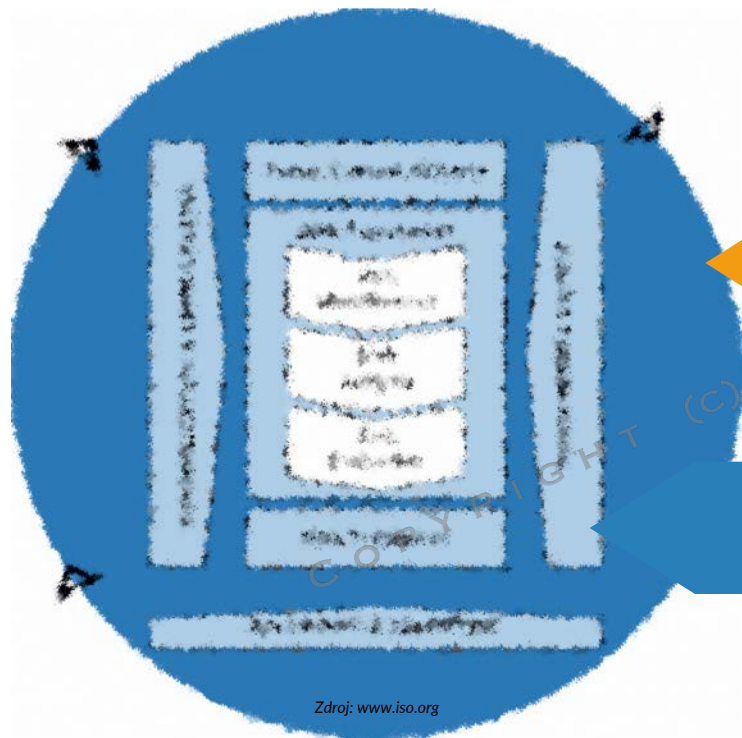
Rámec manažérstva rizika

ISO 31000:2018



Čo potrebujeme ?

Manažérstvo rizika



Zdroj: www.iso.org

1

Predmet, súvislosti, kritériá

Čo, kedy, prečo, ako, s čím, kde ?



2

Identifikácia rizika

Čo sa môže stať ?



3-4

Analýza a hodnotenie rizika

Prečo a ako sa to môže stať?

Ako závažný bude dopad?



5

Riešiť riziká/príležitosti

Čo môžeme urobiť už teraz v predstihu?



6-7

Monitorovať a preskúvať

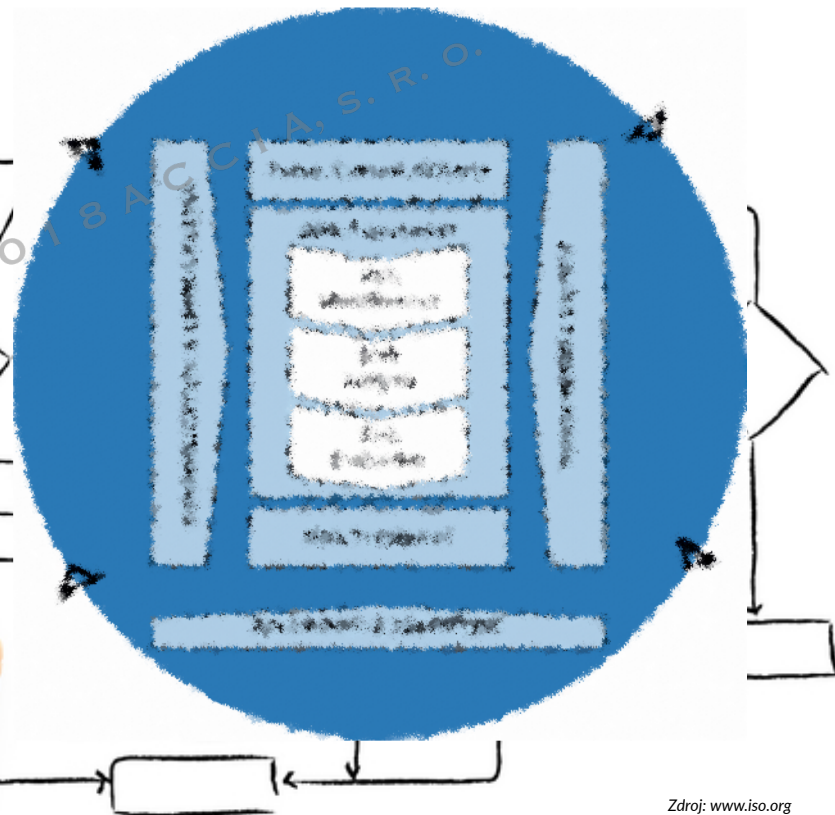
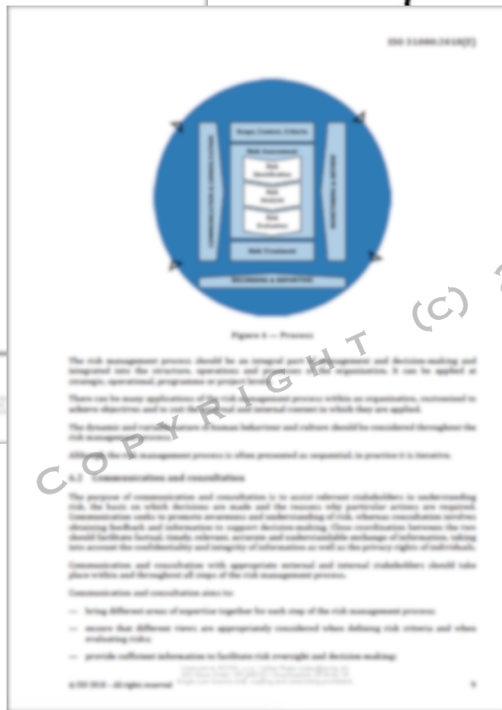
Komunikovať riziká/príležitosti

Zmenilo sa niečo, koho sa to dotýka?



Proces manažérstva rizika

ISO 31000:2018





Zdroj: ČSN EN 31010:2011

Nástroje pre posudzovanie rizika

Norma IEC 31010



Použitelnosť

Veľmi dobre použiteľná – (SA – Strongly Applicable)

Použiteľná – (A – Applicable)

Nepoužiteľná – (NA – Not Applicable)



Metóda B29 Matica následkov a pravdepodobností

Pravdepodobnosť (probability) vs. Vierohodnosť (likelihood)

PRÍLEŽITOSŤ (+)							HROZBA (-)							
Pravdepodobnosť (P)	veľmi vysoká	5	5	10	15	20	25	25	20	15	10	5	5	veľmi vysoká
	vysoká	4	4	8	12	16	20	20	16	12	8	4	4	vysoká
	stredná	3	3	6	9	12	15	15	12	9	6	3	3	stredná
	nízka	2	2	4	6	8	10	10	8	6	4	2	2	nízka
	veľmi nízka	1	1	2	3	4	5	5	4	3	2	1	1	veľmi nízka
		1	2	3	4	5	5	4	3	2	1			
		veľmi nízky	nízky	stredný	vysoký	veľmi vysoký	veľmi vysoký	vysoký	stredný	nízky	veľmi nízky			
Pozitívny dopad (D)							Negatívny dopad (D)							



Vyhľadávacie metódy

- Kontrolné zoznamy
- Predbežná analýza nebezpečenstiev

Podporné metódy

- Brainstorming
- Štruktúrované / semištruktúrované rozhovory
- Delphi
- Štruktúra "Čo sa stane keď?" (SWIFT)
- Analýza bezporuchových činností človeka (HRA)

Analýza scenárov

- Analýza koreňových príčin
- Analýza scenárov
- Toxikologické posudzovanie rizík
- Analýza dopadov na podnikanie
- Analýza stromu poruchových stavov
- Analýza stromu udalostí
- Analýza vzťahu príčina-následok
- Analýza príčin a dôsledkov

Štatistické metódy

- Markovova analýza
- Simulácia Monte Carlo
- Bayesovská štatistika a Bayesove siete

Analýza funkcií

- Analýza spôsobov a dôsledkov porúch (FMEA/FMECA)
- Údržba zameraná na bezporuchovosť
- Analýza parazitných javov
- Štúdia nebezpečenstiev a prevádzkyschopnosti (HAZOP)
- Analýza nebezpečenstiev a kritických kontrolných bodov (HACCP)

Posudzovanie prvkov riadenia rizika

- Analýza ochranných vrstiev (LOPA)
- Analýza typu motýlik

Opatrenia na riešenie rizík

Výber možností na zaobchádzanie s rizikom – preventívne opatrenia



Čo robiť ???



1. Vyhnutie sa riziku

na základe rozhodnutia
nezačať alebo nepokračovať v
činnosti, ktorá spôsobuje riziko



2. Akceptácia/ Zvýšenie rizika

za účelom využitia príležitosti



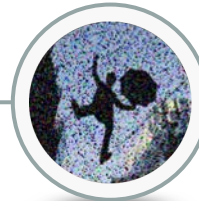
6. Zdieľanie rizika 7. Udržanie rizika

s ďalšou stranou – zákazníkom,
dodávateľom, atď.



4.-5. Zmena pravdepodobnosti / následkov rizika

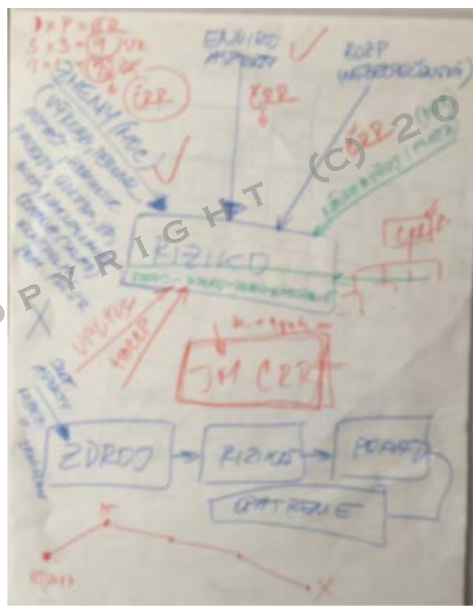
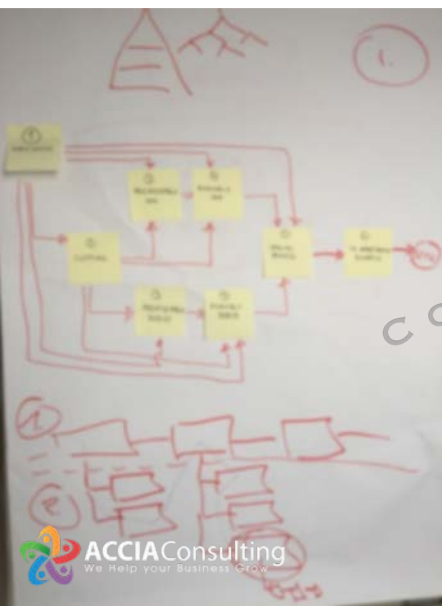
sprísená kontrola, vyškolenie
personálu, poisťné zásoby, atď.



3. Odstránenie zdroja rizika

Čo spôsobuje riziko?
(personál, proces, materiál, atď.)





PROTOCOL ZHIVY + SPRYO4 + M. ENIL

ПРАВДЕПОСВУОС

		1	2	3	3		
1	1	2	3	3	2	1	
2	2	4	6	6	4	2	
3	3	6	9	9	6	3	

1 - 100%

2 - 100%

3 - 100%

4 - 100%

5 - 100%

6 - 100%

7 - 100%

8 - 100%

9 - 100%

10 - 100%

11 - 100%

12 - 100%

13 - 100%

14 - 100%

15 - 100%

16 - 100%

17 - 100%

18 - 100%

19 - 100%

20 - 100%

21 - 100%

22 - 100%

23 - 100%

24 - 100%

25 - 100%

26 - 100%

27 - 100%

28 - 100%

29 - 100%

30 - 100%

31 - 100%

32 - 100%

33 - 100%

34 - 100%

35 - 100%

36 - 100%

37 - 100%

38 - 100%

39 - 100%

40 - 100%

41 - 100%

42 - 100%

43 - 100%

44 - 100%

45 - 100%

46 - 100%

47 - 100%

48 - 100%

49 - 100%

50 - 100%

51 - 100%

52 - 100%

53 - 100%

54 - 100%

55 - 100%

56 - 100%

57 - 100%

58 - 100%

59 - 100%

60 - 100%

61 - 100%

62 - 100%

63 - 100%

64 - 100%

65 - 100%

66 - 100%

67 - 100%

68 - 100%

69 - 100%

70 - 100%

71 - 100%

72 - 100%

73 - 100%

74 - 100%

75 - 100%

76 - 100%

77 - 100%

78 - 100%

79 - 100%

80 - 100%

81 - 100%

82 - 100%

83 - 100%

84 - 100%

85 - 100%

86 - 100%

87 - 100%

88 - 100%

89 - 100%

90 - 100%

91 - 100%

92 - 100%

93 - 100%

94 - 100%

95 - 100%

96 - 100%

97 - 100%

98 - 100%

99 - 100%

100 - 100%

Nerobte veci zložito...

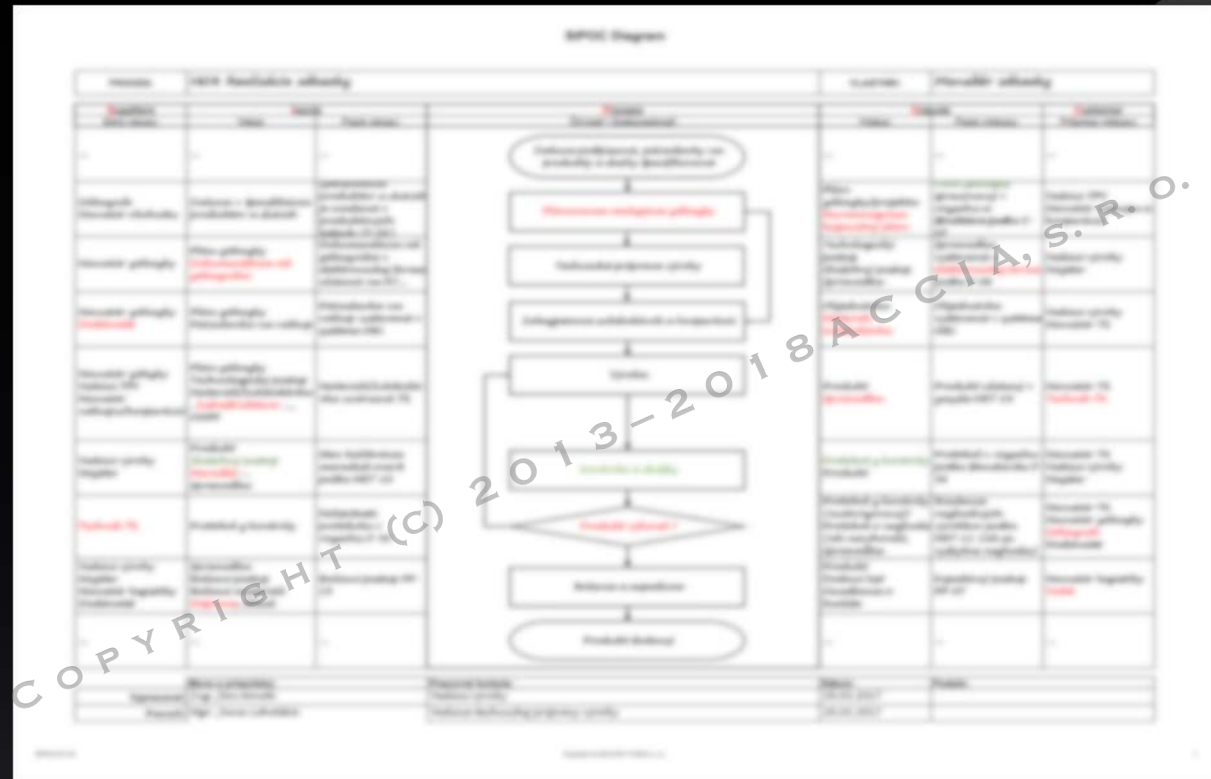
K.I.S.S.

stupid :-)





COPYRIGHT (C) 2013-2018 ACCIA, S. R. O.



Keywords: interrupted; interrupted-syllable; syllable

[illegible]

Model pro posouzení rizik a příležitostí

První část - Riziková analýza

Identifikace	Popis rizika	Pravděpodobnost	Důležitost	Stupeň rizika
1	Riziko	Pravděpodobnost	Důležitost	Stupeň rizika
2	Riziko	Pravděpodobnost	Důležitost	Stupeň rizika
3	Riziko	Pravděpodobnost	Důležitost	Stupeň rizika
4	Riziko	Pravděpodobnost	Důležitost	Stupeň rizika
5	Riziko	Pravděpodobnost	Důležitost	Stupeň rizika
6	Riziko	Pravděpodobnost	Důležitost	Stupeň rizika

Druhá část - Příležitostná analýza

Identifikace	Popis příležitosti	Pravděpodobnost	Důležitost	Stupeň příležitosti
1	Příležitost	Pravděpodobnost	Důležitost	Stupeň příležitosti
2	Příležitost	Pravděpodobnost	Důležitost	Stupeň příležitosti
3	Příležitost	Pravděpodobnost	Důležitost	Stupeň příležitosti
4	Příležitost	Pravděpodobnost	Důležitost	Stupeň příležitosti
5	Příležitost	Pravděpodobnost	Důležitost	Stupeň příležitosti
6	Příležitost	Pravděpodobnost	Důležitost	Stupeň příležitosti

Třetí část - Kombinovaná analýza

Identifikace	Popis	Pravděpodobnost	Důležitost	Stupeň
1	Kombinovaná	Pravděpodobnost	Důležitost	Stupeň
2	Kombinovaná	Pravděpodobnost	Důležitost	Stupeň
3	Kombinovaná	Pravděpodobnost	Důležitost	Stupeň
4	Kombinovaná	Pravděpodobnost	Důležitost	Stupeň
5	Kombinovaná	Pravděpodobnost	Důležitost	Stupeň
6	Kombinovaná	Pravděpodobnost	Důležitost	Stupeň

Čtvrtá část - Závěrečná analýza

Identifikace	Popis	Pravděpodobnost	Důležitost	Stupeň
1	Závěrečná	Pravděpodobnost	Důležitost	Stupeň
2	Závěrečná	Pravděpodobnost	Důležitost	Stupeň
3	Závěrečná	Pravděpodobnost	Důležitost	Stupeň
4	Závěrečná	Pravděpodobnost	Důležitost	Stupeň
5	Závěrečná	Pravděpodobnost	Důležitost	Stupeň
6	Závěrečná	Pravděpodobnost	Důležitost	Stupeň

COPYRIGHT (C) 2013-2018 ACCIA, S. R. O.

Table with multiple columns and rows, featuring a large diagonal watermark: **COPYRIGHT (C) 2013-2018 ACCIA, S.R.O.**

...čo ešte dodať...

„Život je ako bonboniéra,
nikdy neviete čo si vyberiete.“

...alebo viete...???



Kto sme

ACCIA Consulting



Milan ROJKO
Vladimíra DUNÍKOVÁ

Stratégia > strategické riadenie

Procesy > procesné riadenie

Projekty > projektové riadenie

Ľudia > riadenie kompetencií

Znalosti > riadenie znalostí

Riziká > riadenie rizík a príležitostí



Nájdete nás aj na:

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

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

<http://www.youtube.com/user/reviziaiso9001>

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

Naše internetové projekty:

www.revizia9001.sk | www.rizika31000.sk



Naše skúsenosti

...nestali sme sa expertmi za jednu noc...

Prax - Konzultácie

viac ako 20 rokov
skúseností

Projekty

viac ako 30
realizovaných projektov

Workshopy

viac ako 700
pracovných workshopov

Vzdelávanie

viac ako 900 vzdelávacích
a prezentačných aktivít

Ľudia

viac ako 1000
vyškolených ľudí

Členstvo v organizáciách:

TK22 Kvalita pri ÚNMS SR – sme člen technickej komisie

ISO/TC 262 Risk Management – zastupujeme Slovensko v technickej komisii

SPPR – Slovenská spoločnosť pre projektové riadenie – sme člen

IRCA – máme medzinárodnú certifikáciu CQI-IRCA QMS Lead Auditor

ASQ – American Society for Quality – sme člen

PECB – Certification Body for persons, organizations, and products – sme partner



I ♥
REVISION

■ ADRESA

ACCIA, s.r.o.

Armádna 1655/5 | 911 01 Trenčín | 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/>

