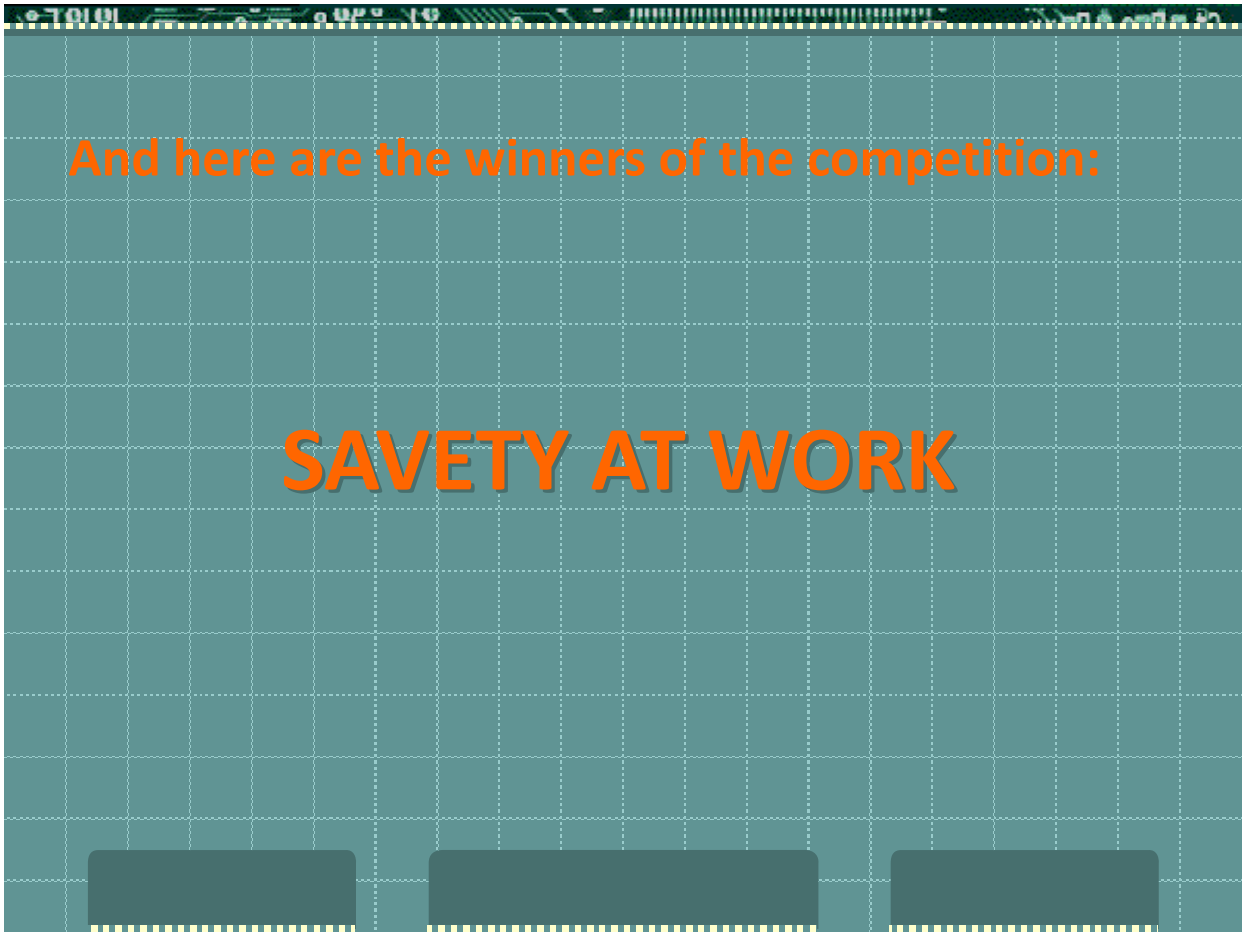
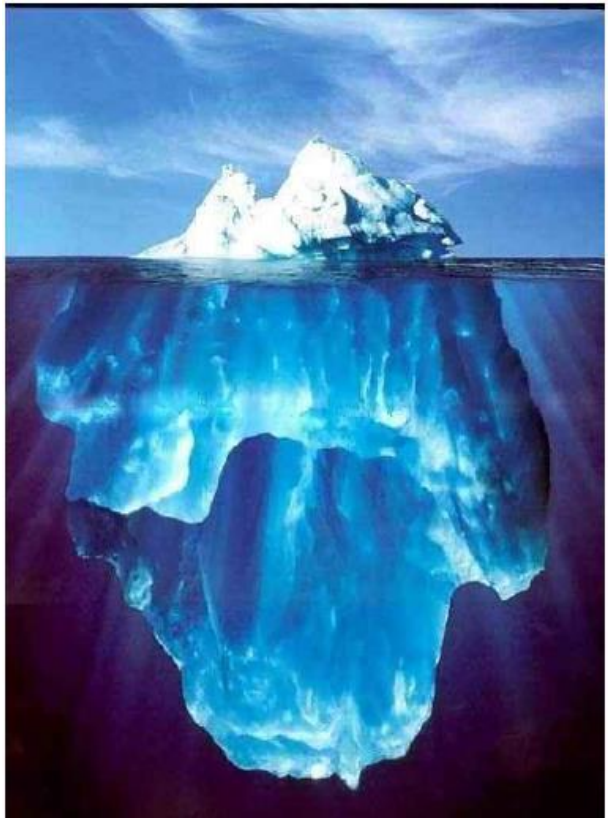
Analýza rizik
Metoda 1

Proč?

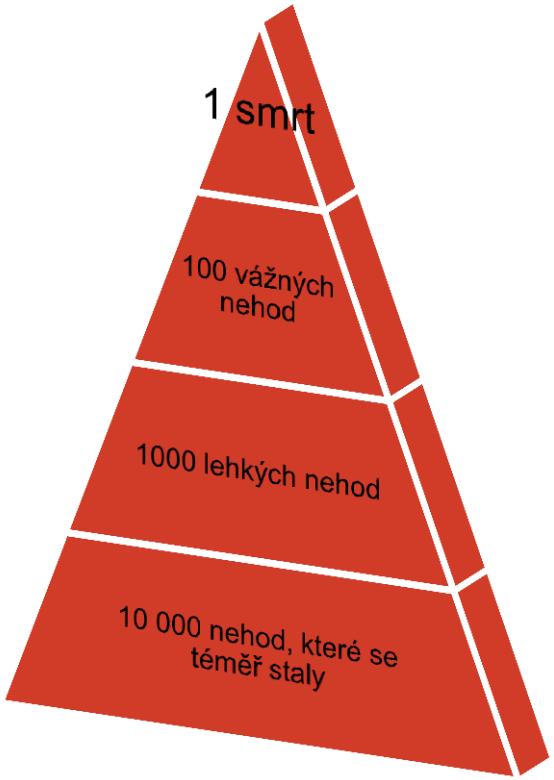
Bezpečnost práce



Pyramida bezpečnosti



Existuje vztah mezi počtem nehod, kterým jsme se těsně vyhnuli a počtem nehod vážných. Heinrich 1931



Analýza rizik - představení

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | About us

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TR 27008
ISO/IEC 27009
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC TR 27019
ISO/IEC 27021
ISO/IEC TR 27023
ISO/IEC 27030
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035
ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039

ISO/IEC 27005:2018 — Information technology — Security techniques — **Information security risk management** (*third edition*)

Introduction

The ISO27k standards are deliberately risk-aligned, meaning that organizations are encouraged to assess risks to their information (called "information security risks" in the ISO27k standards, but in reality they are simply **information risks**) as a prelude to treating them in various ways. Dealing with the most significant **information risks** first makes sense from the practical implementation and management perspectives.

Scope of the standard

The standard 'provides guidelines for information security risk management' and 'supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.'

It cites ISO/IEC 27000 as a normative (essential) standard, and mentions ISO/IEC 27001, ISO/IEC 27002 and ISO 31000 in the content. NIST standards are referenced in the bibliography.

Content of the standard

At 66 pages, ISO/IEC 27005 is a substantial standard although around two-thirds is comprised of annexes with examples and additional information.

The standard doesn't specify, recommend or even name any specific risk management method. It does however imply a continual process consisting of a structured sequence of activities, some of which are iterative:

- Establish the risk management context (*e.g.* the scope, compliance obligations, approaches/methods to be used and relevant policies and criteria such as the organization's risk tolerance or appetite);
- Quantitatively or qualitatively assess (*i.e.* identify, analyze and evaluate) relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a 'level of risk';
- Treat (*i.e.* modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately, using those 'levels of risk' to prioritize them;
- Keep stakeholders informed throughout the process; and
- Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes.

Extensive appendices provide additional information, primarily examples to demonstrate the recommended approach.

Status of the standard

The *third* edition of ISO/IEC 27005 was published in July 2018. This is a "minor revision", a temporary stop-gap measure with very limited changes - the main one being that references to ISO/IEC 27001 now cite the 2013 edition).

A project to revise/rewrite the standard made insufficient progress and was cancelled ... and then re-started. Development of the *fourth* edition of '27005 is under way. Hopefully, the *fourth* edition of ISO/IEC 27005 will be published at about the same time as the next release of ISO/IEC 27001, supporting the updated ISMS specification.

Analýza rizik - představení

- Riziko znamená potenciální odchylky od očekávání nebo potenciální odchylky od našich cílů. Tímto referenčním bodem je riziko formálně definováno jako kombinace možných následků a související nejistoty.

  Běžným způsobem, jak určit riziko, je podívat se na pravděpodobnost nehody a co by mohlo být důsledkem, pokud k ní dojde.

Analýza rizik - představení

- Identifikace, rizikové prvky (1)
- Analýza rizik (2)
- Hodnocení rizik (3)

Analýza rizik - představení

- Identifikace, rizikové prvky (1)

Analýza rizik - představení

- Analýza rizik (2)

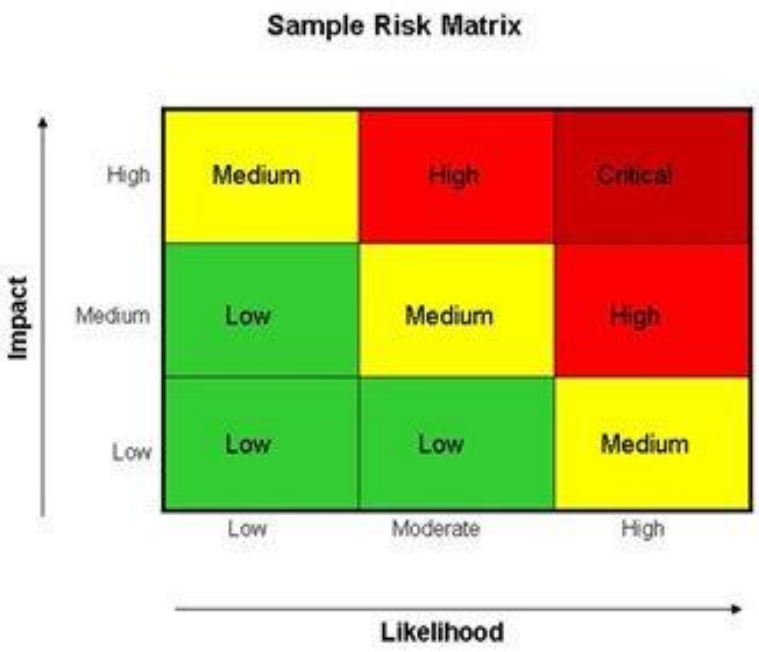
Jde o pochopení rizik

Analýza rizik zahrnuje posouzení:

- příčiny
- zdroje událostí
- následků, které mohou mít
- a pravděpodobnosti výskytu důsledků.

Analýza rizik - představení

- Analýza rizik (2)
- Pravděpodobnost / Dopad



Analýza rizik - představení

- Hodnocení rizik (3)

  Účelem hodnocení rizik je poskytnout podporu pro nadcházející rozhodnutí o rizicích, která je třeba řešit a o stanovení priorit potřebných kroků.

  V některých případech může vyhodnocení rizika vést k rozhodnutí provést další analýzu. Vyhodnocení rizika může rovněž skončit doporučením, aby se rizika neřešila jiným způsobem než jako doposud, tedy stávajícími opatřeními.

Analýza rizik, cvičení, úkoly

- Identifikujte rizikové prvky na vašem pracovišti

Analýza rizik – akční plán

Analýza rizik – akční plán - šablona

RISK ACTION PLAN TEMPLATE

PROJECT NAME	
IDENTIFIED RISK	
PROBABLE IMPACT	
MITIGATION RESPONSE	
PLANNED ACTIONS	
REQUIRED RESOURCES	
PARTIES RESPONSIBLE	
PROPOSED TIMELINE	
REPORTING PROCESS *List steps required & parties responsible*	
MONITORING PROCESS List steps required & parties responsible	

PREPARED BY		DATE	
REVIEWED BY		DATE	

Dotazy ?

FOR THE WORLD YOU MIGHT BE JUST A PERSON.....

BUT FOR A PERSON, YOU MIGHT BE THE HOLE WORLD.

PRO SVĚT MůŽETE BÝT JENOM ČLOVĚKEM ....

ALE PRO ČLOVĚKA CELÝM SVĚTEM

THANK YOU FOR YOUR ATTENTION
DĚKUJI ZA POZORNOST