



Metodiky a rámce použitelné v posudzování rizík informační bezpečnosti

Michal Ďorda

Senior konzultant, Risk Advisory
september 2018

Riziká informačnej bezpečnosti



Riziko je **miera neistoty** s cieľom kvantifikovať pravdepodobnosť.

Informačná bezpečnosť je udržiavanie **akceptovateľnej miery identifikovaného rizika**, ktoré pôsobí na aktíva procesmi a činnosťami zameranými na odvrátenie alebo zmenšenie identifikovaných rizík a prejavov hrozieb.

Posúdenie rizík informačnej bezpečnosti

Aký rámec ste použili pri poslednom posúdení rizík a ich následnom riadení?



ISO/IEC 27005:2011

Information security risk management

Osvedčené postupy

Aktíva -> Hrozby -> Kontroly

Riziko = Pravdepodobnosť x Dopad

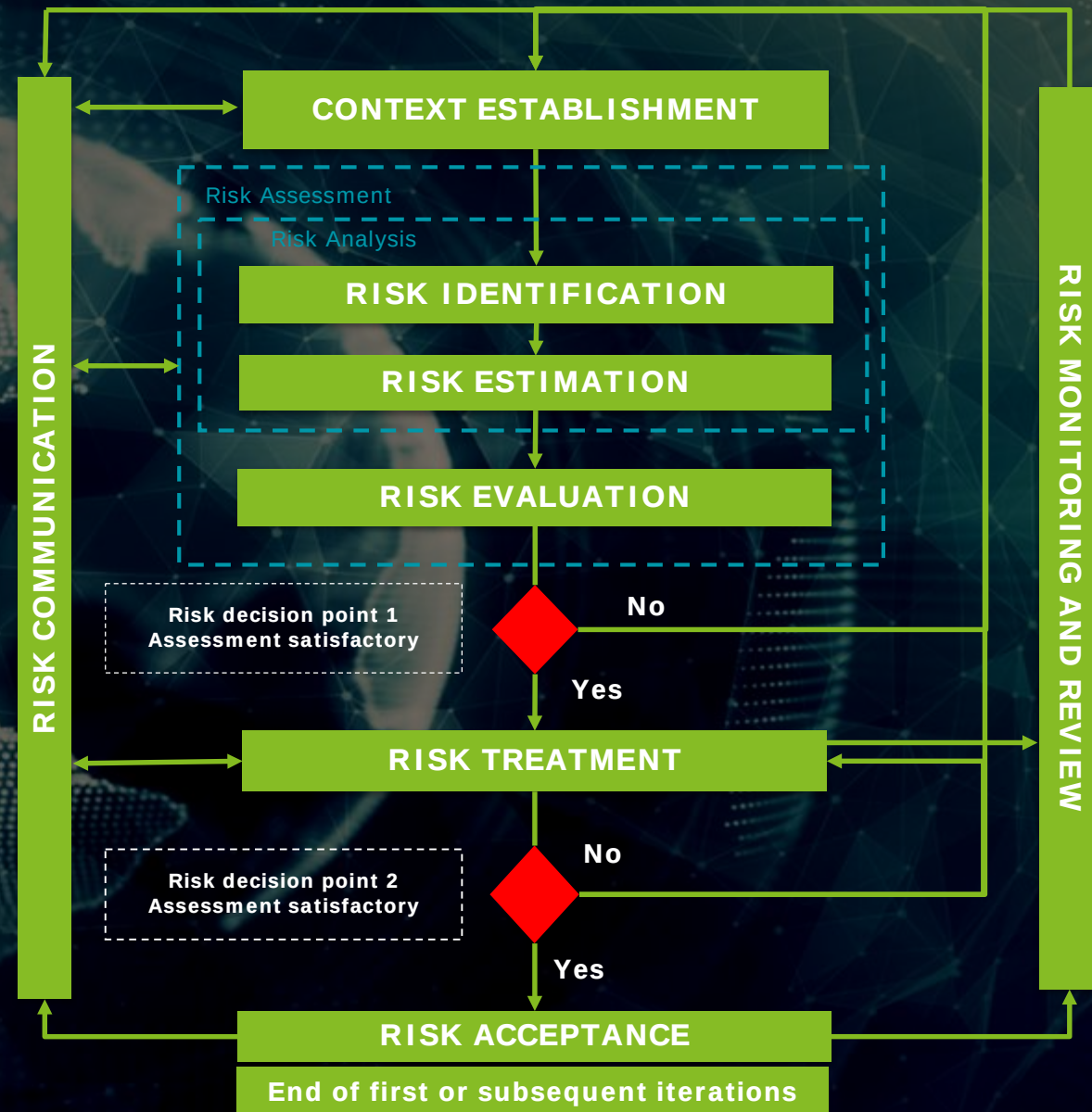
- kvalitatívne a kvantitatívne

ISO/IEC 27001

ISO/IEC 27002



<https://www.iso.org/standard/75281.html>



NIST SP 800-30 Rev. 1

Guide for Conducting Risk Assessments

Federálne informačné systémy a organizácie

Posúdenie rizík na 3 úrovniach:

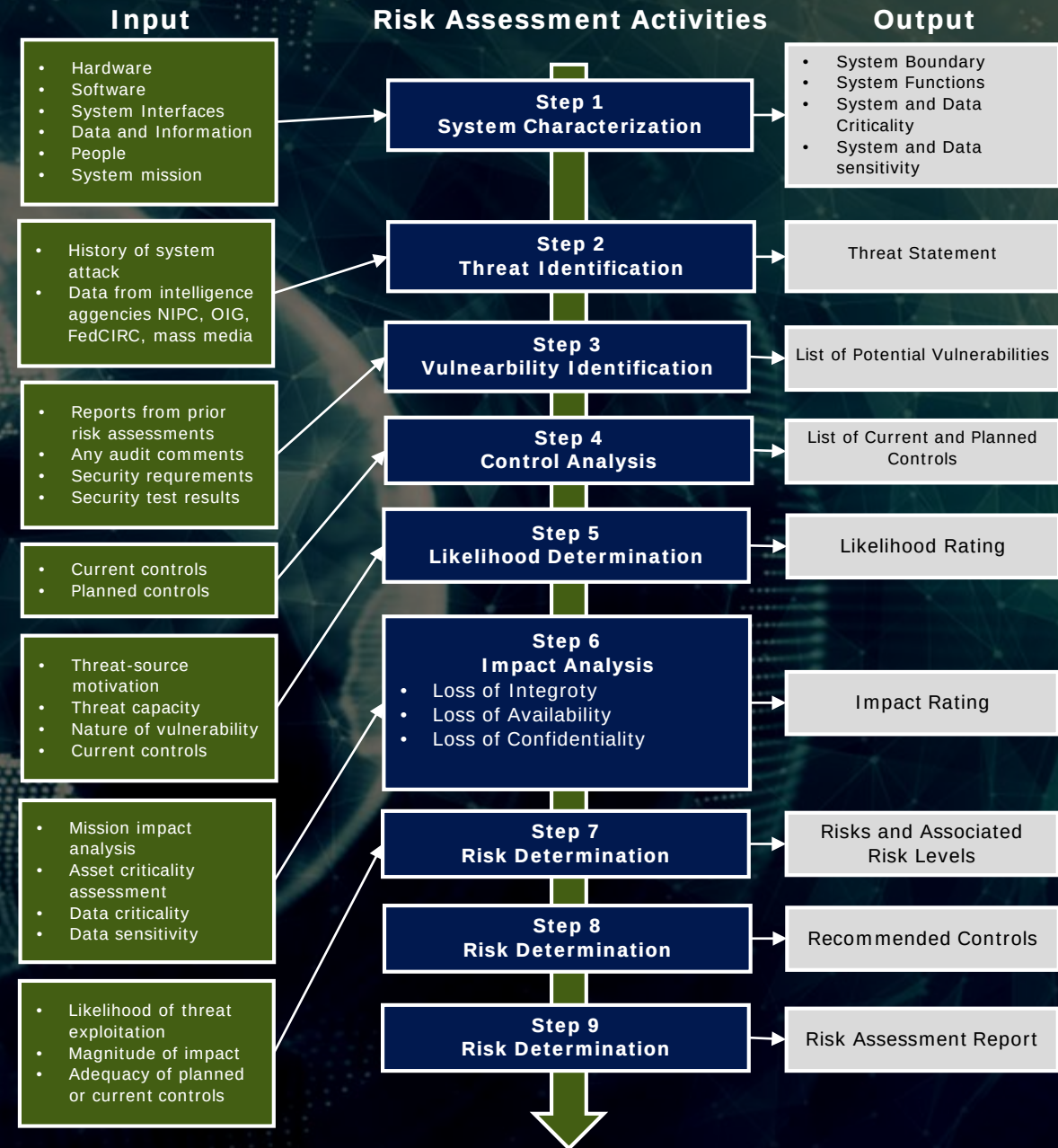
1. Organizačná úroveň;
2. Biznis proces úroveň;
3. Úroveň informačných systémov

SP 800-39

SP 800-53



<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>



Factor analysis of information risk (FAIR)

Ide o **taxonómiu faktorov**, ktoré prispievajú k riziku a ako sa navzájom ovplyvňujú, alebo tiež rámec založený na **princípe pravdepodobností straty dát**.



ISACA RiskIT

IT riziká -> Riadenia podnikových rizík

Obsahuje procesy vo všetkých oblastiach:

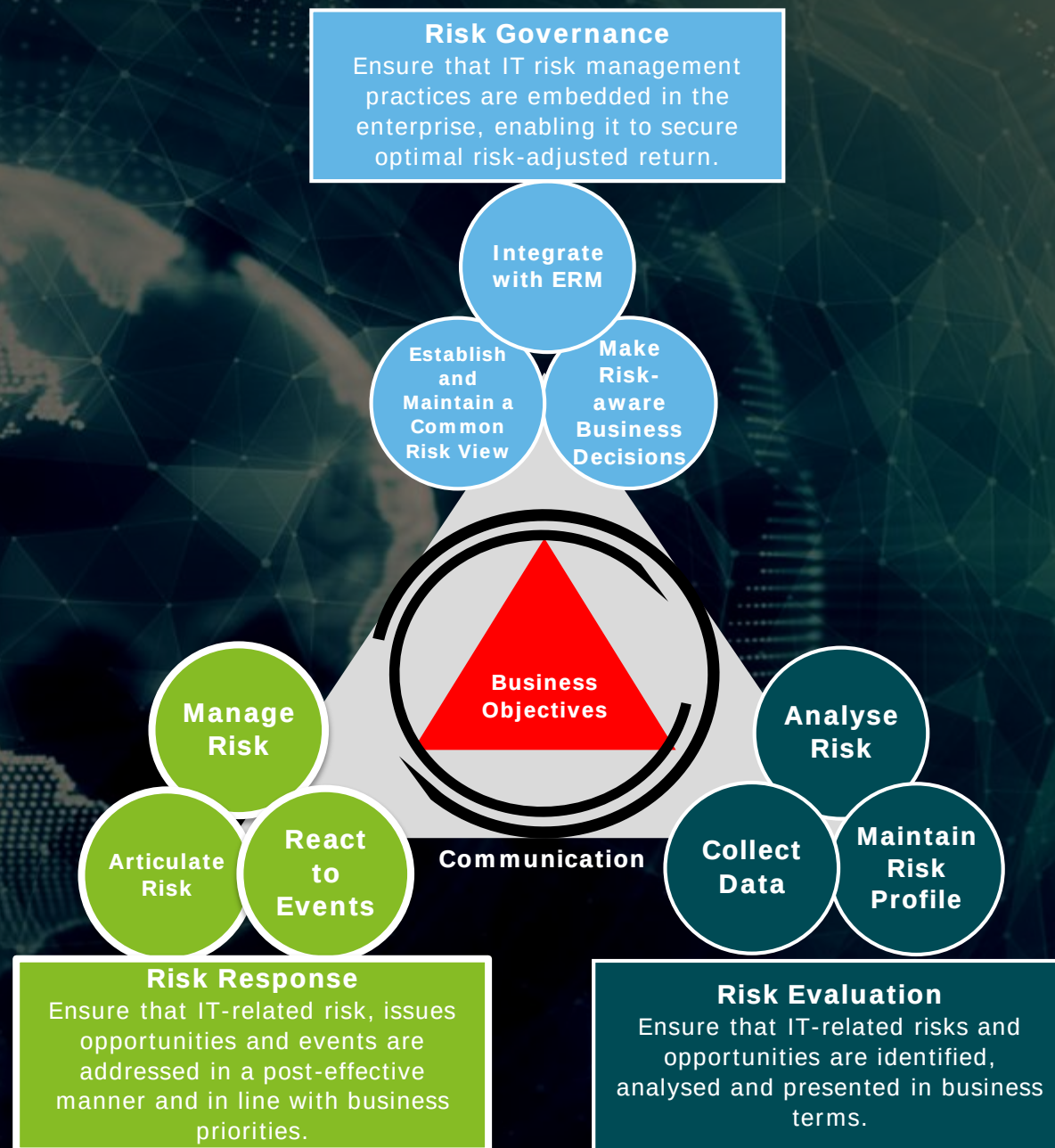
- **Riadenie rizík**
- **Vyhodnotenie rizík**
- **Reakcie na riziká**

ISACA -> COBIT 5

Využíva **FAIR** a **COSO**



<http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx>



ISF IRAM 2

Informačná bezpečnosť -> Hodnotenie podnikových rizík

Širšie a komplexnejšie pokrytie rizík
Zapojenie kľúčových vlastníkov

ISF Standard of Good Practice for Information Security



<https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/>

A. Scoping

A.1 Develop a profile of the environment

A.2 Develop the scope for the assessment

C. Threat Profiling

C.1 Populate the threat landscape

C.2 Profile threats

C.3 Produce a prioritized threat landscape

C.4 Scope and map threat events

C.5 Identify and map assets impacted to threat events

E. Risk Evaluation

E.1 Derive the likelihood of success

E.2 Derive the residual likelihood

E.3 Determine the residual business impact rating

E.4 Derive the residual risk rating

B. Business Impact Assessment

B.1 Identify the information assets

B.2 Assess business impact

D. Vulnerability Assessment

D.1 Identify vulnerabilities and related controls

D.2 Assess effectiveness of identified controls

D.3 Determine the control strength for each combination of threat event and component

F. Risk Treatment

F.1 Evaluate each risk against the risk appetite

F.2 Create a risk treatment plan

F.3 Execute the risk treatment plan and validate results

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

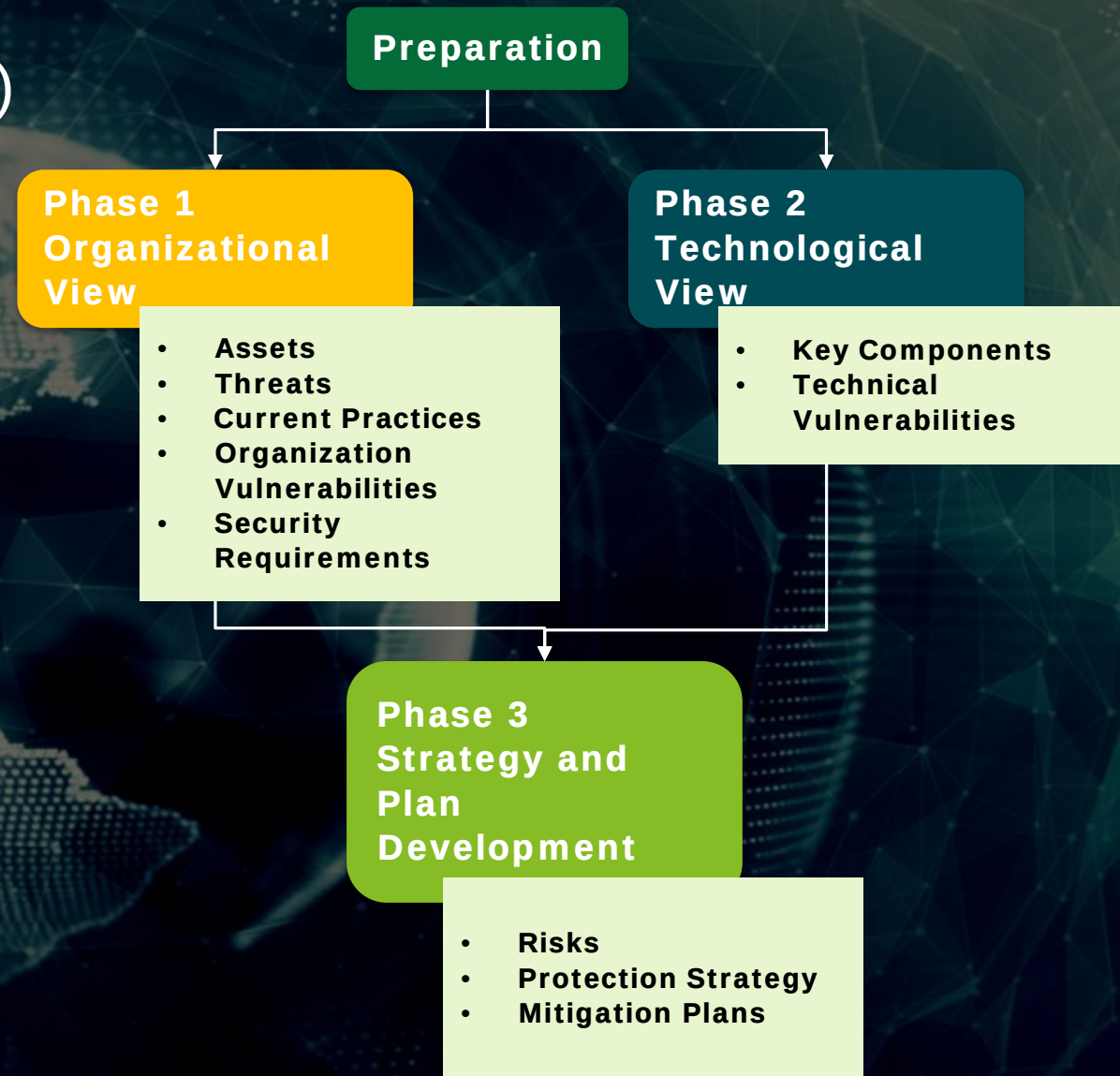
Zamerania na **organizačné riziko**

Kľúčové aspekty:

- operačné riziko
- bezpečnostné postupy
- technológie



<https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419>



Iné rámce

HMG Information Assurance Standard 1 & 2

Poskytuje rámec pre hodnotenie rizika a procesy riadenia rizík pre systémy v UK

CCTA Risk Analysis and Management Method (CRAMM)

Metodológia pre riadenie rizík používaná v NATO

Expression des Besoins et Identification des Objectifs de Sécurité

Metóda pre analýzu, hodnotenie a výber opatrení týkajúcich sa IT rizík

IT-Grundschutz

IT Baseline Protection Catalogs



Committee of Sponsoring Organizations of the Treadway Commission (COSO)

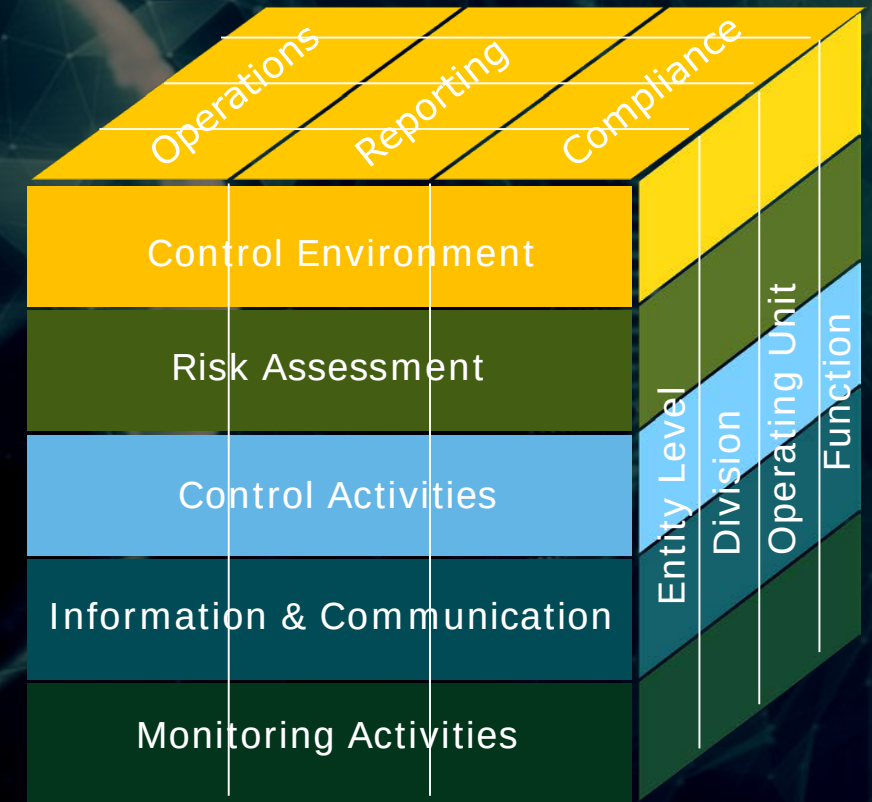
Enterprise risk management

Model na hodnotenie interných kontrol

1. Kontrolné prostredie
2. Posúdenie rizík
 - a) **Ciele pre spoločnosť**
 - b) **Procesne orientované ciele**
 - c) **Identifikácia a analýza rizík**
 - d) **Riadenie zmien**
3. Kontrolné aktivity
4. Informácia a komunikácia
5. Monitoring



<https://www.coso.org/Pages/erm-integratedframework.aspx>



Porovnanie rámcov a metodík

	Typ	Zameranie	Využitie
ISO / IEC 27005	Flexibilné osvedčené postupy pre kvalitatívne a kvantitatívne posúdenie rizík	Riziká informačnej bezpečnosti	Rôzne typy organizácií
NIST SP 800-30	Proces posúdenie rizík na troch úrovniach: Organizácia, Biznis, IT	Analýza technických rizík IT infraštruktúry	Všetky veľkosti súkromných alebo verejných spoločností
RiskIT	Rámec pre stratégiu a riadenie rizík s prepojením na podnikové riziká	IT riziká v podnikových rizikách	Organizácie, ktoré formalizujú procesy
IRAM2	Metodológia posúdenia rizík	Informačná bezpečnosť v podnikových rizikách	Rôzne organizácie
Octave	Metóda posúdenia založená na aktívach zameraná na organizačné riziko	Organizačné riziká	Malé organizácie bez skúseností s rizikami

Zhrnutie

S kybernetickým rizikom musí zaobchádzať každá spoločnosť ako rizikom najvyššej úrovne. Dnešné podnikanie funguje dennodenne pomocou moderných technológií, s rôznymi partnermi a zákazníkmi, zamestnancami a internými procesmi. Tieto všetky premenné vstupujú do kvalitného **posudzovania rizík informačnej bezpečnosti**. A preto by mal byť výber založený na dôkladnej analýze a potrebách spoločností.



<https://www2.deloitte.com/global/en/pages/risk/articles/assessing-cyber-risk.html>





Deloitte označuje jednu, resp. viacero spoločností Deloitte Touche Tohmatsu Limited, britskej súkromnej spoločnosti s ručením obmedzeným zárukou (UK private company limited by guarantee), a jej členských firiem. Každá z týchto firiem predstavuje samostatný a nezávislý právny subjekt. Podrobný opis právnej štruktúry združenia Deloitte Touche Tohmatsu Limited a jeho členských firiem sa uvádza na adrese www.deloitte.com/sk/o-nas.

Spoločnosť Deloitte poskytuje služby v oblasti auditu, daní, práva, podnikového a transakčného poradenstva klientom v mnohých odvetviach verejného a súkromného sektora. Vďaka globálnej prepojenej sieti členských firiem vo viac ako 150 krajinách má Deloitte svetové možnosti a dôkladnú znalosť miestneho prostredia, a tak môže pomáhať svojim klientom dosahovať úspechy na všetkých miestach ich pôsobnosti. Približne 245 000 odborníkov spoločnosti Deloitte sa usiluje konať tak, aby vytvárali hodnoty, na ktorých záleží.