

Nová éra pre manažment IT rizík

Marek Zeman,
vedúci oddelenia bezpečnosti a nových technológií, Tatra banka, a.s.

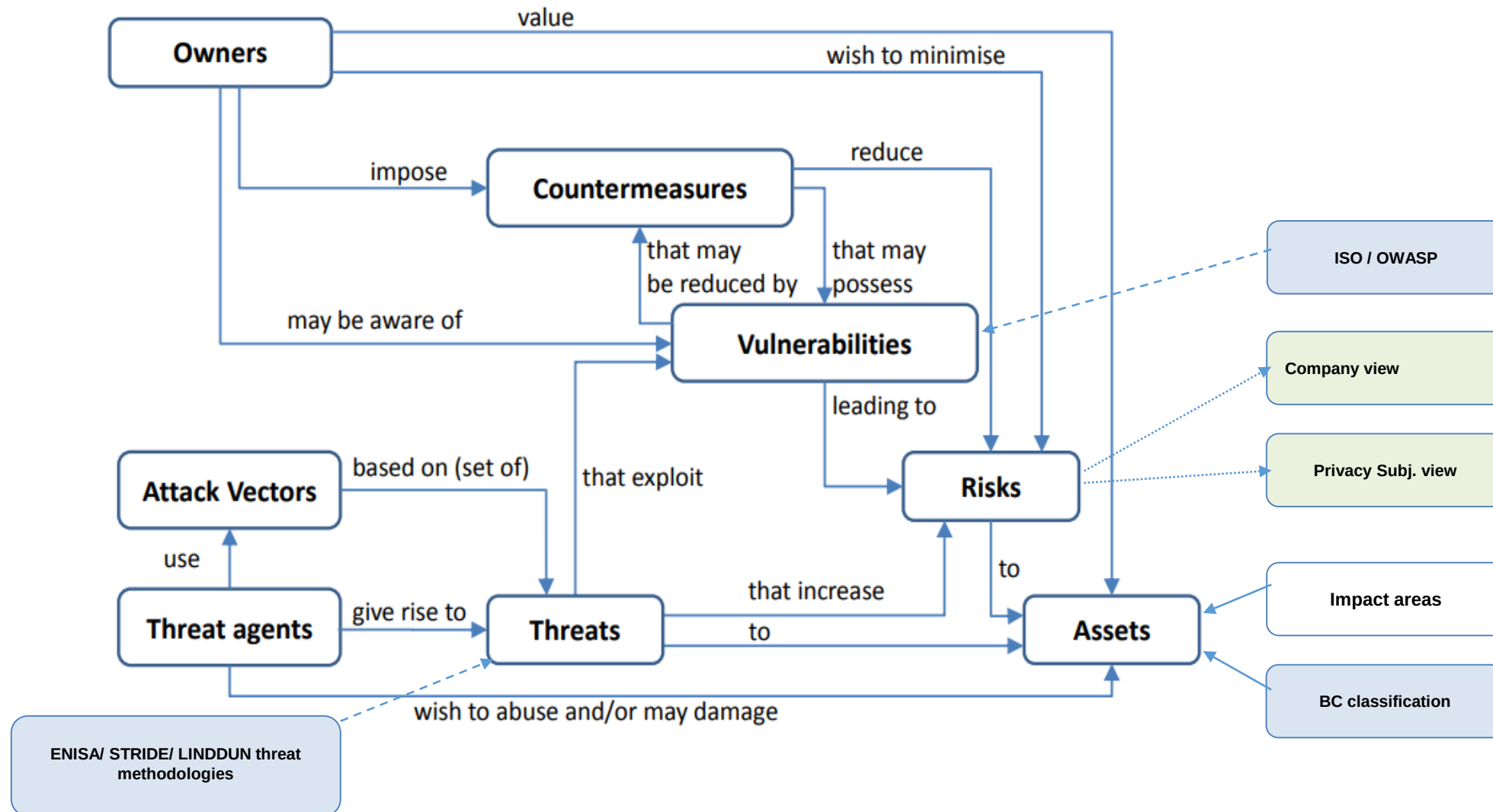
The logo consists of a stylized orange lowercase 'e' followed by the word 'FOCUS' in white uppercase letters. The entire logo is positioned above a horizontal orange line that spans the width of the slide.

eFOCUS

Ako bolo s Risk managementom pred GDPR?

- Každá firma si vybrala vlastné riešenie.
- **Zadefinovali si vlastný Risk management process.**
- Kontrola implementácie:
 - Automatically: Vulnerability scans
 - Semiautomatic: Hardening scripts, Penetration tests
 - Manual: Risk Analysis (Reactive, Proactive)

Vztáhy mezi jednotlivými prvky IS RM s GDPR v TB



IT Assets

- How to choose an approach?

- Business
- IT
- BCM

Asset Group ID	Asset Group Name	Asset Group Value
A1	TBG critical	5
A2	Business critical	5
A3	Business standard	3
A4	IT critical	5
A5	IT standard	3
A6	IT default	2
A7 - AX	Example Privacy relevant / PDPA1-X	5

- IT Asset Categories

- 1-6 - Business priority
- 7- because of regulation
- 8 - X - GDPR - relevant business processes

Vulnerabilities and Threat Agents and motivation

Threat Agent Motivation and Capacity Value Measurement Scale	
Value	Magnitude
1	Very Low
2	Low
3	Medium
4	High
5	Very High

Vulneraname_ID (Vulnerability name)	Examples of RELATED Threats	Exposur e [Metric Values are 1-5]*	Severit y [Metric Values are 1-5]*	Vulnerabilit y Assessment Value*	A 1	A 2	A 3	A 4	A 5	A 6	A7 =A X
V1.Insufficient maintenance/faulty installation of storage media	Breach of information systém maintainability	3	4	2,4					1	1	
V2.Lack of periodic replacement schemes	Destruction of equipment or media	4	3	2,4			1		1	1	
V3.Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing	3	3	1,8							
V4.Sensitivity to electromagnetic radiation	Electromagnetic radiation	2	4	1,6							
V5.Lack of efficient configuration change control	Error in use	4	3	2,4	1	1	1	1	1	1	
V6.Susceptibility to voltage variations	Loss of power supply	3	4	2,4							
V7.Susceptibility to temperature variations	Meteorological phenomenon	3	4	2,4							
V8.Unprotected storage	Theft of media or documents	4	3	2,4			1		1	1	
V9.Lack of care at disposal	Theft of media or documents	3	5	3							

Currently considered Threat Agents	
ID	Description
1	cyber-criminals
2	insiders
3	nation states
4	corporations
5	hacktivists
6	cyber-fighters
7	cyber-terrorists
8	script kiddies

V74.Lack of procedures for classified information handling	Error in use	2	3	1,2							
V75.Lack of information security responsibilities in job descriptions	Error in use	2	3	1,2							
V76.Lack or insufficient provisions (concerning information security) in contracts with employees	Illegal processing of data	2	3	1,2							
V77.Lack of defined disciplinary process in case of information security incident	Theft of equipment	4	3	2,4	1	1	1	1	1	1	
V78.Lack of formal policy on mobile computer usage	Theft of equipment	2	3	1,2							
V79.Lack of control of off-premise assets	Theft of equipment	2	3	1,2	1	1	1	1	1	1	
V80.Lack or insufficient 'clear desk and clear screen' policy	Theft of media or documents	2	3	1,2							
V81.Lack of information processing facilities authorization	Theft of media or documents	2	3	1,2							

Ako riešime Risk management pre existujúce projekty?

- Vydefinovali sme si zoznam biznis procesov s popisom.
- **Vyšpecifikovali top**
- Pre TOP procesy sa urobila analýza časti IS Risk assessmentu pre osobné údaje.
- Vytvorila sa prioritizačná matica, na základe predchádzajúceho.
- Následne sa procesy rozdelili
 - Tie, kde je nevyhnutné vytvoriť DPIA.
 - Tie, kde vyšlo vysoké riziko pre ochranu osobných údajov
 - Ostatné

Ako riešime GDPR pre nové projekty?

- **SDLC – software development life cycle**
- **Návrh a implementácia novej zmeny do systému Tatra banky, a.s.**
- **Biznis analýza a návrh riešenia**
 - IS Security pohľad + 10 základných otázok na HL pochopenie pohľadu ochrany osobných údajov
 - Údaje sú ukladané na interný WEB
- **Schválenie projektovej štúdie**
- **Indikatívna požiadavka + finálna požiadavka**
 - IS Security pomoc pri vytváraní indikatívnej požiadavky
 - Spustenie procesu IS Risk managementu, analyzované z dvoch pohľadov (pohľad Os. údajov a pohľad IS RM)
- **Implementácia**
- **Nasadenie**
- **Denná rutina**

Ďakujeme za pozornosť

?

eFOCUS