

Spojenie GDPR a IS Risk managementu v praxi

Iveta Šťavinová

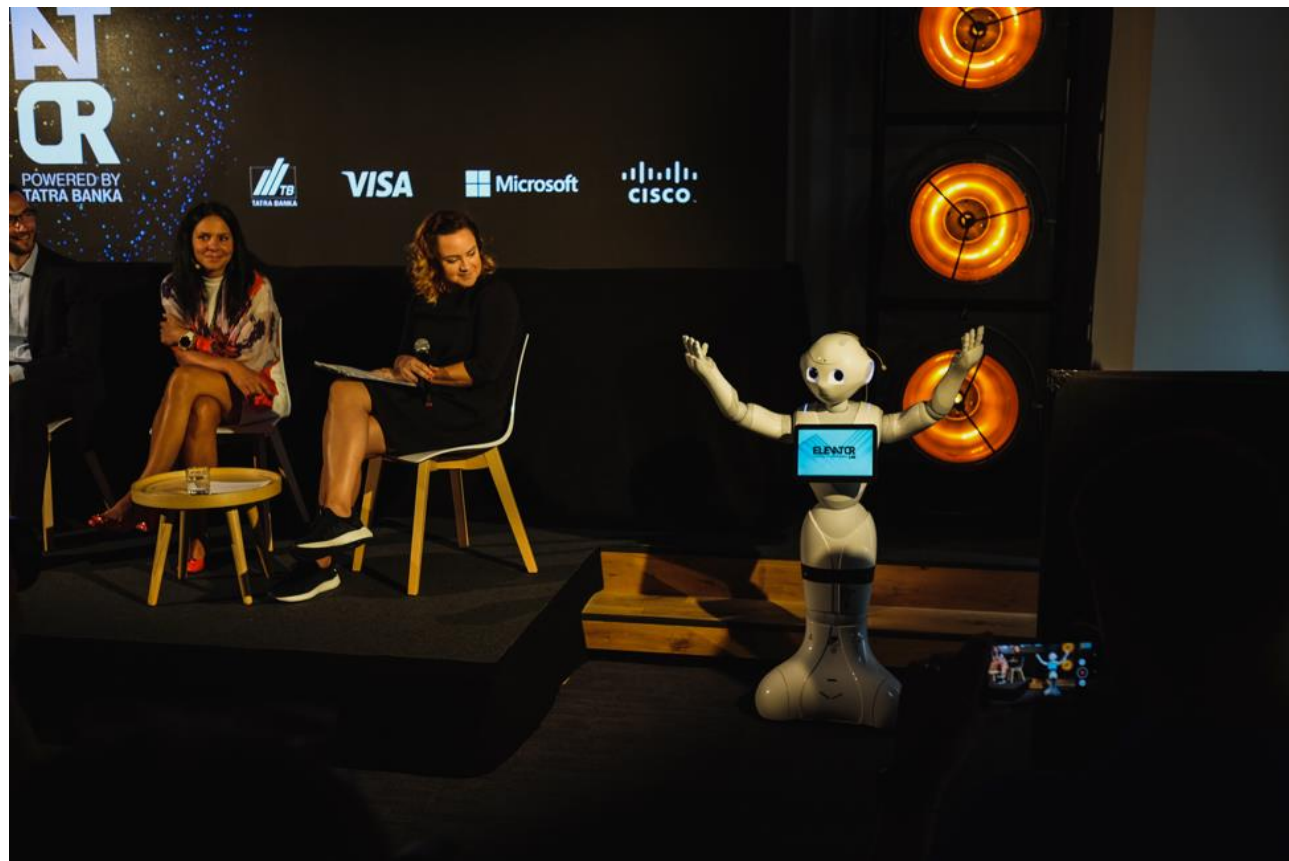
Tatra banka, IS Security Specialist, CISA

spolu sme jedna banka



- **25 rokov inovácii v Tatra banka, a.s.**

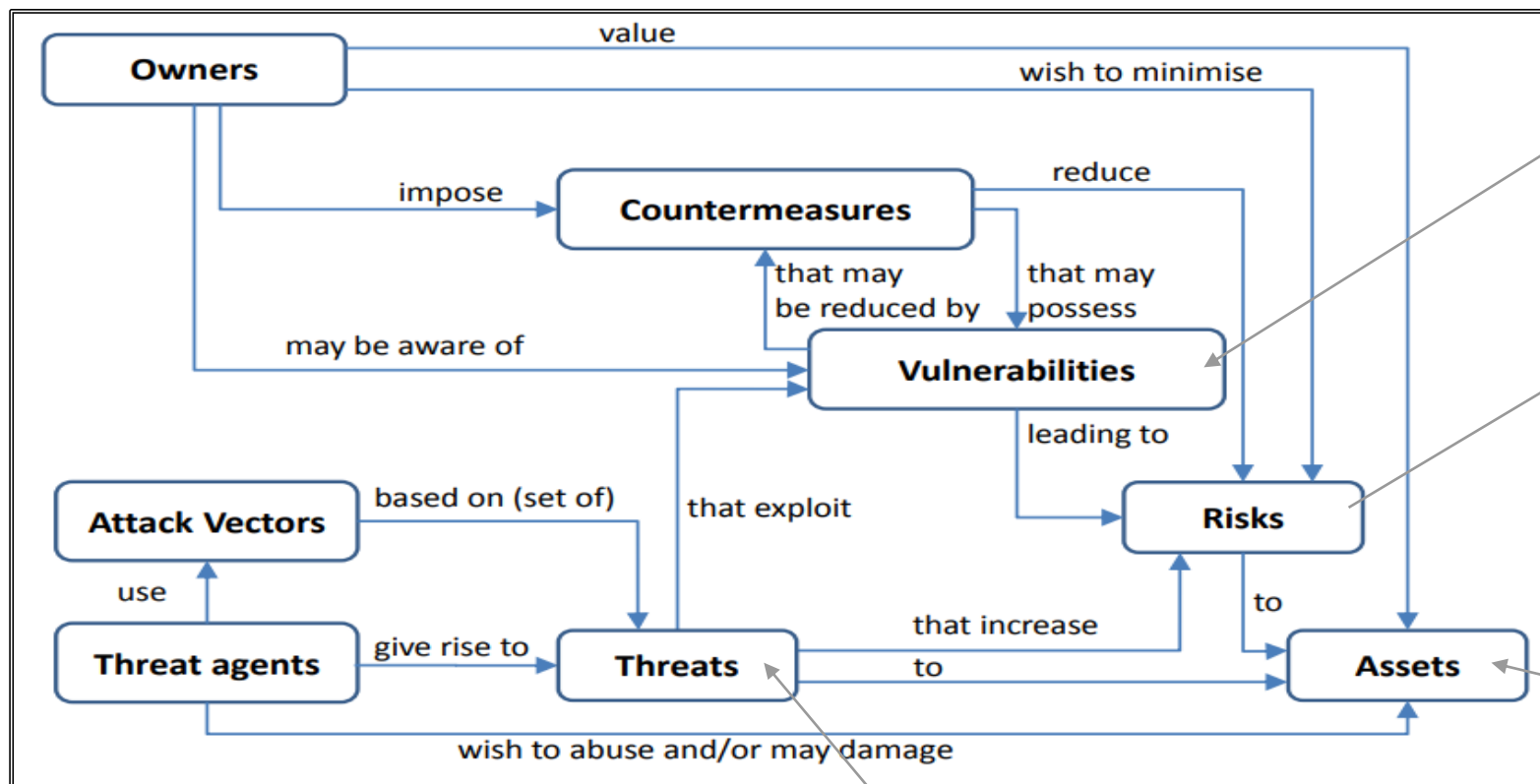
- Inovácie v našej DNA
- Biznis inovácie
 - DIALOG
 - Hlasová biometria
 - Karty
 - MobilPay
 - Online založenie účtu
 - Tvárová biometria
 - Mobilné aplikácie
 - Tatrabanka, Viamo
 - Pobočky
 - Pepper
 - Songoroo



- **agenda**

- riadenie rizík IS
- spojenie IS a GDPR Risk Assessment-u
- softvér pre proces riadenia rizík

◦ kostra riadenia rizík



- ISO
- OWASP
- TATRA

z pohľadu

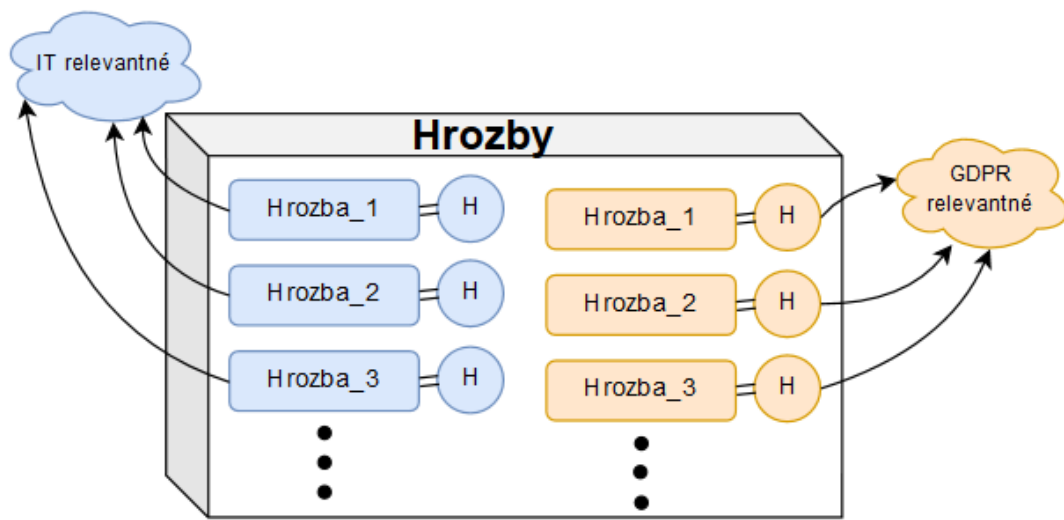
- firemného procesu
- ochrany súkromia

ASSETS to ASSET GROUPS:
A1 = A6 štď. podľa SLA
A7 - AX vzťah k ochrane
súkromia, na báze PDPA

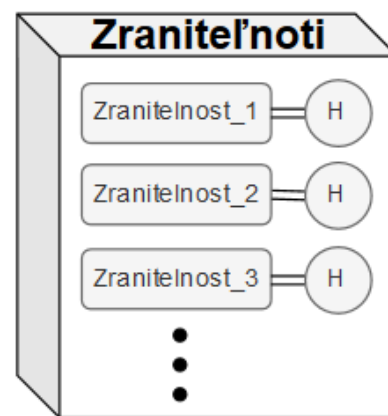
- General ENISA Threat
- STRIDE
- LINDDUN Privacy Threats

◦ tri základné prvky risk manažmentu

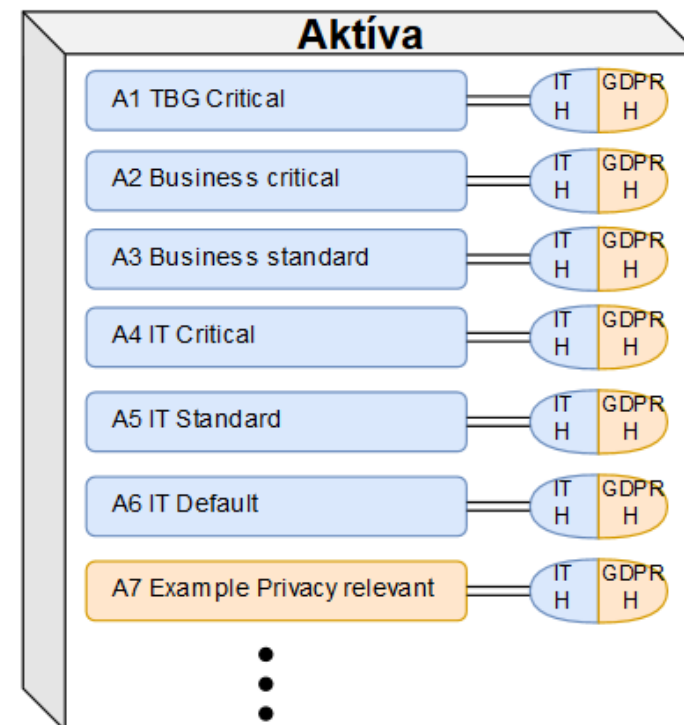
získané z metodík ENISA, STRIDE, LINDDUN Privacy, ISO, OWASP



motivácia a kapacita



závažnosť a risk apetít



- **aktíva**

- aktíva sú zoskupené do tzv. Asset Groups (AG)
 - 6 základných AG, A1 – A6, definovaných podľa požiadaviek BCM procesov a kritickosti dopadu na biznis operácie (tiež v závislosti od SLA)
 - A7 – AX, dynamicky pridávané skupiny, obsahujúce aktíva, ktoré vytvárajú alebo priamo podporujú špecifické činnosti spracovania osobných údajov
 - Aktuálne skupiny boli identifikované preskúmaním biznis procesov v rámci PDPA (Personal Data Processing Activities)
 - Pridávanie nových skupín – závislé od splnenia kritérií DPIA (Data Privacy Impact Analysis)

◦ implementácia evidencie skupín aktív vzťahy medzi skupinami

The screenshot displays a web application interface for managing IT standards. On the left is a dark sidebar with navigation links: Přehled, Úkoly, Případy, RISK, Požadavky, Cíle, Aktiva (highlighted), Hrozby a zranitelnosti, Rizika, Hodnocení, Skupiny, Opatření, Uživatelé, Koš, and Nastavení. The main content area is titled 'Aktiva / A5 IT standard'. It features a top bar with a user profile 'Správce Nepřifázeno', status buttons 'Normální' and 'Schváleno', and a dropdown menu. Below this is the 'Aktivum - A5' section, which includes tabs for 'Registr Aktiv' and 'TB Asset Groups - IT'. A table lists various attributes for the asset group 'A5':

Přístup:	—
Číslo záznamu:	A5
Náklady:	—
Plán platnosti od:	1. 1. 2018
Plán platnosti do:	—
Skutečná platnost od:	—
Skutečná platnost do:	—
Vytvořil:	Admin TB
Vytvořeno:	23. 10. 2018, 20:15
Naposledy upraveno:	25. 10. 2018, 11:19
TATRA BANKA	
IT vlastn:	—
Byznys vlastn:	—

Below the table, there are sections for 'Připojené entity' and 'Hodnocení'. The 'Hodnocení' section shows a rating for 'A05' as 'Střední' (Medium) with a score of 3, represented by a blue bar chart.

spolu sme jedna banka



○ implementácia hodnotenia skupiny aktív

The screenshot displays a web application for risk assessment. On the left is a dark sidebar with navigation items: Přehled, Úkoly, Případy, RISK, Požadavky, Cíle, Aktiva, Hrozby a zranitelnosti, Rizika, Hodnocení (highlighted), Skupiny, Opatření, Uživatelé, Koš, and Nastavení. The main content area is titled 'Hodnocení / A05' and contains a sub-header 'Hodnocení' with a green 'Ohodnotit' button. Below this is a table for 'TB Hodnocení Asset Impact Areas'. A modal window is open, showing a date and time stamp '17. 2. 2019, 13:57' and a table with 7 rows (IA2 to IA7) and 5 columns (1 to 5). The cells contain risk levels: 'Nulové', 'Nizké', 'Střední', 'Vysoké', and 'Kritické'. The 'Střední' cell for IA2 is highlighted in yellow, and the 'Nizké' cell for IA6 is highlighted in green.

	1	2	3	4	5
IA2 ?	Nulové	Nizké	Střední	Vysoké	Kritické
IA3 ?	Nulové	Nizké	Střední	Vysoké	Kritické
IA4 ?	Nulové	Nizké	Střední	Vysoké	Kritické
IA5 ?	Nulové	Nizké	Střední	Vysoké	Kritické
IA6 ?	Nulové	Nizké	Střední	Vysoké	Kritické
IA7 ?	1	2	3	4	5

spolu sme jedna banka



○ impact areas pre hodnotenie skupiny aktív

Impact Area_ID	ImpactArea_Description
IA1	Interruption of service - inability to provide the service
IA2	Loss of customer confidence - damage to reputation
IA3	Disruption of internal operation - disruption in the organization itself
IA4	Disruption of a third party's operation: - disruption in third parties transacting with the organization
IA5	Infringement of laws / regulations: - inability to fulfill legal obligations
IA6	Breach of contract: - inability to fulfill contractual obligations
IA7	Attack on users' private life
IA8	Financial losses
IA9	Loss of goods / funds / assets
IA10	Loss of customers, loss of suppliers
IA11	Judicial proceedings and penalties
IA12	Loss of a competitive advantage
IA13	Loss of technological / technical lead
IA14	Loss of effectiveness / trust
IA15	Loss of technical reputation

○ implementácia evidencie hrozieb

The screenshot displays a web application for threat intelligence management. On the left is a dark sidebar with navigation items: Přehled, Úkoly, Případy, RISK, Požadavky, Cíle, Aktiva, Hrozby a zranitelnosti (highlighted), Rizika, Hodnocení, Skupiny, Opatření, Uživatelé, Koš, and Nastavení. The main content area has a header 'Hrozby a zranitelnosti / T070 Privacy.PT3_Non-repudiation_LINDDDUN'. Below this is a sub-header 'Hrozba · T70' with tabs for 'Registr hrozeb a zranitelnosti', 'Hrozby', 'LINDDDUN Privacy', and 'Non-repudiation'. A table lists threat details: Číslo záznamu: T70, Zdroj: LINDDDUN, Verze: 2018, Pravděpodobnost (ARO): —, Vytvořil: Admin TB, Vytvořeno: 23. 10. 2018, 20:56, Naposledy upraveno: 23. 1. 2019, 10:35. Below the table is a section 'TATRA BANKA' with fields for Reference (dokumentace): ORP 1010: Bezpečnostná politika TBG, Agent hrozby: Kyberzločinci, and a descriptive text: 'Ability to deny having performed an action that other parties can neither confirm nor contradict'. At the bottom, there is a 'Hodnocení' (Rating) section showing 'T070' with a red dot indicating 'Vysoké' (High) and a score of 4.

spolu sme jedna banka



○ implementácia hodnotenia hrozieb

The screenshot displays a web application for risk assessment. The left sidebar contains a navigation menu with items: Přehled, Úkoly, Případy, RISK, Požadavky, Cíle, Aktiva, Hrozby a zranitelnosti, Rizika, Hodnocení (selected), Skupiny, Opatření, Uživatelé, Koš, and Nastavení. The main content area is titled 'Hodnocení / T070'. A modal window is open, titled '17. 2. 2019, 13:53', showing a risk assessment for 'TA Capacity' and 'TA Motivation'. The modal includes a table with 5 columns representing risk levels (1 Very Low, 2 Low, 3 Medium, 4 High, 5 Very High) and a 'Celkem' (Total) row. The 'TA Capacity' and 'TA Motivation' rows both have a '4' (High) selected. The 'Celkem' row shows a total score of 'High 4'.

	1 Very Low	2 Low	3 Medium	4 High	5 Very High
TA Capacity				4 High	
TA Motivation				4 High	
Celkem	High 4				

spolu sme jedna banka



○ implementácia evidencie zraniteľností

Hrozby a zranitelnosti / V036 Unprotected sensitive traffic

Přehled Aktivita Propojení Skupiny

Správce
Nepřifazeno

Normální Vytvořeno

Zranitelnost · V36

Registr hrozeb a zranitelností Zranitelnosti ISO 27001 Síť

Číslo záznamu:	V36
Zdroj:	ISO
Verze:	2017
Vytvořil:	Admin TB
Vytvořeno:	23. 10. 2018, 20:57
Naposledy upraveno:	23. 1. 2019, 10:09
TATRA BANKA	
Reference (dokumentace):	—
Network	

Připojené entity

Hodnocení

V036

Vysoké

4

spolu sme jedna banka



○ implementácia hodnotenia zraniteľnosti

Hodnocení / V036

Hodnocení Ohodnotit

TB hodnocení ISO Vulnerabilities

Chybí hodnocení pro cílový stav.

Název	Stav	Skóre	Platnost od	Platnost do	Typ
-------	------	-------	-------------	-------------	-----

17. 2. 2019, 13:54

Exposure	1 Nulové	2 Nizké	3 Střední	4 Vysoké	5 Kritické
Severity	1 Nulové	2 Nizké	3 Střední	4 Vysoké	5 Kritické
Celkem	Vysoké 4				

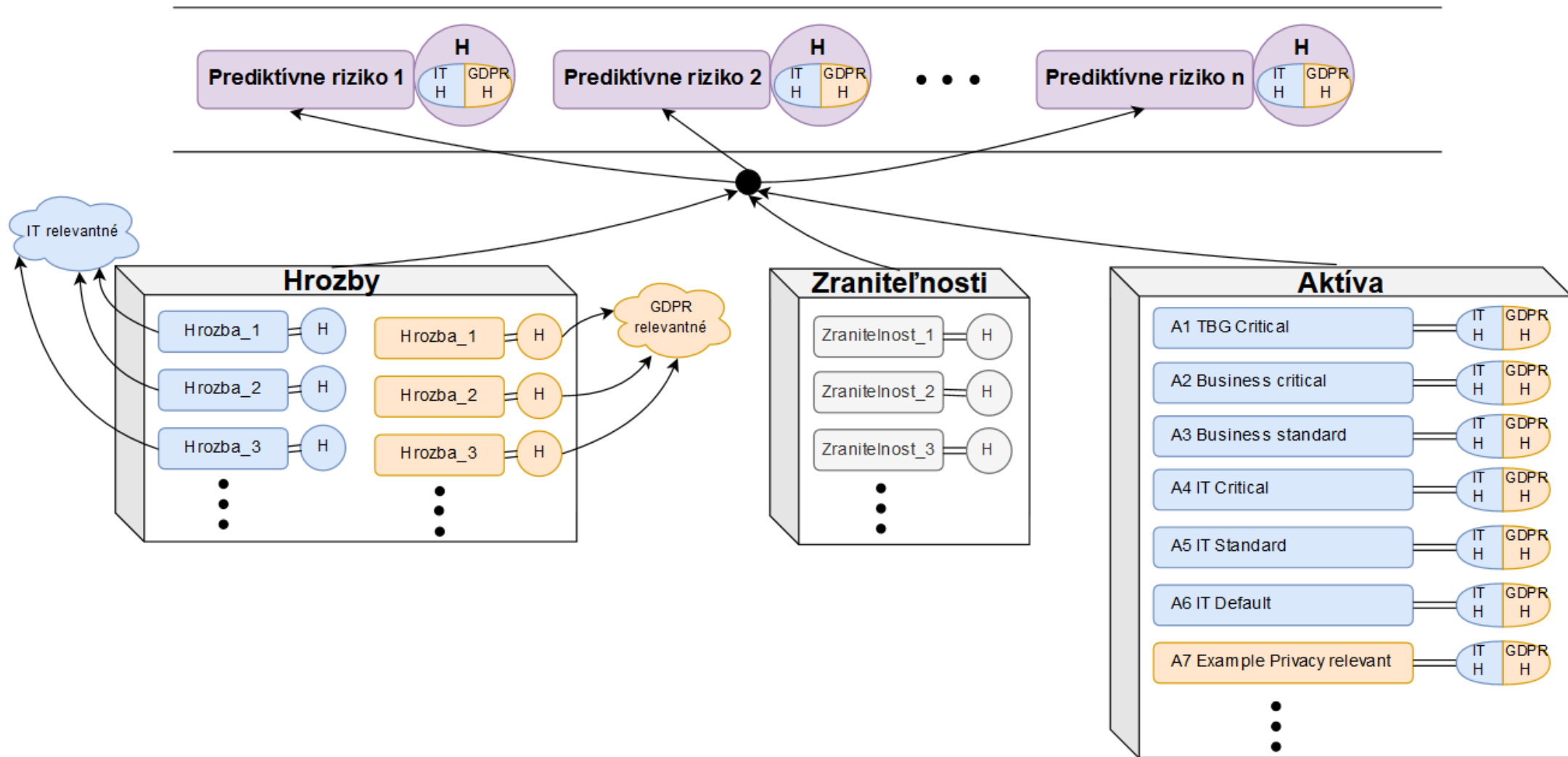
spolu sme jedna banka



- **prediktívne biznis riziká**

- vytvorené rôznymi kombináciami A x Z x H (Aktívum, Zraniteľnosť, Hrozba)
- prediktívne riziká relevantné pre organizáciu
- na základe hodnôt jednotlivých zložiek, prepočtom vytvára jednu celkovú hodnotu závažnosti
- okrem celkovej hodnoty závažnosti nesie prediktívne riziko aj dve samostatné hodnoty (IT a Privacy)

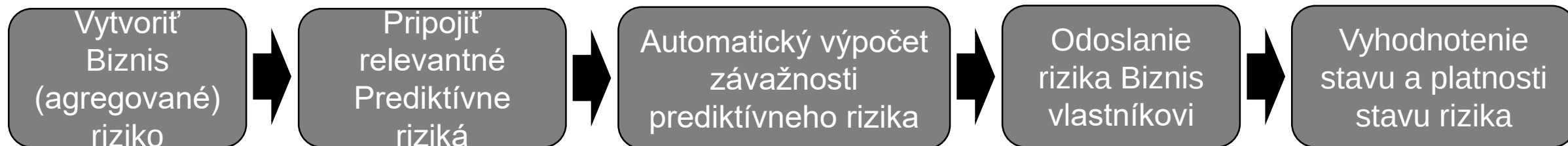
○ prediktívne riziká



spolu sme jedna banka

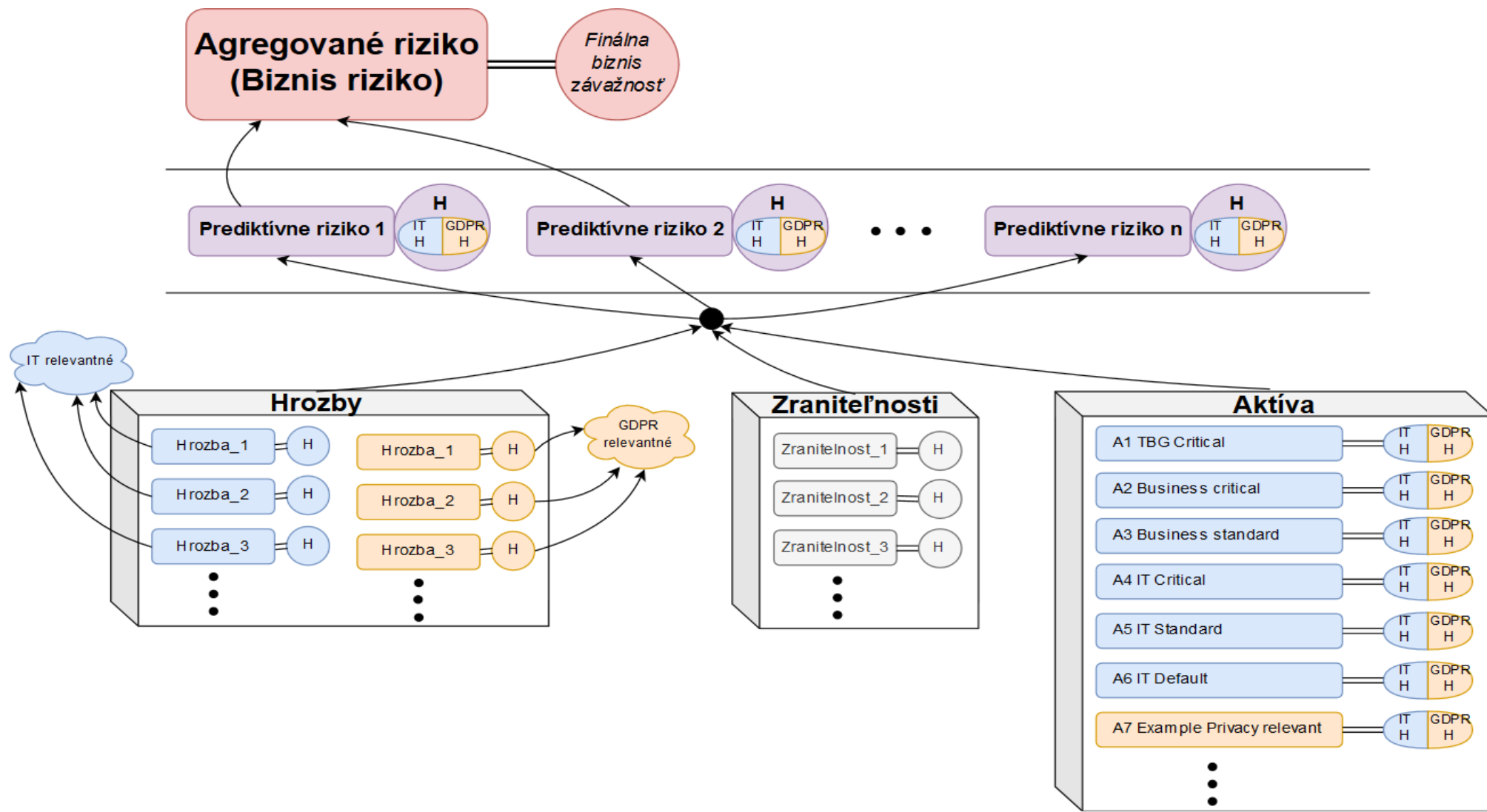


- **poces evidencie biznis rizík**



- výsledná závažnosť v sebe nesie hodnoty všetkých súvisiacich prediktívnych rizík
- hodnotenie je platné na určité časové obdobie
 - pravidelná aktualizácia platných rizík

◦ agregované riziká



spolu sme jedna banka



Business Intelligence

TB_Vulnerability

Number of Risks

25¹
Number of Audit Issues

Q CZ_Risk

A1.V1.T1

A1.V1.T4

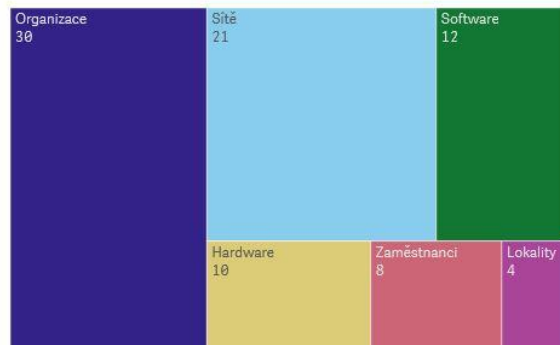
A1.V5.T1

CZ_Asset

CZ_Vulnerability

CZ_Threat

Number of Vulnerabilities by Folder 1



Number of Assets

103

V2
Score Vulnerability : 1,8
Score Vulnerability - Exposure : 3
Score Vulnerability - Severity : 3



ID_V	Q	CZ_Vulnerability
V1		Insufficient maintenance/faulty installation of stor
V1		Insufficient maintenance/faulty installation of stor
V2		Lack of periodic replacement schemes
V2		Lack of periodic replacement schemes
V3		Susceptibility to humidity, dust, soiling
V4		Sensitivity to electromagnetic radiation
V5		Lack of efficient configuration change control
V5		Lack of efficient configuration change control
V6		Susceptibility to voltage variations

TB_Risk

Number of Risks

25

CZ_Risk

CZ_Asset

Q CZ_Incident

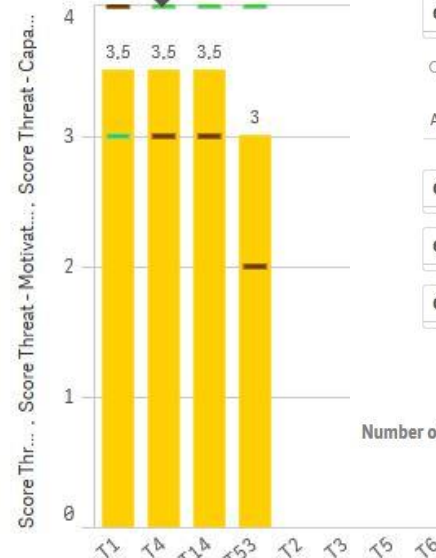
Audit issue 1

CZ_Task

CZ_Threat

CZ_Vulnerability

T4
Score Threat : 3,5
Score Threat - Motivation : 3
Score Threat - Capacity : 4

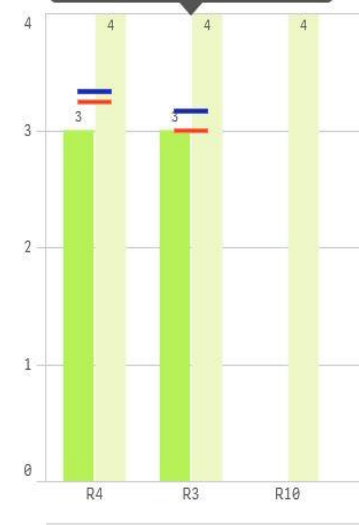


Number of Risks by Importance

Number of Audit Is

1

R3
Score Risk (Final) : 3
Score Risk (Predictive) : 4
dScore Risk - TB impact : 3,167
dScore Risk - Privacy impact : 3
dScore Risk Subcategory : -



spolu sme jedna banka



Ďakujem

spolu sme jedna banka

