

Informačná a kybernetická bezpečnosť prakticky

Igor Straka

*Business Area Manager – Cyber
Security*



Slovakia

Viac hodnoty.
Viac dôvery.

TÜV SÜD na prvý pohľad



150+
ROKOV KVALITY,
BEZPEČNOSTI A
UDRŽATEĽNOSTI



1,000+
ZASTÚPENÍ
VO SVETE **3x** v SR



24,000+
ZAMESTNANCOV *



574,000
CERTIFIKÁTOV



1
POSKYTOVATEĽ
RIEŠENÍ



100%
NEZÁVISLOSTI A
NESTRANNOSTI

*k 31.12.2018
Údaje boli zaokrúhlené.

Akreditácie



- ISO 9001
- ISO 14001
- **ISO 20000**
- ISO 22000
- **ISO 27001**
- **eIDAS**
- **TISAX***
- ISO 45001
- ISO 50001
- ISO 37001
- ISO 3834
- PEFC ST 2003
- TD SFCS 1002,1003, 1005:2014
- IATF 16949
- SA 8000
- EIDAS
- ISCC
- SCC
- AQAP
- IFS, BRC, HACCP

Agenda



1 Zákon o kybernetickej bezpečnosti

2 Základné princípy

3 Skúsenosti zo sveta

4 Implementačný štandard TÜV SÜD

5 Priestor na zlepšenie

Zákon o kybernetickej bezpečnosti

**Zákon č. 69/2018
vyhlášky:
362/2018,
164/2018,
165/2018
166/2018.**

**Povinnosti
Zaradenie do registra
Riadenie rizík
zavedenie procesov
Implementácie
opatrení
Zmluvné ošetrovanie
tretích strán
Vykonanie auditu**



Každý z nás sa spolieha na kritickú infraštruktúru, ako sú elektrárne, dodávky vody, energie, sietí, doprava alebo finančné služby....

Citát Sun Tzu, „Umenie vojny“

Poznať „seba“

- Identifikovať chránené aktíva
- Poznať cenu aktív
- Vedieť o slabinách a riešiť ich
- Riadiť riziká

Poznať „nepriateľa“

- Poznať Vektory útokov
- Postupy, nástroje, techniky

➤ Ak poznáš nepriateľa i seba samého, nebudeš porazený.

➤ Ak nepoznáš nepriateľa, ale poznáš sám seba, máš 50% šancu na víťazstvo.

➤ Ak nepoznáš sám seba, ani nepriateľa, prehráš.“



Jednoduché vysvetlenie zložitej témy

- Návod na implementáciu kybernetickej bezpečnosti pre kritickú infraštruktúru USA
- 12.2.2013 – 12.2.2014
- Aktuálna verzia 1.5 z 2018
- Framework je dobrovoľný a použiteľný pre každý sektor a veľkosť spoločnosti

NIST
**National Institute of
Standards and Technology**

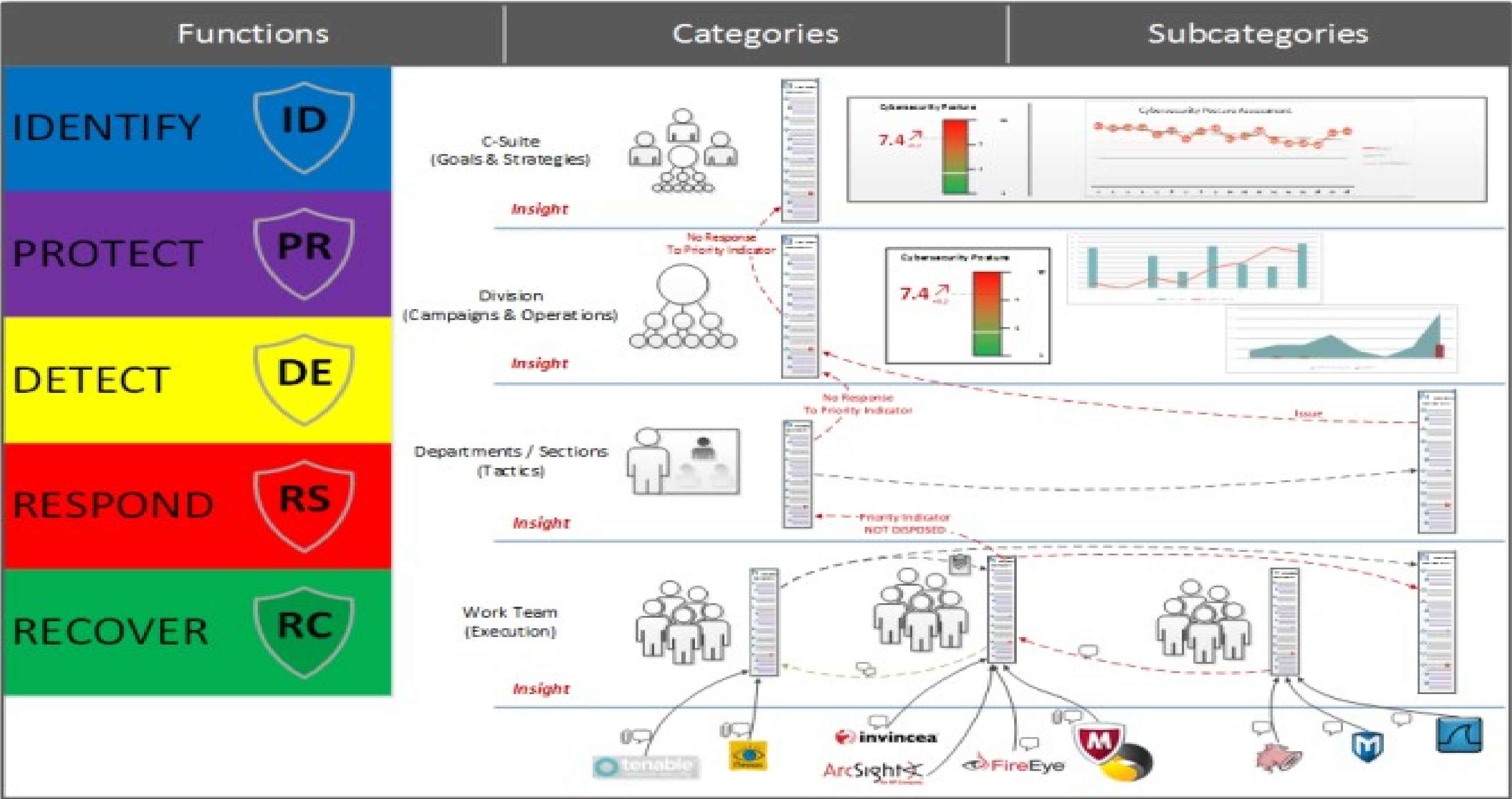


Funkcie – Kategórie – Pod kategórie

NIST Cybersecurity Framework Overview



Funkcie – Kategórie – Pod kategórie



Framework je Flexibilný k „rôznym“ štandardom IB

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6

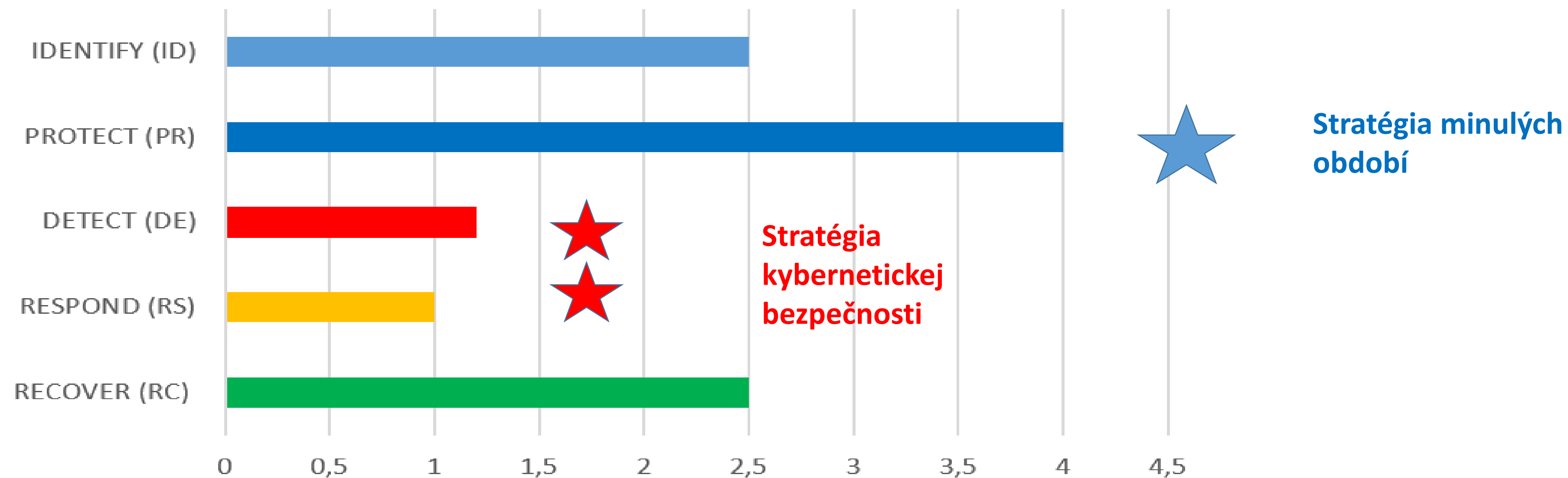
CIS CSC 12
COBIT 5 DSS05.02
ISA 62443-2-1:2009 4.2.3.4
ISO/IEC 27001:2013 A.13.2.1, A.13.2.2
NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8

Príklad mapovanie frameworku na ISO 27001

			Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Risk Assessment (ID.RA)	2	ID.RA-2: Informácia o kybernetickej hrozbe je získavaná z fór a zdrojov na zdieľanie informácií	1	A.6.1.4	Kontakt so záujmovými skupinami	1
						ID.RA-3: Hrozby, interné aj externé, sú identifikované a zdokumentované	1	CI.6.1.2	Posúdenie rizík informačnej bezpečnosti	1
						ID.RA-4: Identifikujú sa potenciálne obchodné vplyvy a pravdepodobnosť	1	A.16.1.6	Ponaučenie sa z incidentov informačnej bezpečnosti	1
						ID.RA-5: Na určenie rizika sa používajú hrozby, zraniteľnosti, pravdepodobnosti a vplyvy	3	CI.6.1.2	Posúdenie rizík informačnej bezpečnosti	1
						ID.RA-6: Identifikovali sa reakcie na riziká a stanovili sa priority	2	A.12.6.1	Správa a riadenie technických zraniteľností	2
			Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk Management Strategy (ID.RM)	2	ID.RM-1: Procesy riadenia rizík sú stanovené, riadené a odsúhlasené zainteresovanými subjektmi	2	CI.6.1.3	Ošetrenie rizík informačnej bezpečnosti	2
						ID.RM-2: Je stanovená a jasne vyjadrená tolerancia organizačného rizika	2	CI.8.3	Posúdenie rizík informačnej bezpečnosti	2
								CI.9.3	Preskúvanie manažmentom	1
						ID.RM-3: Stanovenie tolerance rizika zo strany organizácie je informované o jej úlohe v kritickej infraštruktúre a analýze špecifických sektorových rizík	2	CI.6.1.3	Ošetrenie rizík informačnej bezpečnosti	2
								CI.8.3	Posúdenie rizík informačnej bezpečnosti	2
								CI.8.3	Posúdenie rizík informačnej bezpečnosti	2
			Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply	Supply Chain Risk Management (ID.SC):	1	ID.SC-1: Procesy riadenia rizika kybernetického dodávateľského reťazca sú identifikované, zavedené, vyhodnotené, riadené a odsúhlasené zainteresovanými subjektmi	2	A.15.1.1	Politika informačnej bezpečnosti pre oblasť vs	3
								A.15.1.2	Riešenie bezpečnosti v rámci zmlúv s dodávateľmi	1
								A.15.1.3	Dodávateľské reťazce ICT	2
								A.15.2.1	Monitorovanie a preskúvanie dodávateľských služieb	1
								A.15.2.2	Riadenie zmien dodávateľských služieb	1
						ID.SC-2: Dodávateľia a partneri tretích strán informačných systémov, komponentov a služieb sa identifikujú, určujú priority a hodnotia pomocou procesu hodnotenia rizika cyber dodávateľského reťazca	1	A.15.2.1	Monitorovanie a preskúvanie dodávateľských služieb	1
								A.15.2.2	Riadenie zmien dodávateľských služieb	1
						ID.SC-3: Zmluvy s dodávateľmi a partnermi tretích strán sa používajú na implementáciu vhodných opatrení navrhnutých tak, aby spĺňali ciele programu kybernetickej bezpečnosti organizácie a plánu riadenia rizík kybernetického dodávateľského reťazca.	2	A.15.1.1	Politika informačnej bezpečnosti pre oblasť vs	3
								A.15.1.2	Riešenie bezpečnosti v rámci zmlúv s dodávateľmi	1
								A.15.1.3	Dodávateľské reťazce ICT	2
						ID.SC-4: Dodávateľia a partneri tretích strán sa rutinne posudzujú pomocou		A.15.2.1	Monitorovanie a preskúvanie dodávateľských služieb	1

Porovnanie zrelosti domén

Zrelosť jednotlivých domén

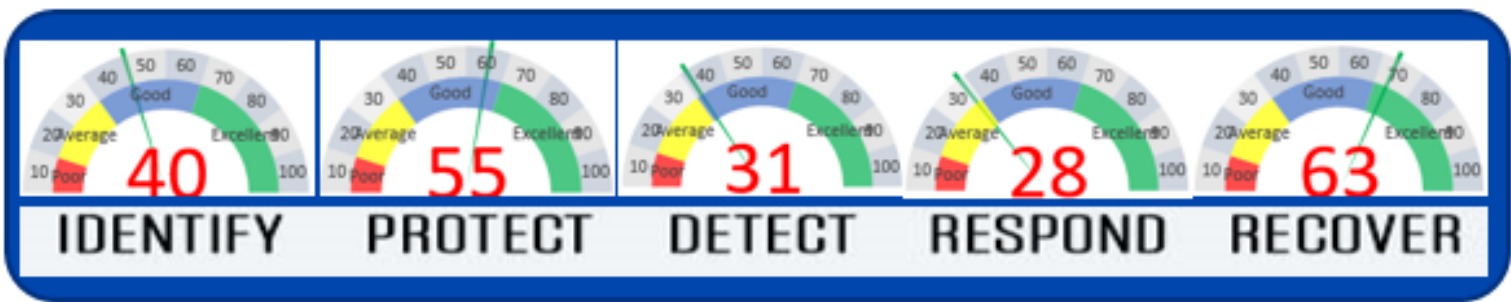


Návrh implementačného štandardu TÜV SÜD

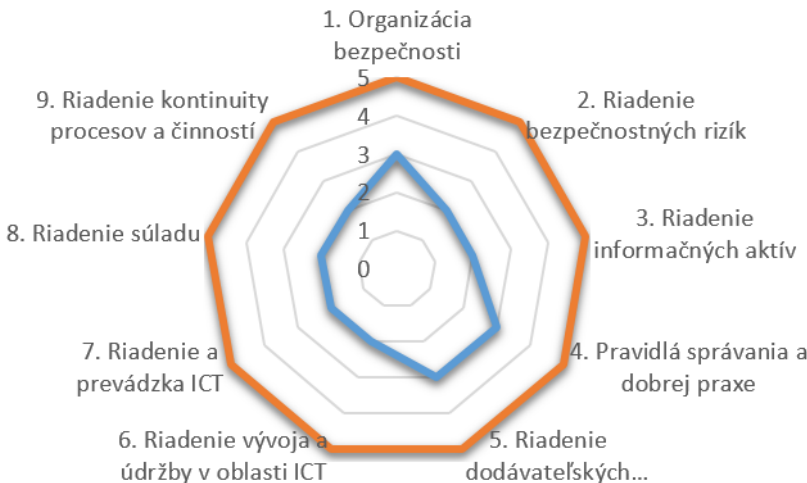
- Založený na ISO 27001
- Riadenie rizík podľa ISO 27005
- BCM podľa ISO 22301
- Špecifické opatrenia podľa CIS 20
- Hodnotenie procesov podľa ISO 14550 (maturita 1-5)
- Univerzálnosť
- Napojenie na požiadavky zákona č.69/2018
- Merateľnosť počas celého životného cyklu
 - Podľa NIST CSF
 - Podľa zákona č.69/2018
 - Podľa vektorov rôznych druhov útokov

Zákon o kybernetickej bezpečnosti

Function	Category	Category	R	Subcategory	Referenc	ISO 27001:2013 Príloha A	
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, reputation, financial, and legal) and the potential for the risk to be realized.	Risk Assessment (ID.RA)	2	1	ID.RA-2: Informácia o kybernetickej hrozbe je získavaná z fór a zdrojov na zdieľanie informácií	A.6.1.4	Kontakt so záujmovými skupinami	1
				ID.RA-3: Hrozby, interné aj externé, sú identifikované a zdokumentované	CI.6.1.2	Posúdenie rizík informačnej bezpečnosti	1
					A.16.1.6	Opaušenie sa z incidentov informačnej bezpečnosti	1
1. Organizácia bezpečnosti	1	3	5	1.1. Riadenie bezpečnostnej architektúry	A.8.1.1	Zoznam aktív	Kontinuálne zlepšovanie
					A.8.1.2	Vlastníctvo aktív	Kvantitatívne riadený
				1.2. Systém riadenia kybernetickej bezpečnosti	A.5.1.1	Politiky pre informačnú bezpečnosť	Nevykonávané
					A.6.1.1	Role a zodpovednosti v informačnej bezpečnosti	Jasne stanovený
					A.18.1.1	Identifikácia platnými právnymi predpismi a z	Plánované a sledované
					A.15.1.1	Politika informačnej bezpečnosti pre oblasť vs	Jasne stanovený
					A.7.2.1	Zodpovednosť manažmentu	Plánované a sledované
				1.3. Riadenie identít a prístupových práv	A.9.2.1	Registrácia a zrušenie registrácie užívateľa	Jasne stanovený
					A.9.2.2	Zriadenie prístupu užívateľa	Vykonávané neformálne
					A.9.2.3	Riadenie privilegovaných prístupových práv	Plánované a sledované
					A.9.2.4	Riadenie tajných autentizačných informácií už	Plánované a sledované
					A.9.2.6	Odobranie alebo úprava prístupových práv	Plánované a sledované
					A.9.3.1	Použitie tajných autentizačných informácií	Kontinuálne zlepšovanie
					A.9.4.2	Bezpečné postupy prihlásenia	Jasne stanovený
					A.9.4.3	Systém správy hesiel	Jasne stanovený
				1.4. Riadenie privilegovaných prístupov	A.11.2.6	Bezpečnostné zariadení a aktív mimo prevádzk	Plánované a sledované
2. Riadenie bezpečnostných rizik	2	2	2	2.1. Testovanie a bezpečnostná certifikácia systémov	A.18.2.2	Súlad s bezpečnostnými politikami a normami	Plánované a sledované
					A.18.2.3	Preskúmanie technického súladu	Plánované a sledované
					A.14.2.8	Testovanie bezpečnostných systémov	Jasne stanovený
				2.2. Metodika posudzovania vplyvu na ochranu osobných údajov	A.18.1.4	Súkromie a ochrana osobných údajov	Plánované a sledované
					A.18.2.2	Súlad s bezpečnostnými politikami a normami	Plánované a sledované
				2.3. Metodika posudzovania rizik	CI.4.1	Porozumenie organizácie a súvislostí v nej	Plánované a sledované
				2.4. Fyzická bezpečnosť a bezpečnosť prostredia	A.11.1.1	Fyzický bezpečnostný periméter	Jasne stanovený
					A.11.1.2	Fyzické kontroly vstupu	Plánované a sledované
					A.11.1.3	Zabezpečenie kancelárií, miestností a vybaven	Jasne stanovený
					A.11.1.4	Ochrana proti vonkajšími a prírodnými hrozbami	Jasne stanovený
					A.11.1.5	Práca v zabezpečených oblastiach	Vykonávané neformálne
3. Riadenie bezpečnostných rizik	3	2	2		A.11.1.6	Oblasti pre nakládku a vykládku	Plánované a sledované
					A.11.2.1	Umiestnenie zariadení a ich ochrana	Jasne stanovený



Súlád voči zákonu č.69/2018



1. Stanovenie aktuálneho stavu
2. Stanovenie cieľového stavu
3. Definovanie rozdielu Δ
4. Vypracovanie akčného plánu

Roadmap implementačného štandardu TÜV SÜD

**1: Identifikácia potreby
zaradenie ZS, DS, Dobrovoľne**

**2: GAP analýza s použitím
štandardu ISO 27001**

**3: Vykonať hodnotenie rizík s
použitím štandardu ISO 27005**

**4: Stratégia KB - politika -
nastavenie cieľovej úrovne**

**5: Zoznam opatrení prechodu
na požadovanú úroveň**

**6: Definovanie časového plánu
implementácie**

**7: Zmluvné vzťahy s tretími
stranami**

**8: Implementácia
dokumentovaných procesov**

**9: Implementácia technických
prostriedkov**

10: Audit systému

Benefits implementačného štandardu TÜV SÜD

- Štandard možno aplikovať pre každý sektor a veľkosť subjektu
- Využíva už zavedené procesy, nebude samostatný systém
- Opatrenia sú interpretované cez štandard ISO27001
- Štandard je šetrný k zdrojom, je viazaný striktne na riadenie rizík
- Aplikovaná zásada merateľnosti a zlepšovania počas implementácie aj počas prevádzky:
 - Podľa NIST CSF
 - Podľa zákona č.69/2018

Podporné aktivity pri zavádzaní kybernetickej bezpečnosti

1

Manažér kybernetickej bezpečnosti (Cyber Security Manager)



2

Interný audítor systémov manažérstva podľa ISO/IEC 27001



3

Manažér riadenie rizík v IT



4

Manažér kontinuity v podnikaní podľa ISO 22301





Ďakujem za pozornosť

Igor Straka

Business Area Manager – Cyber Security

Email: igor.straka@tuv-sud.sk

www.tuv-sud.sk



Slovakia

**Viac hodnoty.
Viac dôvery.**