

Agenda



01

**ISO 27002:2013 vs. ISO 27002:2022
vs. ostatný svet**

02

**Nová verzia štandardu ISO
27001/2:2022**

03

Zmena v opatreniach - Príloha A

04

**Nove možnosti aplikovania ISO
27002:2022**

05

**Prechod na novú normu 27001:2022,
benefity a vyhodnotenie**

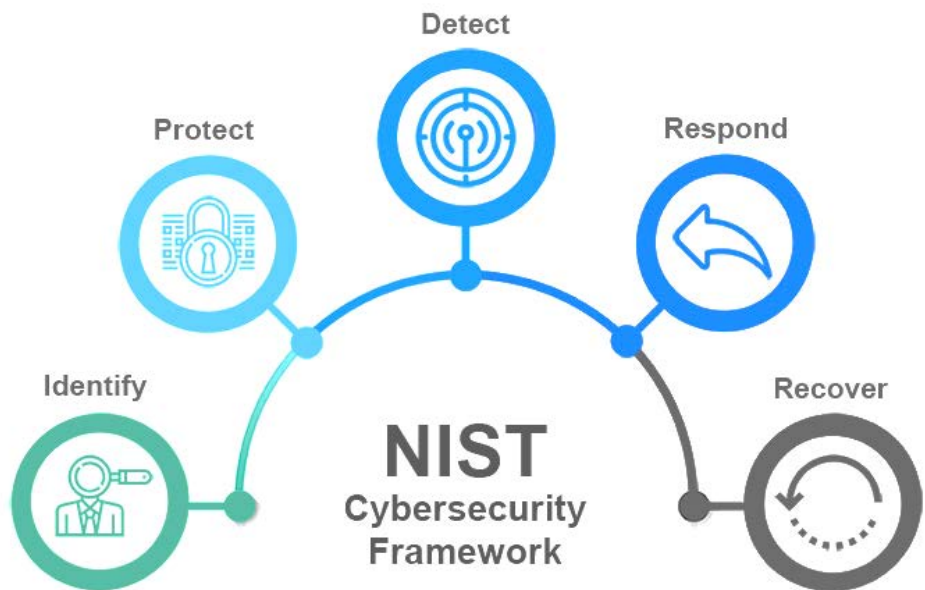
06

Príloha A.



Nová ISO 27001/2:2022

1.1 Porovnanie ISO 27001 /ISO 27002 :2013 s NIST CSF



- Návod na implementáciu kybernetickej bezpečnosti pre kritickú infraštruktúru USA
- Vznik: 12.2.2013 – 12.2.2014
- Aktuálna verzia 1.5 z 2018
- Framework je dobrovoľný a použiteľný pre každý sektor a veľkosť spoločnosti
- Zadávatel': Prezident USA - Barack Obama
- Dôvod: Jednoduchým spôsobom vysvetliť riadenie KB pre kritickú infraštruktúru USA

1.2 Porovnanie ISO 27001 /ISO 27002 :2013 s NIST CSF



NIST CSF:

- Celkové hodnotenie ako aj hodnotenie cez funkčné časti
- Hodnotenie plnenia opatrení cez CMM, nie binárne
- Cieľová hodnota nemusí byť len „5“ (Automotive TISAX cieľová hodnota „3“)
- Jednotlivé opatrenia referencované cez štandardy CIS CSC, COBIT, ISA 62443, ISO 27001, NIST SP 800
- Framework je dobrovoľný a použiteľný pre každý sektor a veľkosť spoločnosti



1.3 ISO 27001/ ISO 27002 - čo je čo?



- ISO 27001 je ústredným rámcom série ISO 27000 a využíva prístup založený na rizikách, ktorý pomáha organizáciám riadiť informačnú bezpečnosť.
- Základné požiadavky normy sú podporované súborom bezpečnostných opatrení, známym ako príloha A.
- ISO 27002 pojednáva o tom, ako možno jednotlivé opatrenia z ISO 27001 prílohy A implementovať.
- Na rozdiel od ISO 27001 organizácie sa nemôžu certifikovať podľa ISO 27002.
- Organizácie si môžu vybrať ďalšie opatrenia z iných štandardov, ako je napríklad rámec PCI DSS, NIST, CIS 20 atc.

Hlavné zmeny štandardu ISO 27001/ ISO 27002 :2022



2.1 Hlavné zmeny štandardu ISO 27001/ ISO 27002 :2022



Zmena, ktorá zásadne mení celé zameranie normy.
Táto zmena je priamo na prednej obálke štandardu

~~Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky.~~

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia — Systém manažérstva informačnej bezpečnosti
Požiadavky.

~~Bezpečnostné metódy; Pravidlá dobrej praxe riadenia informačnej bezpečnosti“.~~

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Riadenie informačnej bezpečnosti.

Štandard zahŕňa nové opatrenia týkajúce sa:

- ☐ kybernetických hrozieb
- ☐ cloudových služieb
- ☐ bezpečného vývoja
 - ☐ Privacy.

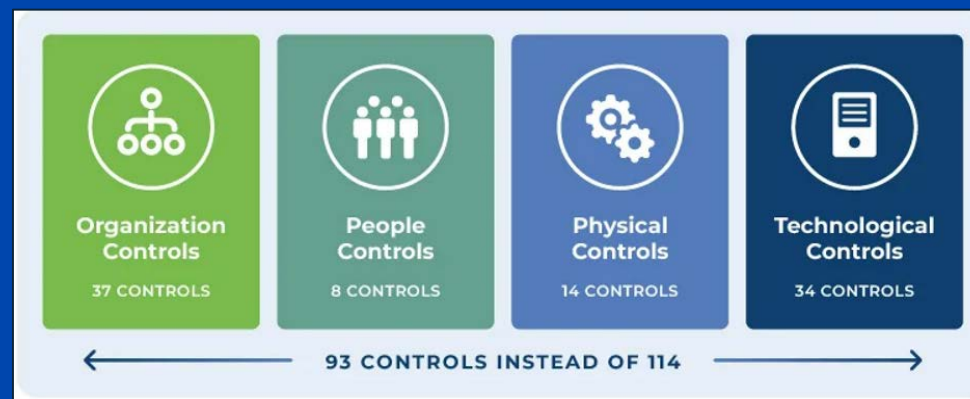
2.2 Čo sa zmenilo oproti verzii ISO 27002:2013?



Hlavným rozdielom novej ISO 27002 je štruktúra opatrení. Zatiaľ čo väčšina opatrení ISO 27002 zostáva nezmenená, ovládacie prvky boli preskupené zo 14 kategórií do 4 širokých kategórií, ktoré zahŕňajú

Organizačné opatrenia (37 opatrení) skupina 5.
Riadenie ľudí (8 opatrení) skupina 6.
Fyzické opatrenia (14 opatrení) skupina 7
Technologické opatrenia (34 opatrení) skupina 8

Počet opatrení sa znížil zo 114 na 93
Pribudlo 11 nových opatrení
Bolo vypustených 3 existujúcich opatrení
Konsolidovaných 48 opatrení do súčasných 19 opatrení.



3.1 Zlúčené opatrenia



Consolidated Controls			
5.1 – Policies for information	5.1.1, 5.1.2	8.1 – User endpoint devices	6.2.1, 11.2.8
5.9 – Inventory of information and other associated assets	8.1.1, 8.1.2	8.8 – Management of technical vulnerabilities	12.6.1, 18.2.3
5.14 – Information transfer	13.2.1, 13.2.2, 13.2.3	8.15 – Logging	12.4.1, 12.4.2, 12.4.3
5.15 – Access control	9.1.1, 9.1.2	8.24 – Use of cryptography	10.1.1, 10.1.2, 18.1.5
5.16 – Identity management	9.2.1, 9.4.3	8.25 – Secure development lifecycle	14.1.1, 14.2.1
5.17 – Authentication information	9.2.4, 9.3.1	8.26 – Application security requirements	14.1.2, 14.1.3
5.18 – Access rights	9.2.2, 9.2.5, 9.2.6	8.29 – Security testing in development and acceptance	14.2.8, 14.2.9
5.22 – Monitoring, review and change management of supplier services	15.2.1, 15.2.2	8.31 – Separation of development, test and production environments	12.1.4, 14.2.6
5.29 – Information security during disruption	17.1.1, 17.1.2, 17.1.3	8.32 – Change management	12.1.2, 14.2.2, 14.2.3, 14.2.4
7.10 – Storage media	8.3.1, 8.3.2, 8.3.3		

3.2 Nové a zrušené opatrenia



New Controls	
5.7 – Threat intelligence	8.11 – Data masking
5.23 – Information security for use of cloud services	8.12 – Data leakage prevention
5.30 – ICT readiness for business continuity	8.16 – Monitoring services
7.4 – Physical security monitoring	8.22 – Web filtering
8.9 – Configuration management	8.28 – Secure coding
8.10 – Information deletion	
Deleted Controls	
8.2.3 – Handling of assets	11.2.5 – Removal of assets
16.1.3 – Reporting information security weaknesses	

3.3 Nových 11 nových opatření

THE NEW CONTROLS ARE:



Threat
intelligence



Information
security for use
of cloud services



ICT readiness
for business
continuity



Physical
security
monitoring



Configuration
management



Information
deletion



Data
masking



Data leakage
prevention



Monitoring
activities



Web
filtering



Secure
coding

4.1 Pridanie atribútov k opatreniam



heštegy

Ďalšie riadiace atribúty nad rámec ISO/IEC 27002 Článok 4.2 normy ISO/IEC 27002:2022 hovorí: „Organizácia môže použiť atribúty na vytvorenie rôznych pohľadov, ktoré predstavujú rôzne kategorizácie opatrení“. Táto časť navrhuje niekoľko ďalších atribútov, ktoré by sa podľa potreby mali zväžiť..

4.2 Pridanie atribútov k opatreniam



Ďalším doplnkom je, že každému **opatreniu** sú priradené **heštagy**, ktoré zodpovedajú 5 atribútom **opatrenia**:

- **Vlastnosti informačnej bezpečnosti** (#Dôvernosť; #Integrita; #Dostupnosť).
- **Typ opatrenia** (#Preventívne; #Detekčné; #Nápravné).
- **Koncepcia kybernetickej bezpečnosti** #Identifikovať; #Chrániť; #Objaviť; #Reagovať; #Obnoviť). **Tieto atribúty sú v súlade s NIST Cybersecurity Framework.**
- **Bezpečnostné domény** (#Riadenie a ekosystém; #Ochrana; #Obrana; #Odolnosť).
- **Prevádzkové oblasti** (#Governance; #Asset_management; #Information_protection; #Human_resource_security; #Physical_security; #System_and_network_security; #Application_security; #Secure_configuration; #Identity_and_access_management; #Threat_and_vulnerability_management; #Continuity; #Supplier_relationships_security; #Legal_and_compliance; #Infor_sec_event_management; #Infor_security_assurance

Ďalšie riadiace atribúty nad rámec ISO/IEC 27002 Článok 4.2 normy ISO/IEC 27002:2022 hovorí: „Organizácia môže použiť atribúty na vytvorenie rôznych pohľadov, ktoré predstavujú rôzne kategorizácie opatrení“. Táto časť navrhuje niekoľko ďalších atribútov, ktoré by sa podľa potreby mali zvážiť..

4.3 Prvky opatrenia a ich rozloženie



7.9 Security of assets off-premises

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Off-site assets should be protected taking into account the different risks.

Purpose

To prevent loss, damage, theft or compromise of off-site assets and interruption to the organization's operations.

Guidance

Any device used outside the organization's premises which stores or processes information (e.g. mobile device), including devices owned by the organization and devices owned privately and used on behalf of the organization (BYOD) needs protection. The use of these devices should be authorized by management.

Názov : Krátky názov opatrenia;

Tabuľka atribútov : Tabuľka zobrazujúca atribúty daného opatrenia;

Popis opatrenie : Definícia požiadaviek na dané opatrenie;

Cieľ : Aký je cieľ opatrenia a čo by malo dosiahnuť;

Usmernenie : Popis implementácie opatrenia;

Ďalšie informácie : Vysvetľujúci text alebo odkazy na iné súvisiace zdroje.

4.4 Praktické využitie atribútov opatrení

NIST CSF



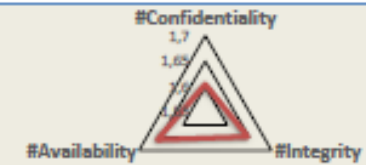
4.5 Praktické využitie atribútov opatrení

Report Nr.3 - Information security properties

Kategória opatrenia	Počet patrení	Piomer súladu (1-5)
#Confidentiality	86	1,60
#Integrity	82	1,65
#Availability	82	1,66



Súl'ad kategórii opatrení

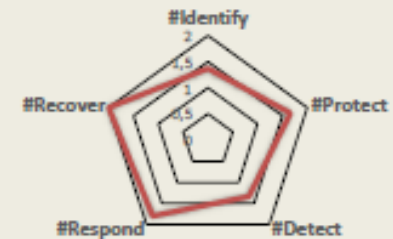


Report Nr.4 - Cybersecurity concepts

Kategória opatrenia	Počet patrení	Piomer súladu (1-5)
#Identify	19	1,37
#Protect	71	1,66
#Detect	15	1,33
#Respond	10	1,80
#Recover	4	2,00



Súl'ad kategórii opatrení



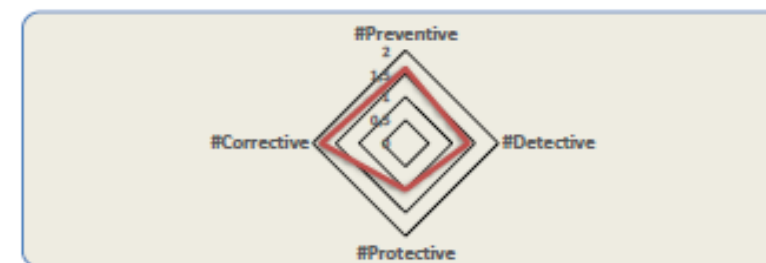
4.6 Praktické využitie atribútov opatrení

Report Nr.2 - Control type

Kategória opatrenia	Počet patrení	Piomer súladu (1-5)
#Preventive	82	1,61
#Detective	14	1,36
#Protective	1	1,00
#Corrective	11	1,82

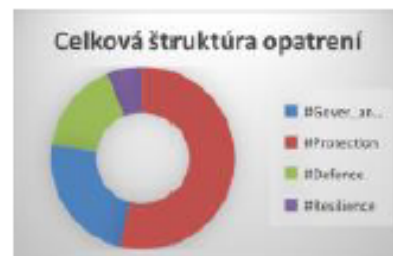


Súlad kategórií opatrení



Report Nr.6 - Security domains

Kategória opatrenia	Počet patrení	Piomer súladu (1-5)
#Gover_and_Ecosystem	30	1,40
#Protection	69	1,68
#Defence	21	1,33
#Resilience	8	1,75



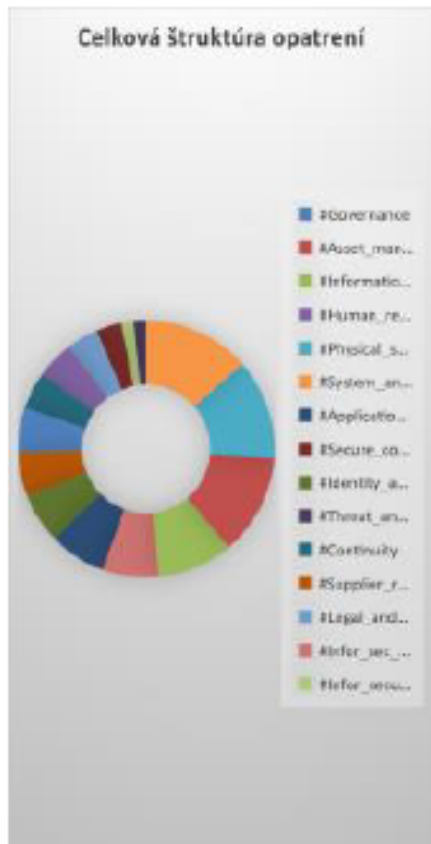
Súlad kategórií opatrení



4.7 Praktické využitie atribútov opatrení

Report Nr.5 - Operational capabilities

Kategória opatrenia	Počet patrení	Piemer súladu (1-5)
#Governance	7	2,00
#Asset_management	16	1,81
#Information_protection	12	1,17
#Human_resource_security	6	1,50
#Physical_security	16	2,44
#System_and_network_security	17	1,12
#Application_security	9	1,00
#Secure_configuration	4	1,25
#Identity_and_access_management	8	2,13
#Threat_and_vulnerability_management	2	0,50
#Continuity	6	1,67
#Supplier_relationships_security	7	1,00
#Legal_and_compliance	5	2,00
#Infor_sec_event_management	9	1,33
#Infor_security_assurance	2	1,00

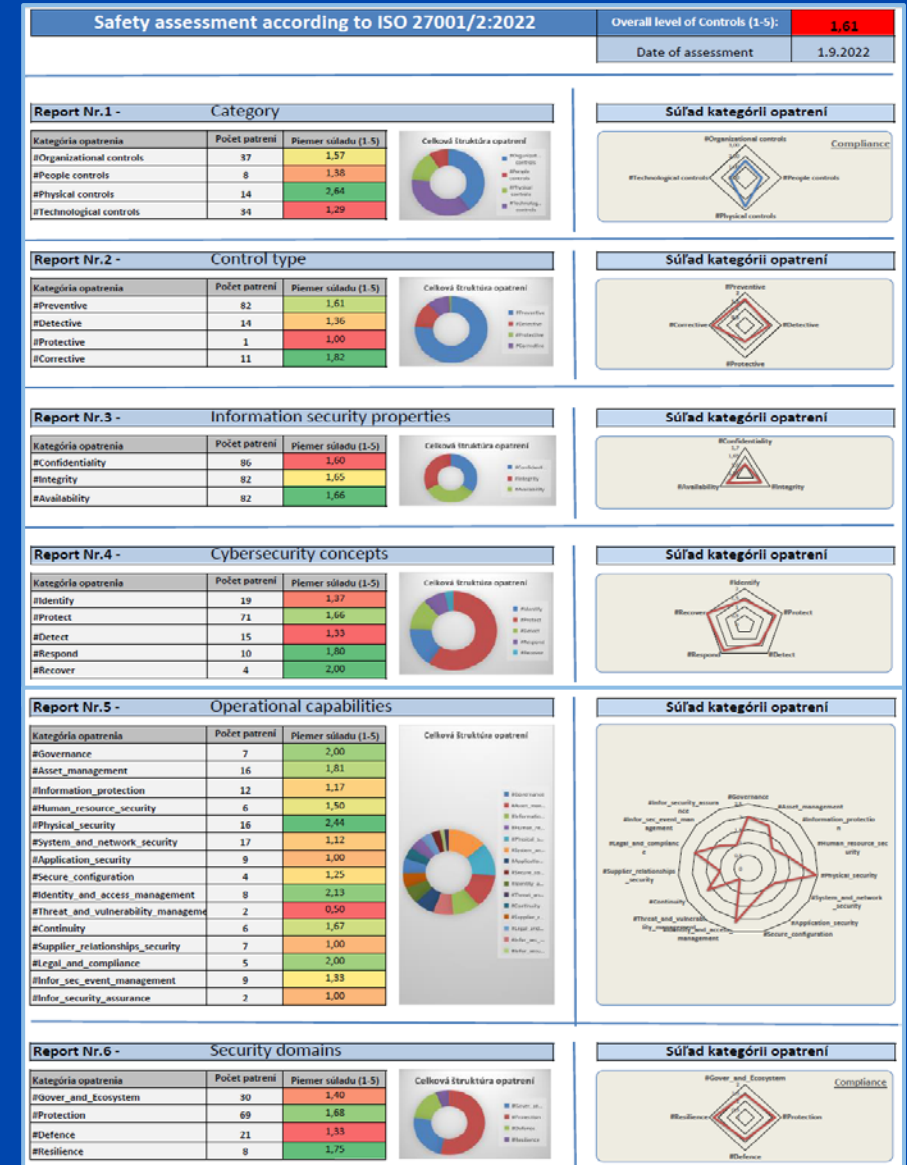


Súlad kategórii opatrení



4.8 Ako aplikovať #heštegovy?

- Vykonať v rámci SOA hodnotenie formou CMM (0-5)
- Prepojenie SOA s prevodovou tabuľkou atribútov opatrení.
- Dostávate report



5.1 Úprava Vášho zabezhnutého systému ISMS podľa ISO 27001:2013

- Aktualizovať hodnotenie rizík, z dôvodu aktualizácie opatrení na zníženie rizík.
- Aktualizácia vyhlásenia o aplikovateľnosti (SOA).
- Aktualizácia niektorých politík/ smerníc/ postupov, aby odrážali zmeny v ISO 27002:2022.
- Aktualizovať KPI, aby odrážali zmeny v prílohe A.
- Aktualizovať program interného auditu ISMS, aby odrážal zmeny vo vašom ISMS.
- Pokiaľ uznáte za vhodné, aplikovať atribúty na analytické reporty



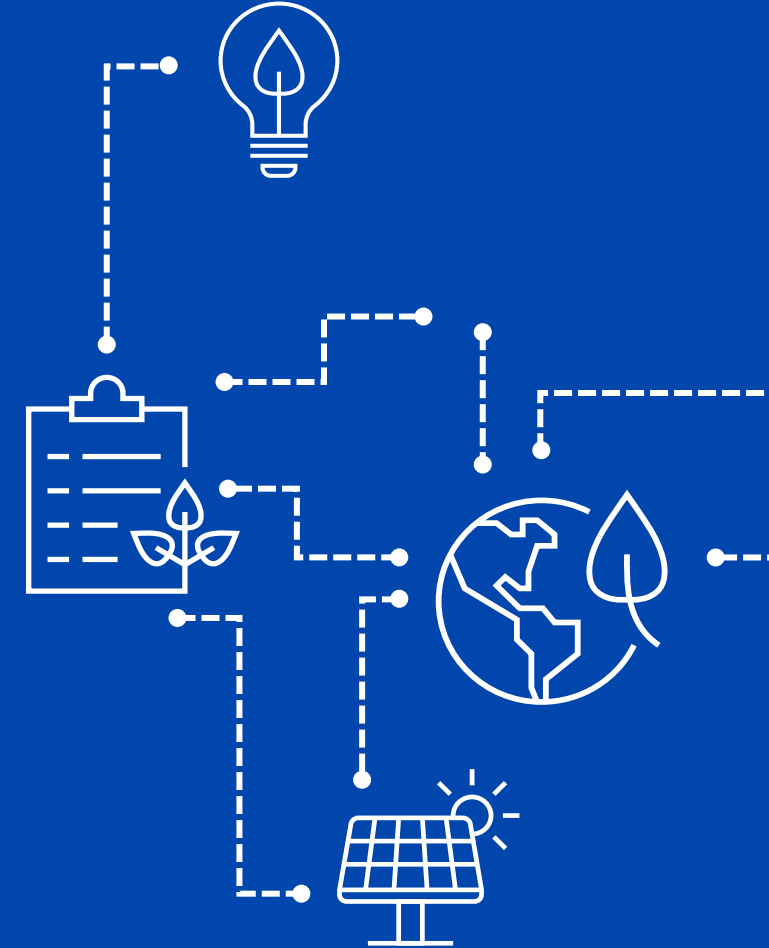
5.2 Hlavné benefity novej verzie ISO 27001 27001/2:2022



Obsah opatrení rozšírený o oblasti kybernetických hrozieb, cloudu, developmentu a Privacy.

Získanie analytického / reportovacieho nástroja – aplikovanie #heštegov

Zjednodušenie riadenia rizík, kde dostávajú jeden register opatrení pre IB, KB, CLOUD, PRIVACY



Porovnanie ISO 27001/2:2013 vs. ISO 27001/2:2022 vs. CSF NIST



Štandard	Rozsah	Referencovnie	Analytika / Report.	Výsledok
ISO 27001/2:2013	★	★ ★	★	4 ★
ISO 27001/2:2022	★ ★ ★	★ ★	★ ★ ★	8 ★
CSF NIST	★ ★	★ ★ ★	★ ★	7 ★



Otázky?

Ďakujem za pozornosť



Ing. Igor Straka, TÜV SÜD

Business Area Manager

Lead Auditor: ISO 27001, ISO
20000:1, ISO 22301, eIDAS, GDPR,
AKB, CEH08

Email: igor.straka@partner.tuvsud.com
0917 941 299

Sledujte nás aj na:



tuvsud.com/sk
Info.sk@tuvsud.com