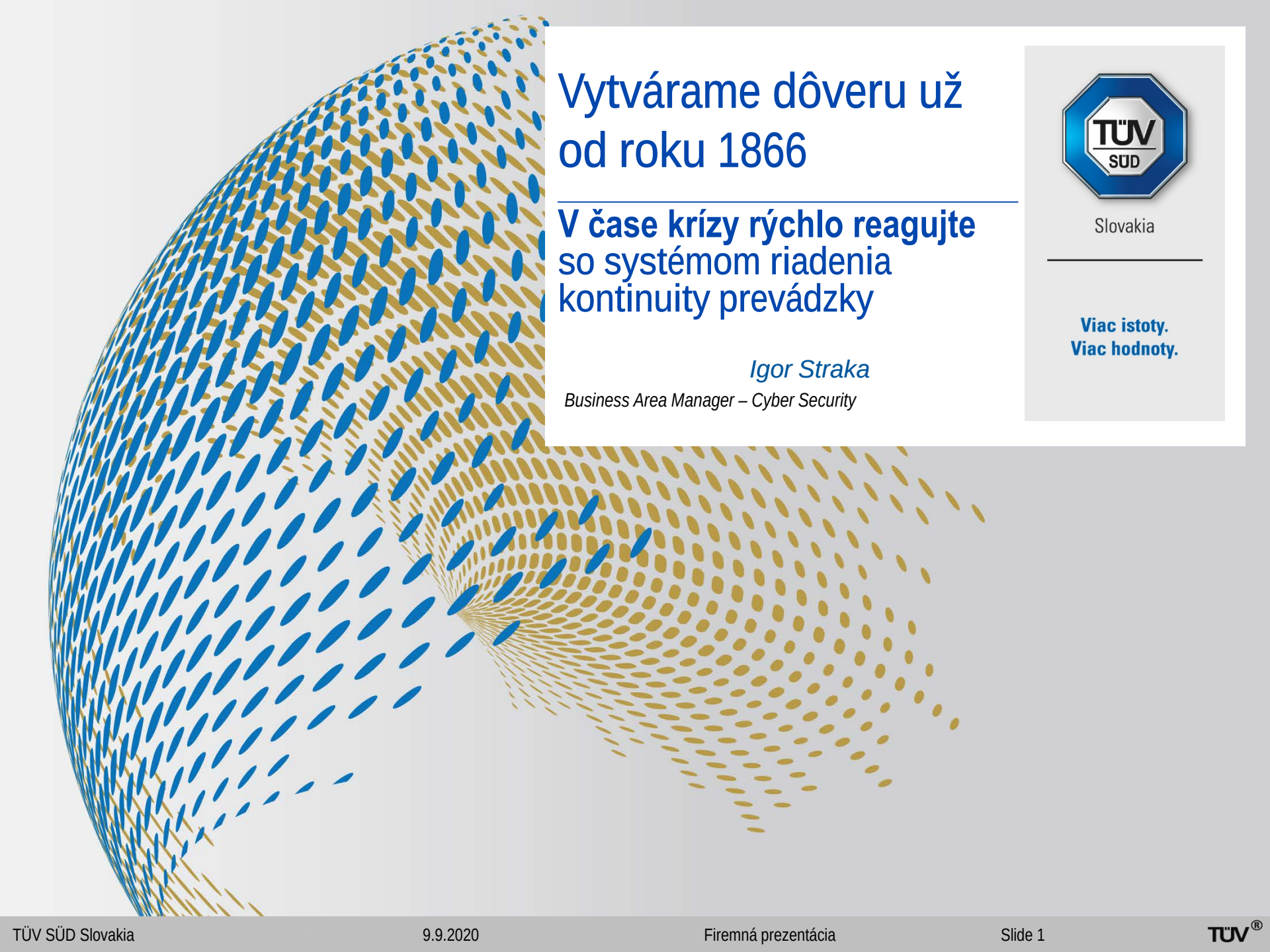




Vytvárame dôveru už od roku 1866

V čase krízy rýchlo reagujte so systémom riadenia kontinuity prevádzky

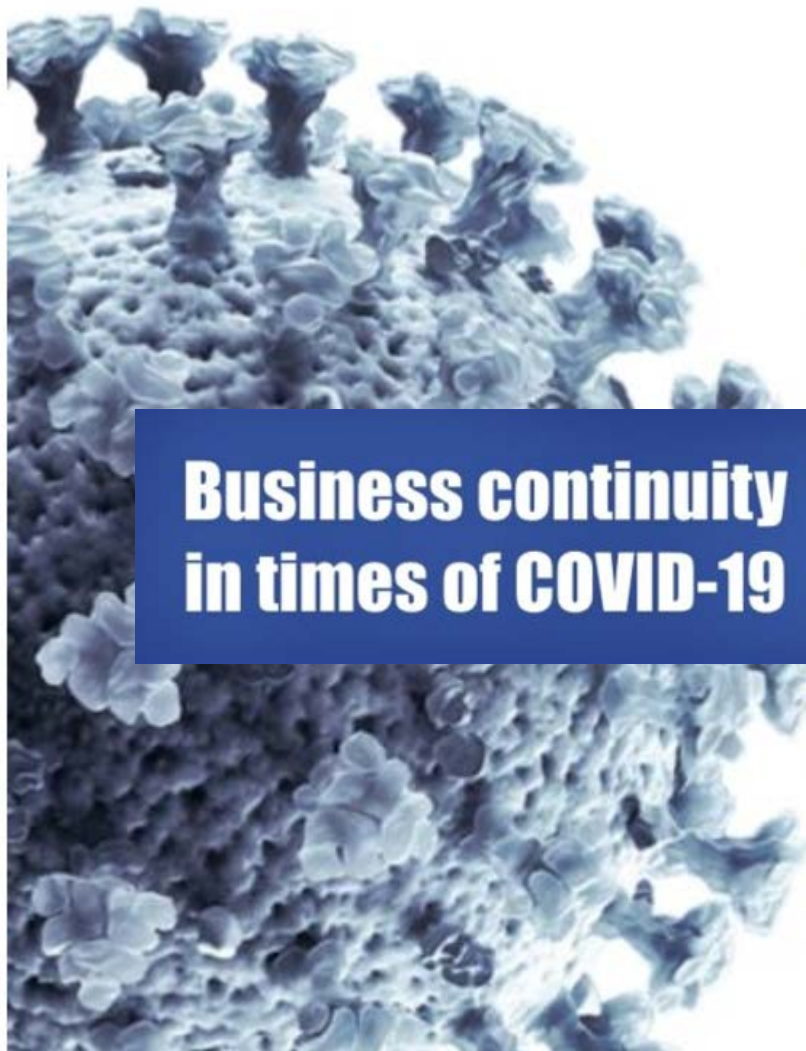
Igor Straka

Business Area Manager – Cyber Security



Slovakia

**Viac istoty.
Viac hodnoty.**



1 Aplikovateľnosť BCMS vo svete

2 Dôvody pre Ne/zavedenie BCMS

3 Riziká COVID-19 pre ICT

**4 Zavedenie BCMS podľa štandardu
ISO 22301**

5 Benefity BCMS

BCM - je rámec na zníženie potenciálneho finančného, právneho, prevádzkového alebo reputačného dopadu vyplývajúceho z krízy.

KRÍZA - narušuje poskytovanie obchodných činností

- Výpadok budovy (open space)
- Výpadok personálu
- Výpadok ICT

Väčšina kríz je kombináciou základných kríz

- Ako je na tom **KORONA?**

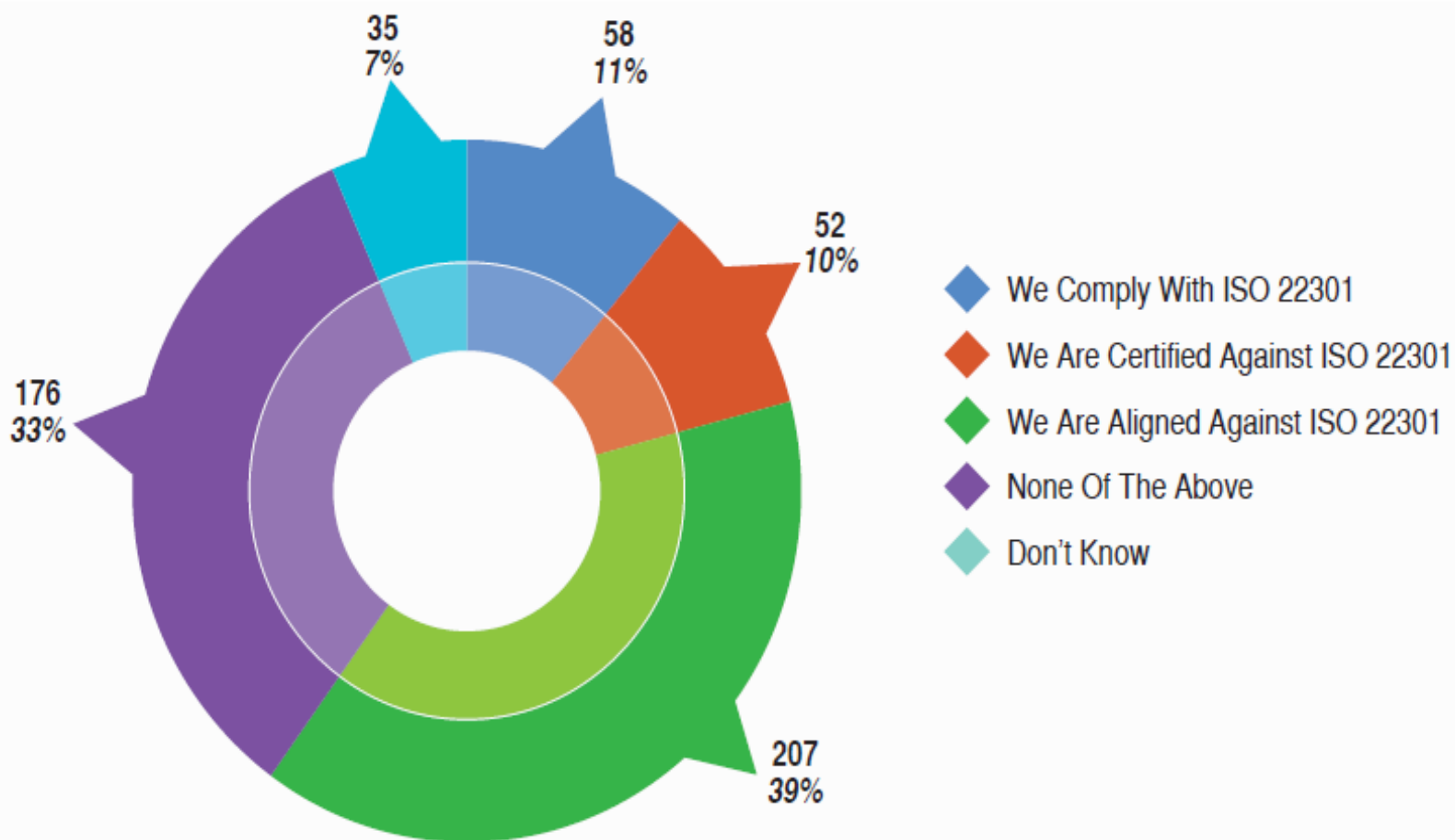


1.2 Počet zavedení BCMS



Slovakia

Approach to ISO 22301



2.1 Prečo nemáme zavedené BCM?

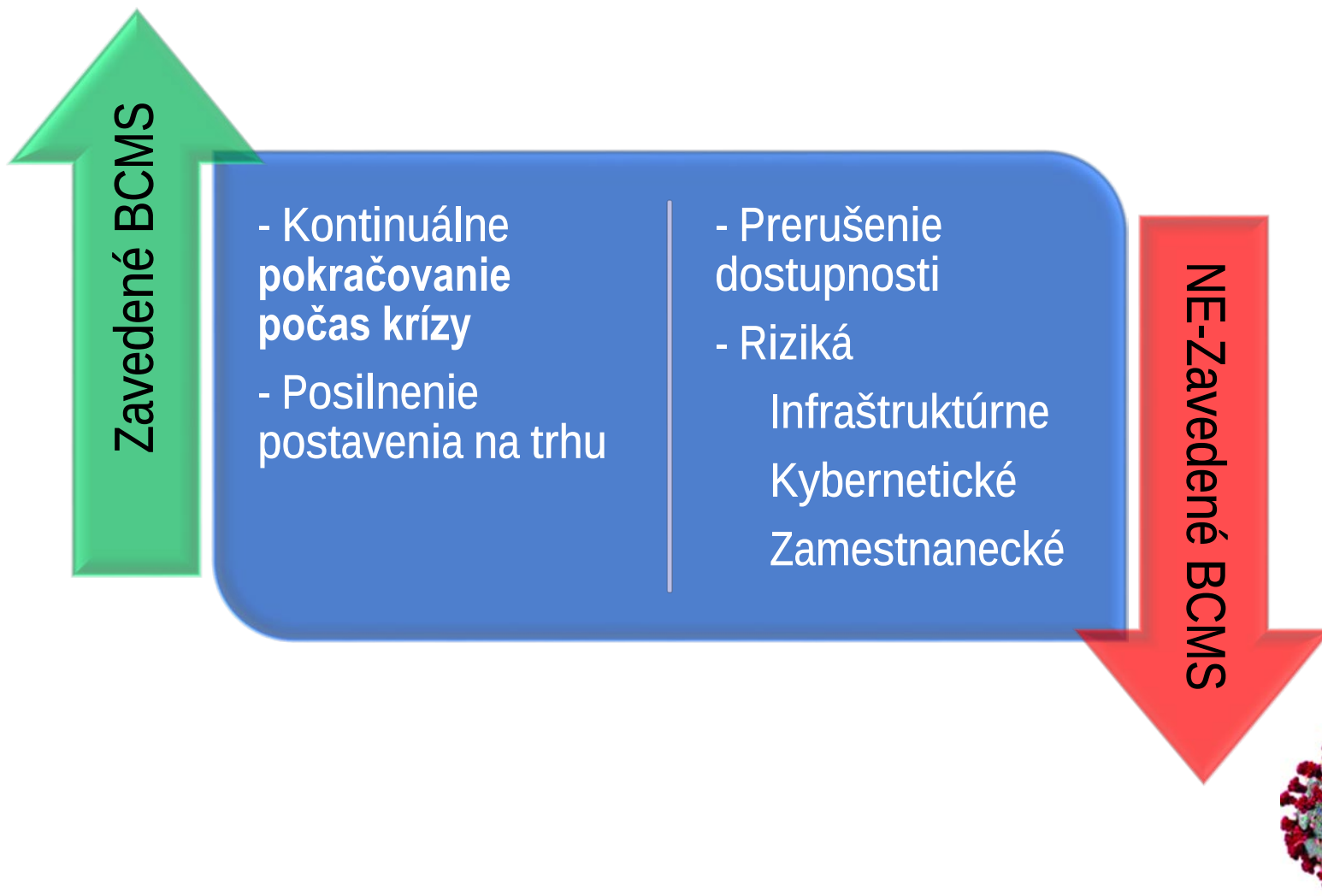


Slovakia

Mnoho organizácií sa pokúsilo ospravedlniť z programu BCM - verí tomu,

že „Nám sa to nestane“ :

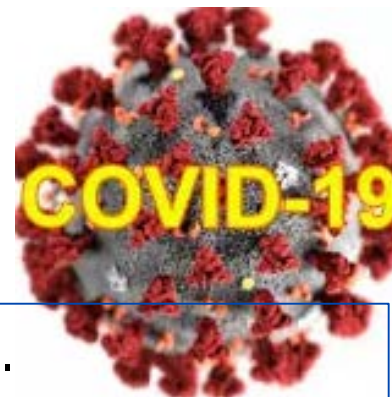
- I. **Nemáme čas** na vývoj a implementáciu programu BCM
- II. Program BCM je určený iba pre väčšie podniky. Sme príliš malá firma.
- III. Naš región nie je náchylný na prírodné katastrofy.
- IV. Program BCM je nevyhnutný, ale v tom čase nie je najvyššou prioritou.
- V. Naše podnikanie má veľmi minimálne externé riziká.
- VI. Máme zálohu dát a riešenie obnovy po havárii v IT



3.2 Dopady KORONA krízy na ICT prostriedky



Slovakia



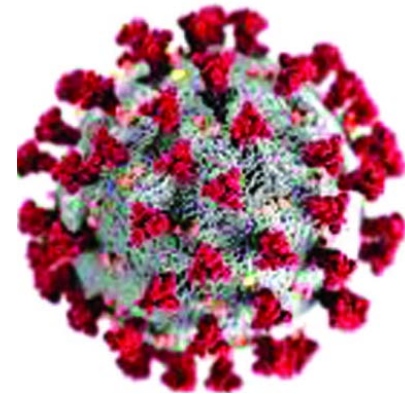
- Počet ľudí pracujúcich z domu sa výrazne zvýšilo.
- Internetový prenos sa zvýšil o 25 až 30%
- Nárast DDoS útokov narástol o 20-40%
- V tímoch sa pripája dvojnásobok ľudí
- Video hovory v marci 2020 vzrástli o viac ako 1 000%.
- Využívanie VPN je celosvetovo päťkrát vyššie.

3.3 COVID-19 – Infraštruktúrne riziká



Slovakia

- Pripravenosti infraštruktúry v súvislosti so zvýšeným náporom zo strany zamestnancov pracujúcich na diaľku.
- Overenie prevádzkyschopnosti **systémov** spoločnosti **na diaľku** bez fyzického prístupu IT zamestnancov
- Mapovanie kritických miest v infraštruktúre v prípade prevádzky na diaľku a návrh opatrení
- Definícia **zodpovedností dodávateľov** podľa zmluvy o úrovni poskytovaných služieb (SLA) v prípade krízových situácií a návrh na ich úpravu
- Nastavenie **dostatočnej IT podpory** pre zamestnancov pracujúcich na diaľku
- Zhodnotenie **počtu licencií** pre aplikácie zaisťujúce vzdialený prístup

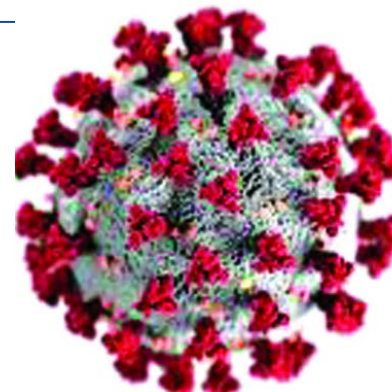


3.4 COVID-19 – Kybernetické riziká

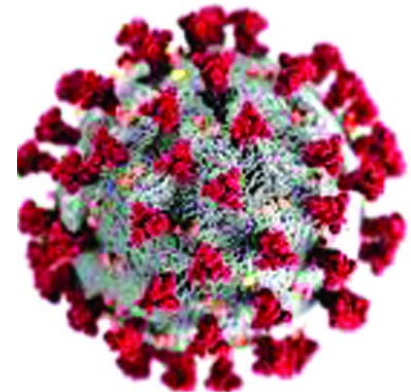


Slovakia

- Kontrola zabezpečenia a monitoring aplikácií pre vzdialený prístup
- Overenie aplikácií pre vzdialený prístup (VPN a pod.) + patchovanie, Hardening
- Zvýšenie povedomia o špecifických prípadoch útokov sociálneho inžinierstva v rámci komunikácie



- **Analýza kľúčových rolí** vyžadujúcich on-site prístup a riešenie ich absencie (napr. zastupiteľnosť)
- Návrh opatrení na zabezpečenie zvládania stresu a stresových situácií u zamestnancov
- Určenie spôsobu lokalizácie a rozloženia zamestnancov pri rôznych stupňoch utlmenia prevádzky
- Určenie prístupu k mobilite zamestnancov (delenie smien, transport a pod.)



4.1 Štandard na zavedenie BCM



Slovakia

BCMS - zaistiť kontinuitu a obnovu kľúčových procesov a činností organizácie v časoch krízy

- **BS 25999-1:2006** Business Continuity Management.
 - **BS 25999-2:2007** Specification for Business Continuity Management
-
- **ISO 22301:2012** – Business continuity management systems – Requirements
 - **ISO 22313:2012** — Guidelines for – Business continuity management systems
 - **ISO/IEC 27002** — Code of practice for information security management
 - **ISO/IEC 31000** — Risk management - Guidelines



- Kapitoly 1 -3 všeobecná časť **(Kontext)**
- Kapitola 5 **(Vedenie)** prezentuje požiadavky na podporu vedenia, role, zodpovednosti, politika.
- Kapitola 6 **(Plánovanie)** prípravu plánov pre jednotlivé krízy.
- Kapitola 7 **(Podpora)** poskytnutie zdrojov.
- Kapitola 8 **(Prevádzka)** vyžaduje nastavenie procesov BCM, posúdenie rizík, stanovenie priorít pre obnovu, analýzy dopadov, vytvorenie stratégie, zavedenie plánov a postupov kontinuity činností a ich testovanie.
- Kapitola 9 **(Vyhodnocovanie)** predpisuje monitorovanie, meranie, vykonanie auditov
- Kapitola 10 **(Zlepšovanie)** požaduje implementáciu nápravných opatrení na odstránenie identifikovaných nezhôd



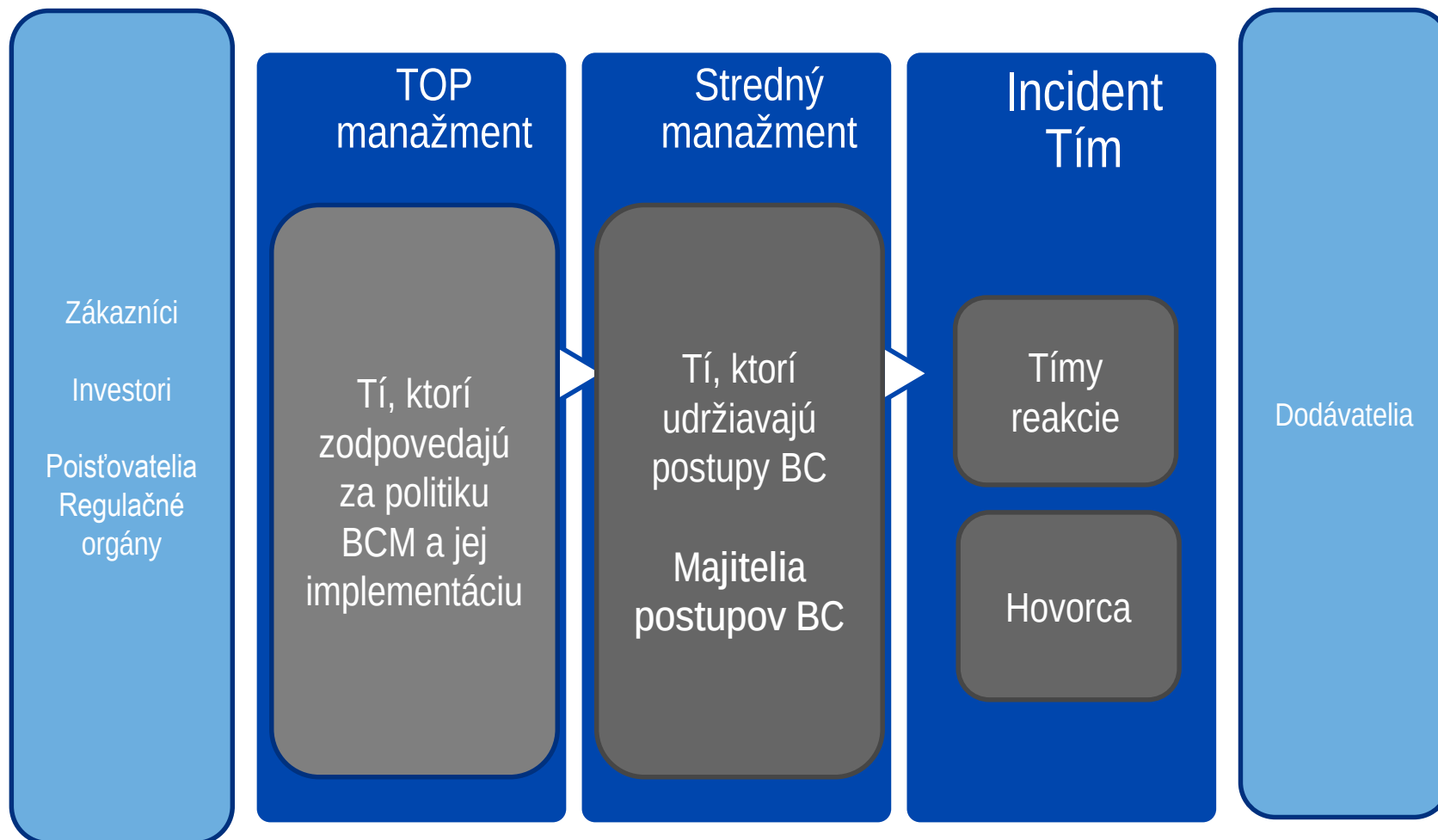


4.4 Potreby a očakávania zainteresovaných strán



Slovakia

Potreby a očakávania zainteresovaných strán



4.5 Analýza dopadov na podnikanie (BIA)



Slovakia

MTO (Maximum Tolerable Outage) - určuje pre každú činnosť maximálnu tolerovanú dobu narušenia činnosti, pre ktorú sú dopady pre organizáciu ešte akceptovateľné.

RTO (Recovery Time Objective) - určuje čas obnovy na požadovanú (čiastočnú alebo plnú) úroveň *

RPO (Recovery Point Objective) maximálna strata údajov (databázy, aplikácie a súbory, ale aj všetky služby napr. E-mail). *

MBCO (Minimum Business Continuity Objective) - Minimálne ciele kontinuity činnosti - určiť minimálnu prijateľnú úroveň kapacity požadovanú ihneď po zotavení.

Požadované zdroje - berúc do úvahy MBCO (počet transakcií, zákazníkov, produktov atď.), Mali by ste určiť, koľko ľudí a ďalších zdrojov potrebujete na zotavenie.

Identifikácia závislostí – definovanie závislostí na iné procesy, dodávateľov....

4.6 Zistenie RTO a RPO – Zber informácií



Slovakia

ICT	BIA číslo	Dopad 1 - 4						RPO 1 - 4						RTO (hod)	RPO (hod)
		2h	4h	8h	24h	48h	168h	2h	4h	8h	24h	48h	168h		
Systém 1	6	2	2	3	3	4	4	1	1	2	3	4	4	8h	24h
Systém 2	7	2	2	2	3	3	4	1	2	3	3	4	4	24h	8h
Systém 3	5	2	3	3	4	4	4	1	3	3	4	4	4	4h	4h
Systém 4	8	2	2	3	3	4	4	1	1	2	3	3	4	8h	24h
Systém 5	4	2	3	3	4	4	4	1	1	2	3	4	4	4h	24h
Systém 6	9	1	2	3	3	3	3	1	1	2	3	3	4	8h	24h

Výstupy:

1. Zoznam kritických systémov
2. Zistenie SLA (RTO) – nutné konfrontovať s architektúrou
3. Zistenie RPO – podklad pre backup politiku
4. Zameranie sa na Riziká s cieľom zníženia dopadu a frekvencie
5. Návrh BCP s časom obnovy menším ako RTO

- Prieskum dokumentácie
- Anketa / Dotazník
- Interview
- Cvičenie založené na workshope / scenári

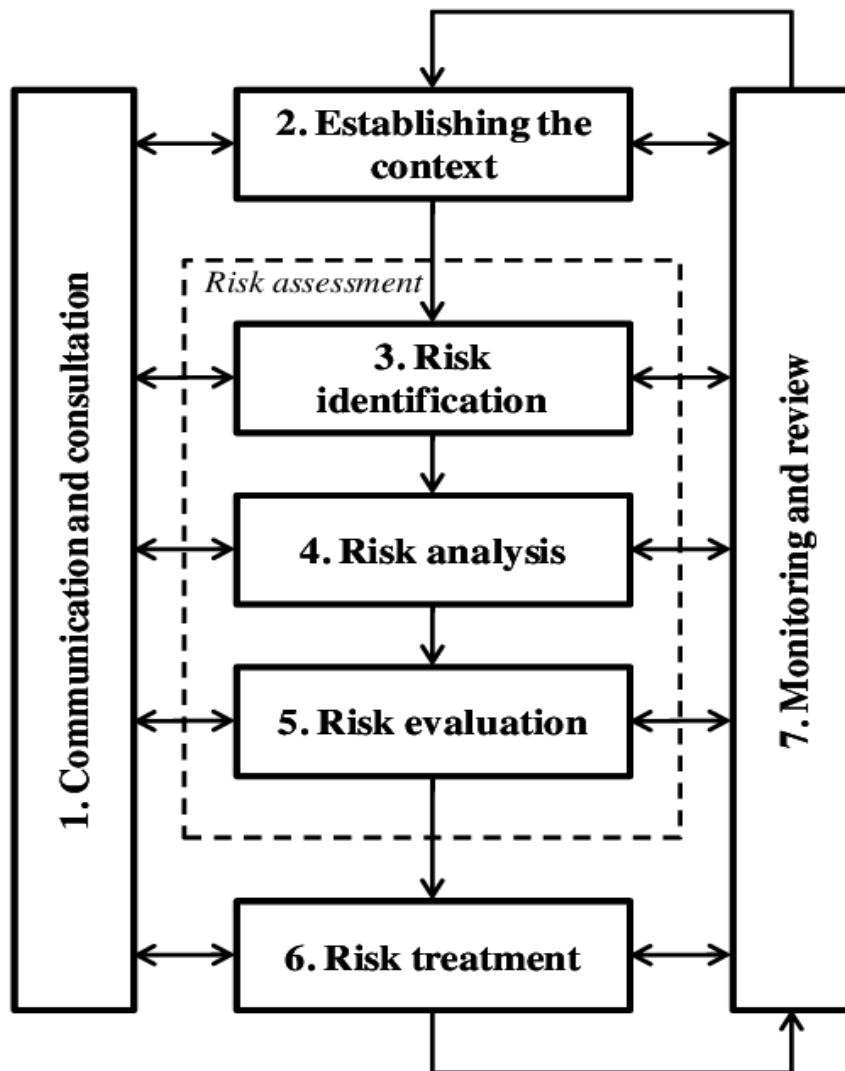
Zaistite, aby údaje boli:

- Správne - údaje sú presné a spoľahlivé, vierohodné a rozumné
- Konzistentné - údaje sú jasné a opakovateľné
- Aktuálne - údaje sú aktuálne a sú k dispozícii
- Kompletné - údaje sú komplexné

4.8 Proces riadenia rizík podľa normy ISO 31000



Slovakia



Identifikácia rizík

- Interné faktory - Aké interné faktory ovplyvnia organizáciu?
- Externé faktory - Aké vonkajšie faktory ovplyvnia organizáciu?

Identifikácia rizík narušenia

k prioritným činnostiam organizácie:

- Procesy
- Systémy
- Informácie
- Ľudia
- Aktíva
- Zadávať externým partnerom
- a ďalšie zdroje, ktoré ich podporujú.



Možnosti zníženia rizika

- Vyvarovanie sa riziku rozhodnutím, nevykonávať činnosti, ktoré vedú k riziku
- Odstránenie zdroja rizika
- Zmena pravdepodobnosti
- Zmena dôsledkov
- Zdieľanie rizika s inou stranou alebo stranami
- Udržanie rizika informovaným rozhodnutím



Každý plán obsahuje :

- Účel a rozsah
- Ciele
- Aktivačné kritériá a postupy
- Podrobný popis činností s definovaným časom
- Úlohy, zodpovednosti a právomoci
- Komunikačné požiadavky
- Vnútorne a vonkajšie vzájomné závislosti a interakcie
- Požiadavky na zdroje



- BCM musí byť neoddeliteľnou súčasťou Manažmentu zmien
- Čo sa zmenilo od poslednej aktualizácie?
- Aký je dopad týchto zmien?
- Aké plány je potrebné aktualizovať? Ako distribuovať novú verziu?



■ Definovanie kríz

- Nedostupná budova
- Nedostupný personál
- Nedostupná služba ICT

■ Personálne zabezpečenie

- BCM Officer
- BCM tím
- Vzdelávanie

■ Návrh plánov obnovy

- Na jednotlivé krízy
- Čo najdetailnejšie
- Presné stanovenie postupností a času

■ Testovanie plánov a optimalizácia

- Funkčnosť plánov
- Kompetencia členov BCT
- Čas

▪ Fluktuácia ľudí

- Plány musia byť dostatočne podrobné a jasné
- Musí byť registrovaný a školený každý člen BCT

▪ Procesné zmeny

- BCO musí byť zahrnutý do riadenia zmien

▪ Technologické zmeny

- BCO musí byť zahrnutý do riadenia zmien

▪ Dodávatelia

▪

- Začleniť „KO“ požiadavku na BCM do **výberu nových dodávateľov**
- **Stanoviť stávajúcim** dodávateľom požiadavku na zabezpečenie BCM procesu

5.1 Benefity z implementácie BCMS



Slovakia

- Vytvára **dôveru** medzi vašimi zákazníkmi.
- Zachováva hodnotu vašej **značky a vašu povesť**.
- Poskytuje **cenné** obchodné **údaje**. (BIA)
- Súlad s **legislatívnymi požiadavkami**
- Pomáha zmierniť vaše **finančné riziko**.
- Chráni váš **dodávateľský reťazec**.
- Poskytuje vám **konkurenčnú výhodu**.



- Spoločnosť : SK NIC – správca DOMÉN NAJVVYŠŠEJ ÚROVNE .sk
- Služba: zabezpečí kontinuitu dodávania služieb a poskytne systém, ktorý podporuje monitorovanie služieb registra a funkcie, ktoré zabezpečia mesačnú správu o úrovni poskytovaných služieb registra vo vzťahu k požadovaným úrovniam služieb.
- Zavedený systém BCMS rok 2018
 - Vypracovanie BCP pre nasledovné krízy
 - Výpadok budovy (open space)
 - Výpadok personálu
 - Výpadok ICT



Vznik krízy

- Krízový manažment vyhlásil stav krízy
- Aplikovanie BCP „Výpadok budovy“
- Do dvoch hodín po vyhlásení spoločnosť poskytuje služby bez obmedzenia

5.3 Čo ponúka TÜV SÜD pre podporu zavádzania BCM



Slovakia

Manažér kontinuity v podnikaní podľa ISO 22301



Manažér riadenie rizík v IT



Interný audítor systémov manažérstva podľa ISO/IEC 27001



Otázky....



**Ďakujem za
pozornosť**

Prípadné ďalšie otázky smerujte
na: igor.straka@tuv-sud.sk



Slovakia

**Choose certainty.
Add value.**