

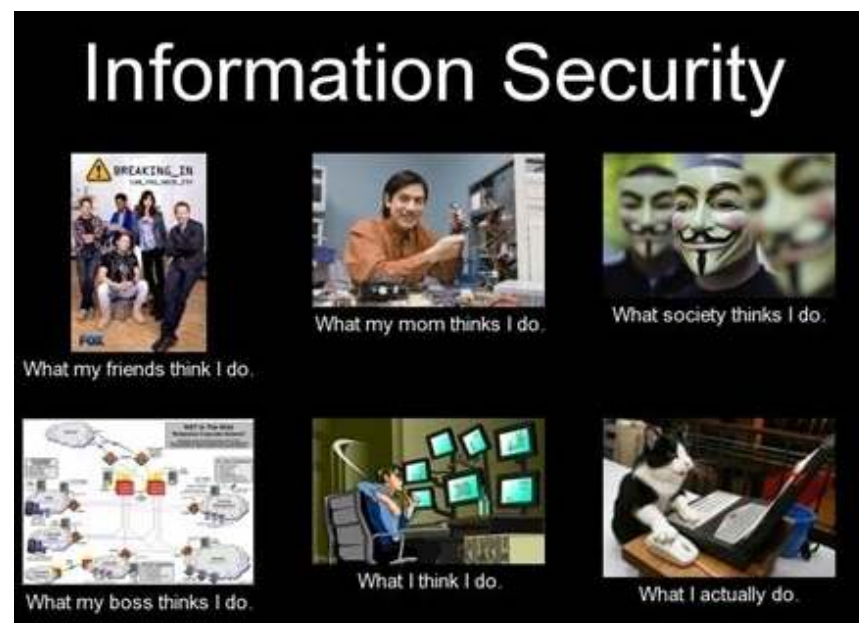
Revidiranje neprekinjenega poslovanja

Matic Štern

Gradivo je last Slovenskega inštituta za revizijo in je predmet avtorske zaščite in drugih oblik zaščite intelektualne lastnine. Prepovedano je kakršnokoli reproduciranje, razen izključno za osebno uporabo in v nekomercialne namene, pri čemer se morajo ohraniti vsa opozorila o avtorskih ali drugih pravicah, zato se ne smejo prepisovati, razmnoževati ali kako drugače razširjati. Naveden mora biti tudi vir.

Kdo sem in kaj počnem?

- Preteklih 6 let **notranji revizor** v Telekomu Slovenije (TS); v timu notranjih revizorjev pretežno izvajam notranje revizije in svetovalne posle, ki so bolj povezani s področjem strategije, upravljanja in varnosti informacijsko-komunikacijskih tehnologij. Kmalu po pridružitvi timu notranjih revizorjev sem pridobil licenco CISA.
- Pred tem sem več kot 10 let delal v IT – od systemske in omrežne administracije, upravljanja baz podatkov, razvoja informacijskih rešitev (še pred prihodom v TS) ter sodeloval pri vodenju večjih IT projektov, predvsem na področju IT analize, testiranja, po-projektne podpore produkciji, vzpostavitvi in izboljšavah nekaterih IT procesov ...
- Rad pridobivam ter delim izkušnje in znanje.



Struktura predstavitve



KAJ – neprekinjeno poslovanje

Neprekinjeno poslovanje je zmožnost / sposobnost organizacije, da nadaljuje z dostavo izdelkov in storitev v sprejemljivih časovnih okvirih z vnaprej določenimi zmogljivostmi med prekinitvijo.

Business Continuity is the capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.

Vir: ISO 22301:2019, poglavje 3 – izrazi in definicije; točka 3.3; Business Continuity.

KAJ – upravljanje neprekinjenega poslovanja

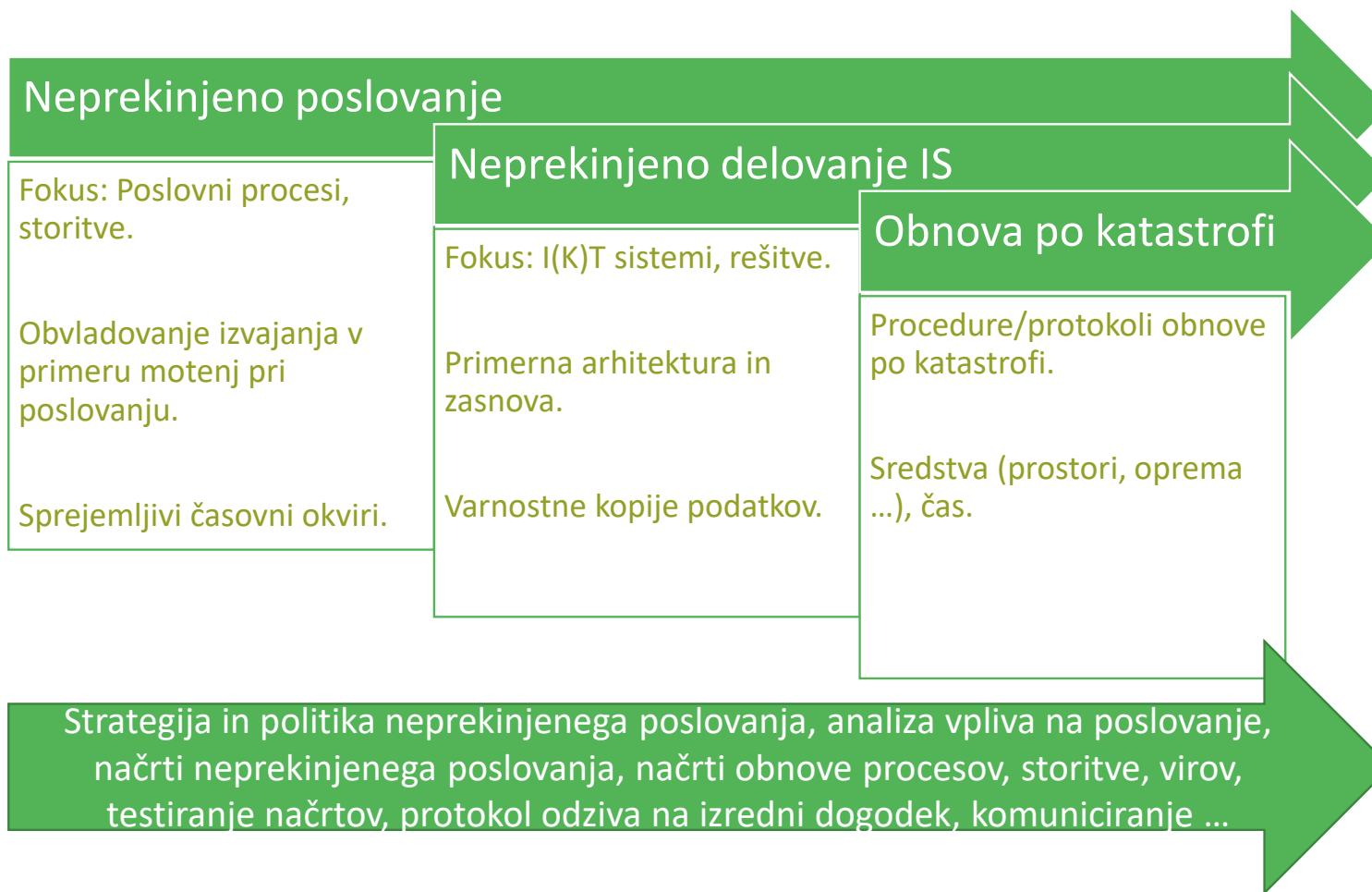
Upravljanje neprekinjenega poslovanja je celovit proces upravljanja, ki opredeljuje morebitne grožnje za organizacijo in vplive na poslovanje organizacije, če bi se te grožnje uresničile. Proces upravljanja zagotavlja okvir za povečanje odpornosti organizacije in zmožnost njenega učinkovitega odziva na grožnje, kar varuje interese ključnih deležnikov, ugled in dejavnosti ustvarjanja vrednosti.

Vir: [Revizijsko poročilo Neprekinjeno poslovanje Lekarne Ljubljana, Računsko sodišče RS](#); str. 10

Business Continuity Management is a Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Vir: [What is Business Continuity Management, DRI International](#).

KAJ – neprekinjeno delovanje IS, obnova poslovanja

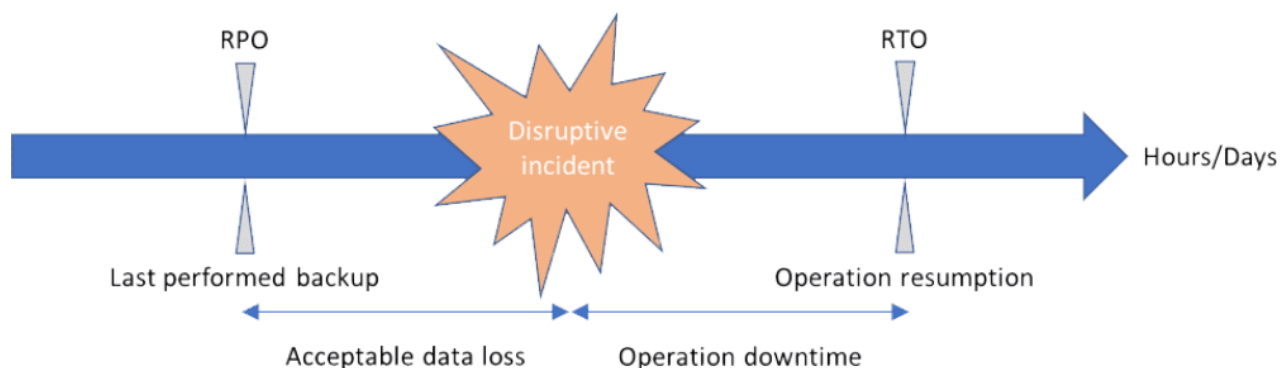


KAJ – sprejemljivi časovni okviri

- Najdaljši sprejemljivi čas prekinitve poslovanja/delovanja (angl. *Recovery Time Objective – RTO*)

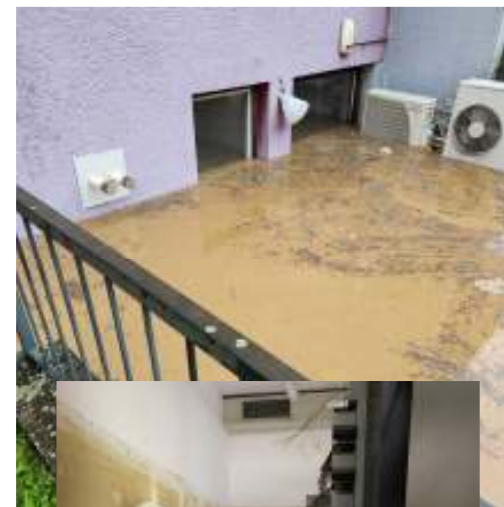
- Največji sprejemljivi izpad podatkov (angl. *Recovery Point Objective – RPO*)

The difference between RTO and RPO



Vir: [What is the difference between RTO and RPO, Advisera.](#)

ZAKAJ – poplave 2023 (Slovenija)



Vir: [Poplave Avgust 2023, gvo.si](https://gvo.si/).

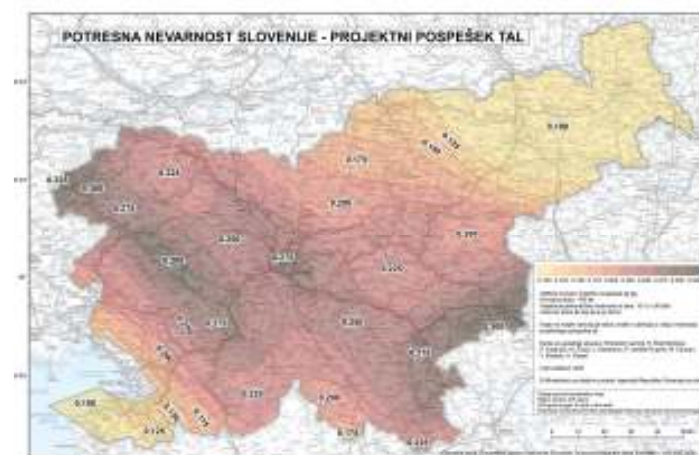
ZAKAJ – potres 2023 (tujina)



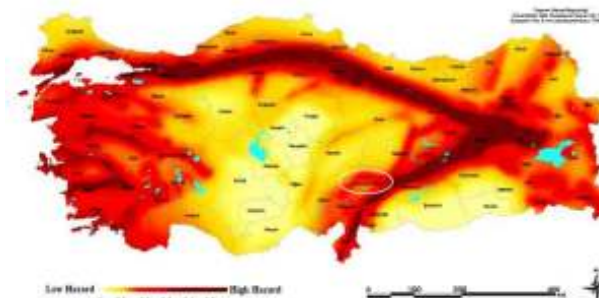
The USGS Prompt Assessment of Global Earthquakes for Response (PAGER) service estimated a 35 percent probability of **economic losses between US\$10 billion and US\$100 billion**. There was a 34 percent probability of **economic losses exceeding US\$100 billion**. The service estimated a 36 percent probability of **deaths between 10,000 and 100,000**; 26 percent probability of deaths exceeding 100,000. For the second large earthquake, there was a 46 percent probability of deaths between 1,000 and 10,000; 30 percent probability of deaths between 100 and 1,000. The service also estimated a 35 percent probability of economic losses between US\$1 billion and US\$10 billion; 27 percent probability of economic losses between US\$10 billion and US\$100 billion

Vir: [2023 Turkey-Syria earthquakes, Wikipedia](#).

Kakšna je nevarnost v Sloveniji?



Vir: [Karta potresne nevarnosti 2021, ARSO](#).



Vir: [Potresi v JV Tručiji 6. 2. 2023 in popotresi, ARSO](#).

ZAKAJ – kibernetiski napadi (tujina, Slovenija)

SolarWinds, ZDA

The [SolarWinds breach](#) is already one of the most significant cybersecurity incidents ever. And as with any unprecedented cyber event, this will have long-term effects on the way businesses and government consider their security programs. While many questions remain unanswered, the SolarWinds impact on the insurance sector has become clearer after an analysis we've completed with one of our partners. So, what should we expect the financial impact of SolarWinds on cyber insurers? And how can cyber insurers quantify a breach of this scale in the future?

Today, Bitsight and Kovit [announced our new partnership](#) and released a joint analysis of the financial impact of the [SolarWinds hack](#) to the insurance industry. We find that although the SolarWinds attack is a cyber catastrophe from a national security perspective, insurers may have narrowly avoided a catastrophic financial incident to their businesses. **We estimate the insured losses to be \$90,000,000**, which includes incident response and forensic services for companies who were impacted by this incident and have cyber insurance coverage.

Vir: [The Financial Impact of SolarWinds Breach, Bitsight, 2021](#).

Colonial Pipeline, ZDA

Looking back at the legacy of the Colonial Pipeline ransomware attack, experts are still unclear on why this was the incident that sparked such a massive sea change across policymaking and boardrooms.

Flashback: This weekend marks [two years since a Russian ransomware gang](#) targeted Colonial's pipeline, which provides roughly 45% of the fuel used on the East Coast.

- The ransomware attack led to a six-day shutdown of the pipeline, [prompting gas shortages](#) and [an emergency declaration](#) in D.C. and 17 states.
- The attack brought ransomware to everyday Americans' attention for the first time, inspired Congress to [pass new laws](#), and prompted [various federal agencies](#) to institute [new cybersecurity requirements](#).

Vir: [Colonial Pipeline ransomware attack's unexpected legacy, Axios, 2023](#).

SLOVENIJA

Direktor: 'vojni napad' lekarne stal več kot dva milijona evrov

Ljubljana, 08.08.2019, 8:31 | Posodobljeno pred 4 leti

PREVIDEN ČAS BRANJA: 3 min



AVTOR
J.M.V. / M.S. / STA



REPORERARJI
24



Lekarna Ljubljana je po treh dneh nedelovanja znova vzpostavila centralni informacijski sistem, vanj pa je že vključenih več lekarn. V drugih enotah trenutno še vedno izdajajo zdravila na papirnat recept, nakup zdravila pa ni mogoč. Po besedah direktorja Marjana Sedeja je nastalo za več kot dva milijona evrov škode.

Vir: [Članek na spletnem portalu 24ur.com, 2019](#).

Napadi na podjetja ne pojenjajo, na udaru so predvsem mala in srednje velika podjetja

Na področju zlonamerne kode so v preteklem letu prednjačili trojanski konji, specializirani za krajo podatkov (shranjena gesla, poverilnice VPN, kriptodenarice itd.), katerih tarča so bila primarno podjetja. Na SI-CERT smo lani obravnavali 278 primerov trojanskih konjev vrste t.i. infostealer, leta 2021 pa 171. Trojanski konji se najpogosteje linijo v obliki **priponk elektronske pošte** s sporočili, ki želijo naslovnika prepričati, da nanjo klikne in s tem nevede v računalnik namesti zlonamerno kodo. Lažna sporočila, tudi s pomočjo orodij umetne inteligence, postajajo čedalje prepričljivejša, z različnimi tehnikami pa tudi preslepajo filtre poštnih strežnikov. Taka lažna sporočila običajno predstavljajo prvi korak pri nepooblaščenem dostopu do omrežja podjetja skozi okužbo računalnika enega od zaposlenih.

Posledica odprtega škodljive priponke je lahko tudi okužba z izsiljevalskim virusom, pri čemer so podjetja bolj izpostavljena kot posamezniki. Po podatkih SI-CERT je v preteklem letu bil v 78 % vseh obravnavanih incidentih z izsiljevalskimi virusi tarča napada poslovni subjekt.

Vrivanje v poslovno komunikacijo (ang. BEC, business email compromise) je enostavna, a izredno škodljiva oblika kibernetiskega napada, ki prav tako cilja na podjetja. Z vdorom v poštni predal napadaci spreminjajo komunikacijo v podjetju in ob pošiljanju fakture v njej zamenjajo podatek o bančnem računu in tako preusmerijo nakazila denarja. Zneski oškodovanja so praviloma zelo visoki. Najvišji zabeleženi znesek preusmerjenega nakazila v letu 2022 iz kategorije napadov BEC je bil 3.000.000 evrov. Na srečo je bil prenos denarja zaradi nadzornih mehanizmov bank in Urada RS za preprečevanje pranja denarja pravočasno zaustavljen.

Vir: [Poročilo o kibernetiski varnosti za leto 2022, SI-CERT](#).

The total amount of direct damage to Ukraine's infrastructure caused due to the war as of June 2023 exceeded \$150 billion

🕒 2 August 2023

Total estimate of infrastructure damage by industry
in monetary terms, as of June 2023

Property type	Damage, \$ billion
Housing	55,9
Infrastructure	36,6
Assets of enterprises, industry	11,4
Education	9,7
Energy	8,8
Agriculture and land resources	8,7
Forests	4,5
Transport	3,1
Healthcare	2,8
Utilities	2,7
Trade	2,6
Culture, sport, tourism	2,4
Administrative buildings	0,5
Digital infrastructure	0,5
Social sphere	0,2
Total	150,5

Vir: [The total amount of direct damage to UKR infrastructure caused due to the war exceeded \\$150 billion, Kyiv School of Economics, 2023.](#)

ZAKAJ – požar (tujina, Slovenija)

What was the Possible Cause of the OVHcloud Data Centre Fire in 2021?



In late May, France's Bureau of Investigation and Analysis on Industrial risks (BEA-Ri) issued its technical report on the March 10, 2021 fire at the OVH data centre in Strasbourg. Although all staff were fortunately unharmed and evacuated safely, the fire destroyed SBG2, a five-storey data centre occupying 500m², and damaged servers in adjacent buildings.

In September 2021, Parisian law firm Ziegler & Associates began adding clients who had lost data due to the fire, to their firm's roster. Over 140 customers filed a class-action lawsuit, intending to seek damages for their losses. In sum, OVHcloud is being pursued for more than €10 million in compensation from the law firm's clients. Ziegler & Associates is also preparing formal notices to OVHcloud asking OVH for damages that companies are entitled to claim, and expects that it will finish sending out letters on behalf of all its clients by the end of June 2022.

Vir: [What was the possible cause of the OVHCloud DC fire in 2021, W.media.](#)

Požar na Krasu, 2022



Vir: [Članek na spletnem portalu Dnevnik.si.](#)



Vir: Interna gradiva, Telekom Slovenije.

ZAKAJ – žled 2014 (Slovenija)



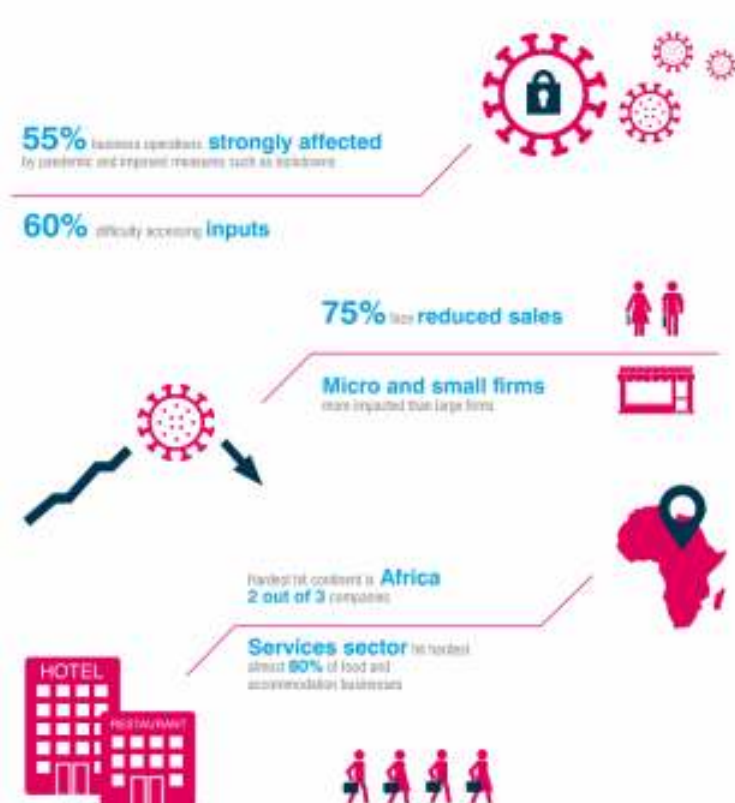
Vir: [Žled 2014, fotogalerija, Laboratorij za preskrbo z elektr. energijo FTE ULJ.](#)



Vir: [Objava Facebook, Telekom Slovenije.](#)

ZAKAJ – pandemija 2020-2022 (tujina, Slovenija)

COVID-19 impact on business



Vir: [COVID-19 impact on business, UN, 2021.](#)

Aktivnosti Telekom Slovenije, d.d., v povezavi z epidemijo koronavirusa

17.3.2020

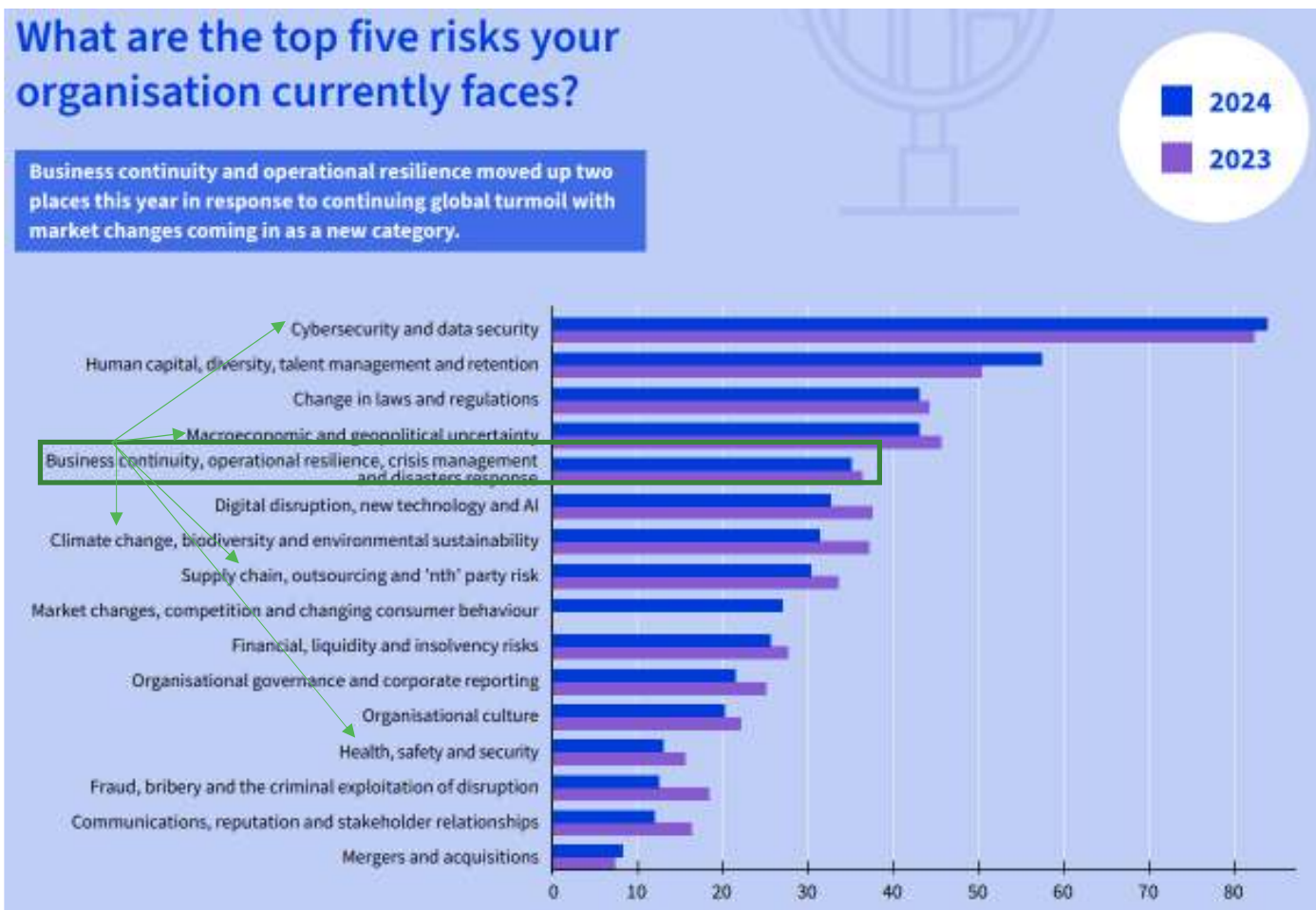
V Telekomu Slovenije, d.d., smo po tem, ko se je koronavirus COVID-19 pričel širiti v Evropi, na podlagi Sistema upravljanja neprekinjenega poslovanja (SUNP), ki ga imamo vzpostavljenega za primer izrednih dogodkov in ki je certificiran po standardu ISO/IEC 22301, pričeli s pripravo aktivnosti in sprejemom prvih preventivnih ukrepov.

Vir: [Objava ukrepov ob začetku pandemije Covid-19, Telekom Slovenije.](#)



Vir: [COVID-19 Cyberthreats, Interpol.](#)

ZAKAJ – trendi globalnih tveganj



Vir: [2024 Risk in focus, ECIA](#).

ZAKAJ – trendi globalnih tveganj



Vir: [Allianz Risk Barometer 2023, Allianz](#).

ZAKAJ – predpisi

ZAKON O INFORMACIJSKI VARNOSTI (ZInfV)

III. Informacijska varnost izvajalcev bistvenih storitev

11. člen

(varnostne zahteve)

(1) Izvajalci bistvenih storitev skladno z metodologijo iz tretjega odstavka 12. člena tega zakona, določijo svoje ključne, krmilne in nadzorne informacijske sisteme ter dele omrežja, s katerimi zagotavljajo izvajanje bistvenih storitev.

(2) Izvajalci bistvenih storitev izvedejo analizo, oceno in vrednotenje tveganj ter na tej osnovi pripravijo in izvedejo potrebne ukrepe za obvladovanje tveganj glede varnosti omrežij in informacijskih sistemov, ki jih uporabljajo pri bistvenih storitvah.

(3) Izvajalci bistvenih storitev sprejmejo ustrezne ukrepe za preprečitev in zmanjšanje vpliva incidentov, ki vplivajo na varnost tistih omrežij in informacijskih sistemov, ki se uporabljajo za zagotavljanje bistvenih storitev, **da bi zagotovili neprekinjeno izvajanje teh storitev.**

SMERNICE EBA O UPRAVLJANJU TVEGANJ, POVEZANIH Z IKT VARNOSTJO

1.7. Upravljanje neprekinjenega poslovanja

77. Finančne institucije bi morale vzpostaviti trden proces upravljanja neprekinjenega poslovanja, s čimer bi maksimalno povečale zmožnost zagotavljanja neprekinjenega poslovanja in omejile izgubo v primeru resne motnje poslovanja v skladu s členom 85(2) Direktive 2013/36/EU in naslovom VI Smernic organa EBA o notranjem upravljanju (EBA/GL/2017/11).

ZAKON O ELEKTRONSKIH KOMUNIKACIJAH (ZEKom-2)

124. člen

(**upravljanje neprekinjenega poslovanja** za primer stanj ogroženosti)

(1) Operaterji morajo za primer stanj ogroženosti sami, oziroma kadar to ocenijo za primerno, tudi z drugimi operaterji, **vzpostaviti, dokumentirati, izvajati in vzdrževati procese, postopke in kontrole za zagotavljanje SUNP, vključno z zagotavljanjem nadomestnih poti.** Navedeno še posebej velja za tiste dele omrežja, storitev in povezav, ki so nujni za nemoteno delovanje omrežij ključnih delov sistema varnosti države in komunikacij v sili ter za podporo delovanju kritične infrastrukture, izvajalcem bistvenih storitev ter organom državne uprave.

(2) Operaterji morajo vzpostaviti in vzdrževati ustrezne zmogljivosti, ukrepe in dogovore z drugimi operaterji, ki zagotavljajo hitro okrevanje omrežja in obnovo storitev iz prejšnjega odstavka v primeru katastrofalnega izpada ali ob naravnih in drugih nesrečah.

(3) Operaterji morajo ob upoštevanju sprememb in predhodnih negativnih dogodkov neprestano izvajati in spremljati ter redno izboljševati ukrepe, načrte in zmogljivosti za zagotavljanje SUNP iz prvega odstavka tega člena.

(4) V delu, kjer se SUNP iz prvega odstavka tega člena nanaša na zagotavljanje komunikacije v sili, se uporablja določba petega odstavka 115. člena tega zakona.

ZAKON O KRITIČNI INFRASTRUKTURI

19. člen (upravljalci kritične infrastrukture)

(1) **Upravljalci kritične infrastrukture zagotavljajo neprekinjeno delovanje kritične infrastrukture.**

(2) Upravljalci kritične infrastrukture določijo kontaktno osebo ali več takih oseb za sodelovanje na področju kritične infrastrukture z drugimi upravljalci kritične infrastrukture, nosilci sektorjev kritične infrastrukture in ministrstvom.

KAKO – namen in cilji

Podati zagotovilo o **skladnosti** s predpisi / standardi.

Telekom Slovenije prvi v Sloveniji prejel certifikat ISO 22301 za sistem upravljanja neprekinjenega poslovanja



Ljubljana, 2. junij - Telekom Slovenije je kot prva družba v Sloveniji prejel mednarodni certifikat ISO 22301:2012. Certifikat ISO 22301:2012 predstavlja mednarodni standard, s katerim podjetje izkazuje zanesljivo delovanje storitev in procesov ter hiter in učinkovit odziv ob izrednem dogodku, kar pomeni tudi manjše tveganje za daljši izpad storitev in procesov. Certifikat je družbi po temeljiti presoji podelil Slovenski inštitut za kakovost in meroslovje.

Vir: [Telekom Slovenije prvi v Sloveniji prejel certifikat ISO 22301 za SUNP, STA, 2016.](#)

Podati zagotovilo, da UNP v organizaciji pripomore k **uspešnosti in učinkovitosti doseganja strateških ciljev in obvladovanju tveganj varovanja premoženja** organizacije.



KAKO – možna sodila in orodja/okviri

ISO 22301:2019

Security and resilience

Business continuity management systems

Requirements

Vir: [ISO 22301:2019 - Security and resilience — Business continuity management systems](#).

Global Technology Audit Guide (GTAG) 10: Business Continuity Management

Vir: [Global Technology Audit Guide \(GTAG\) 10: Business Continuity Management \(theiia.org\)](#).

Domain: Deliver, Service and Support	
Management Objective: DSS04 - Managed Continuity	
Focus Area: COBIT Core Model	
Description	
Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise.	
Purpose	
Adapt rapidly, continue business operations and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).	

Vir: [COBIT 2019 Framework: Governance and Management Objectives, Isaca](#).



Vir: [IT BC Audit Program, Isaca](#).

KAKO – temeljna revizijska vprašanja (1/4)

Strategija, politika in predpisi neprekinjenega poslovanja

- Ali je poslovodstvo neprekinjeno poslovanje vključilo v strategijo organizacije?
- Ali ima organizacija sprejeto politiko z vsemi ključnimi načeli in izhodišči za zagotavljanje neprekinjenega poslovanja (namen in cilj, podlage ...)?
- Ali so v internih predpisih vzpostavljene aktivnosti, viri, vloge, odgovornosti in pooblastila za področje UNP, ki zajemajo celotno organizacijo?

Obseg

- Sorazmerno s kompleksnostjo poslovnega modela in poslovnih procesov organizacije je potrebno redno presoјati obseg procesov in storitev, ki so del UNP.
- Ali so popisane storitve in procesi organizacije, ki so pomembne za doseganje strateških ciljev?
- Ali se izvaja analiza vpliva na poslovanje (ocena tveganj), kjer so upoštevani razni scenariji potencialnih prekinitev poslovanja?
- Ali so procesi in storitve na podlagi analize vpliva na poslovanje ustrezno rangirani po pomembnosti in zastopani v obsegu UNP?

Struktura/gradniki UNP

- Ali je vzpostavljen protokol obravnave izrednega dogodka?
- Ali so (formalno) določene ključne kontaktne osebe? So informacije ažurne?
- Ali je določen protokol komuniciranja v primeru izrednega dogodka?
- Ali so vzpostavljeni in vzdrževani (dokumentirani) načrti okrevanja procesov/storitev/virov?



KAKO – temeljna revizijska vprašanja (2/4)

Načrti okrevanja procesov in storitev

- Ali imajo procesi in storitve (formalno) določene vsebinske/poslovne in tehnične skrbnike?
- Ali so v načrtih okrevanja procesov in storitev identificirani ustrezni ključni viri za izvajanje teh procesov in storitev ter vrstni red njihovega okrevanja?
- Ali je izvedena analiza vpliva na poslovanje za ključne scenarije?
- Ali so za procese in storitve določeni ključni parametri glede na strateške cilje organizacije, kot so maksimalni čas prekinitve delovanja (RTO), maksimalna izguba podatkov (RPO)?



Načrti okrevanja virov

- Protokole okrevanja virov je potrebno preveriti tako z vidika *bistvenih sestavnih delov* (skrbnik vira, opis vzpostavitve vira – arhitektura, seznam ključnih procesov in storitev, ki jih vir podpira, lokacija, morebitni rezervni deli, lokacije varnostnih kopij ...) kot z vidika *zadostnosti protokola* ponovne vzpostavitve delovanja vira.
- Na kakovost načrtov okrevanja vira vpliva več dejavnikov, kot so nadgradnje, menjava infrastrukture, spremembe omrežnih povezav, spremembe lokacij. Če je dinamika sprememb pri načrtih okrevanja procesov in storitev še zmerna, je pri informacijskih virih visoka.



Varnostno kopiranje

- Ali so urniki varnostnega kopiranja skladni z definiranimi RPO?
- Ali so varnostne kopije ustrezno zaščitene (npr. šifriranje, omejitev dostopov)?
- Ali se izvaja ustrezna hramba varnostnih kopij (npr. ustrezen medij, lokacija, zaščita, ločena omrežja)?
- Ali so kapacitete rešitev za varnostno kopiranje zadostne?
- Ali se izvaja preverjanje uspešnosti in učinkovitosti restavracije podatkov iz varnostne kopije?



KAKO – temeljna revizijska vprašanja (3/4)

Alternativne lokacije

- Ali so določene sekundarne / alternativne lokacije za izvajanje kateregakoli procesa (npr. proizvodnje, prodaje, poslovne podpore ...) ter rezervne lokacije informacijskih virov (sistemski prostori)?
- Ali alternativne lokacije zagotavljajo zadostno zmogljivost v primeru prenosa aktivnosti in virov?
- Ali so lokacije ustrezne (npr. zadostna geografska razdalja, opremljenost, pripravljenost)?

TESTIRANJE NAČRTOV NEPREKINJENEGA POSLOVANJA

- Ali se redno izvajajo zadostna testiranja načrtov neprekinjenega poslovanja? Ali so vključeni scenariji testiranja, ki ponazarjajo dejansko možno stanje izrednega dogodka?
- Ali so vključeni vsi potrebni udeleženci testiranj (tudi tretje osebe/zunanji izvajalci)?
- Ali se za testiranja pripravi dokumentirano poročilo ter predvidi ukrepe v primeru ugotovitve pomanjkljivosti?



Usposabljanje in ozaveščanje

- Ali imajo vsi deležniki UNP zadostno poznavanje in veščine obvladovanja UNP?
- Ali so znani in jasno predstavljeni komunikacijski kanali in vzводи za prijavo motenj pri poslovanju ter kriteriji za aktiviranje skupine, ki prevzame upravljanje in odločanje v primeru izrednega dogodka?
- Ali so vsem deležnikom UNP (vsebinski/poslovni skrbniki procesov in storitev, skrbniki virov, člani skupine za koordinacijo v primeru izrednega dogodka, ipd.) jasne njihove naloge in odgovornosti in se za to redno usposabljujejo?

KAKO – temeljna revizijska vprašanja (4/4)

Obravnava izrednih dogodkov

- Ali so vzpostavljeni kriteriji za opredelitev izrednega dogodka?
- Ali je vzpostavljen protokol ukrepanja v primeru izrednega dogodka?
- Ali se koordinacija in ukrepi v primeru izrednega dogodka primerno dokumentirajo?
- Ali iz obravnave izrednih dogodkov izhajajo morebitni ukrepi za izboljšave?

Spremljanje in izboljševanje UNP

- Ali se za uspešnost in učinkovitost UNP izvajajo redne presoje in revizije?
- Ali se priporočila za izboljšave strukturirano implementirajo ter se njihova implementacija spremlja in poroča?
- Ali je UNP področje certificirano?



Vir: [The importance of Disaster Recovery and Business Continuity, LinkedIn](#).



KAKO – možni pristopi

Področje upravljanja neprekinjenega poslovanja je kompleksno, široko in tvegano – vključitev notranje revizije UNP v letni načrt.

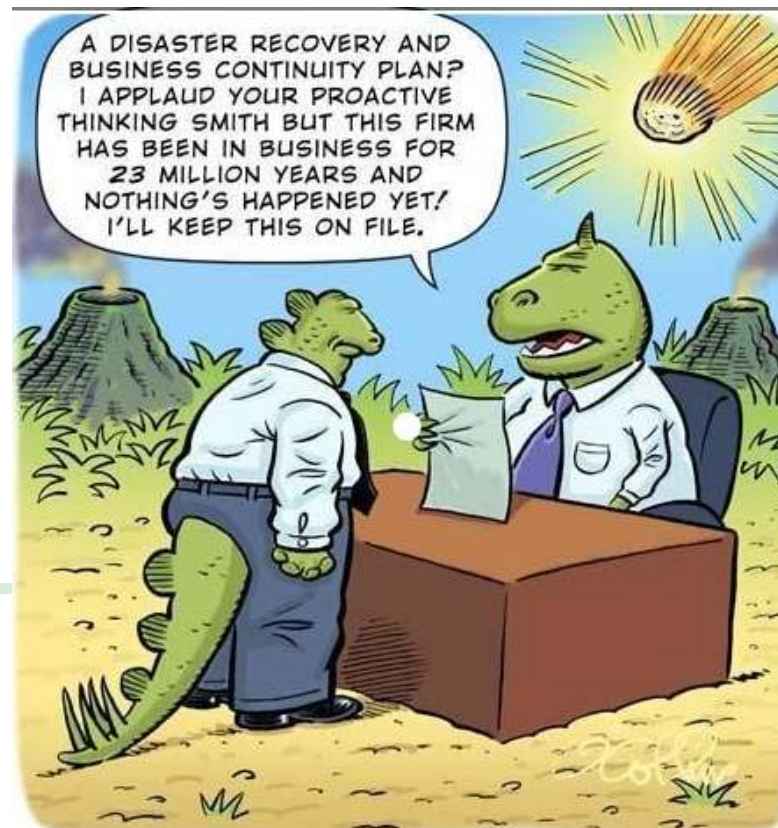
Pri pregledu *načrtov okrevanja virov* in *varnostnega kopiranja* je smiselno sodelovanje revizorja, katerega glavna naloga je revidiranje IT, oz. presoditi soizvajanje z zunanjim strokovnjakom na tem področju.

- Področje UNP v celotnem obsegu.
- Izvedba po delih področja UNP (npr. „varnostno kopiranje“ kot samostojna notranja revizija).
- Vključitev delov področja UNP v posamezni notranji reviziji določenega področja ali procesa, kjer je med ključnimi tveganji tudi UNP.



"Remember: When disaster strikes,
the time to prepare has passed"

- Stephen Cyros



Vir: [Disaster Recovery and Business Continuity – Are You Ready?, Silexsys.](#)

Hvala za pozornost!

