



UMJETNA INTELIGENCIJA

u reviziji i upravljanju
kibernetičkom sigurnošću

Koliko joj možemo vjerovati?

AI vs

OD ODGOVORA
DO DOKAZA.

AI

OD RIZIKA
DO UPRAVLJANJA.

22. 9. 2026.
Hotel Antunović, Zagreb

15+ godina iskustva u kibernetičkoj sigurnosti

Globalno iskustvo. Dokazani rezultati.



15+

godina na tržištu



90%+

klijenata na najrazvijenijim
svjetskim tržištima



Savjetovanje i revizija

u upravljanju rizikom
kibernetičke sigurnosti i usklađenosti

POVJERENJE SU NAM UKAZALI

AMGEN®

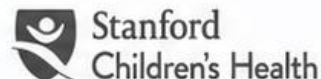
MERCK



Fina

BBCNBank®

Zillow®



nanobit



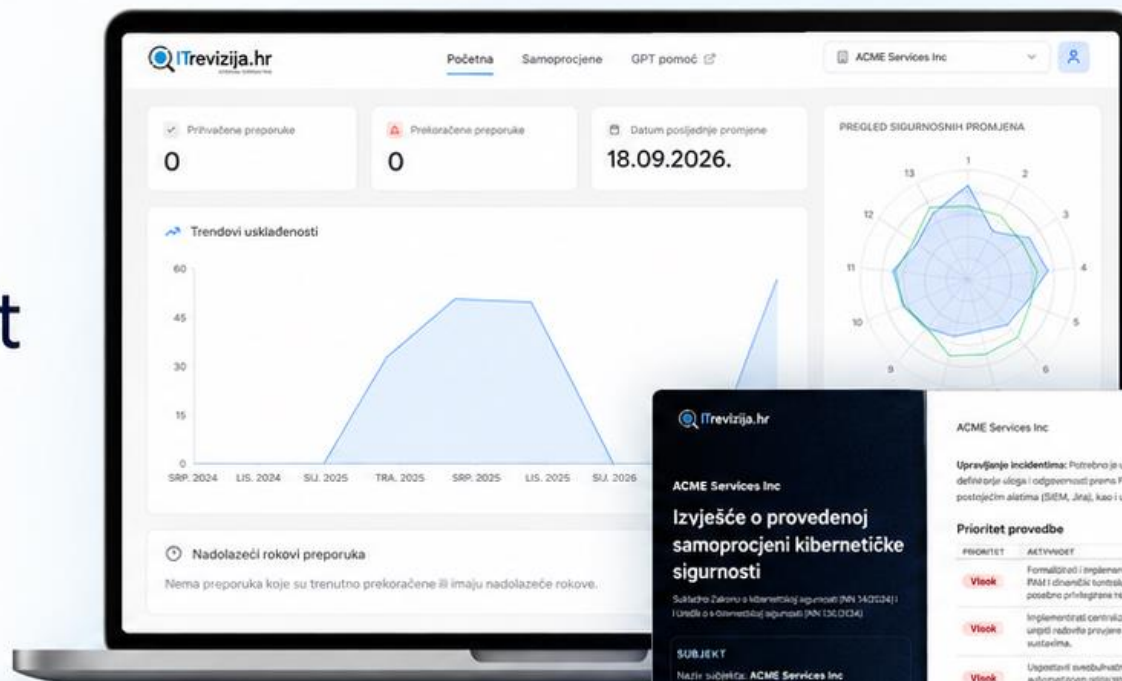
zappi

ENGLISH
HERITAGE

RAZLIČITA INDUSTRIJA. ISTI STANDARDI.
VEĆA OTPORNOST.

AI platforma za usklađenost u području kibernetičke sigurnosti u Hrvatskoj.

Od procjene do konkretnog plana.



2024.
Razvoj započeo krajem 2024.

Razvijena u Hrvatskoj
za potrebe upravljanja kibernetičkom sigurnošću i usklađenošću

SRCE
Prvi put javno predstavljena na Danu Hrvatskog centra kompetencija za HPC

ACME Services Inc		
Izvjeshće o provedenoj samoprocjeni kibernetičke sigurnosti		
Sukladno Zakonu o kibernetičkoj sigurnosti (ZKIS) i Uredbi o sigurnosti informacija (NIS 2) i Uredbi o sigurnosti informacija (NIS 2) i Uredbi o sigurnosti informacija (NIS 2)		
SUBJEKT		
Naziv subjekta: ACME Services Inc Razina mjere: SRCE OIB subjekta: 27718234025 Adresa subjekta: Acme Street 555, 10000, Zagreb Broj mobitela: +385995555555		
Klasifikacija izvješća: Povjerljivo Period revizije: 01.06.2025. - 18.09.2026. Datum izdavanja: 18.09.2026. 18:08:51		
Prioritet provedbe		
PRIORITET	AKTIVNOST	OČEKIVANI UČINAK
Visok	Formalizirati i implementirati cjeloviti IAM sustav uključujući PAM i dinamički pristupni pristup za sve kritične sustave, posebno privilegirane račune.	Značajno smanjenje rizika od neovlaštenog pristupa i zloupotrebe identiteta u produžetom ciklusu.
Visok	Implementirati centralizirani SIEM sustav za nadzor logova i upori radovima provjere ranojosti na svim ključnim sustavima.	Poboljšano otkrivanje i odgovor na sigurnosne incidente u stvarnom vremenu.
Visok	Uspostaviti sveobuhvatnu politiku kriptografije i automatskom osiguravanjem sigurnosti ključnim sustavima (PostgreSQL, objektivno pohrana).	Zaštita osjetljivih podataka od neovlaštenog pristupa i prijenosa za kriptiranje prijenosa.
Visok	Uspostaviti cjeloviti sustav upravljanja incidentima (klasifikacija, PIR, model, automatizirana trijaža, integracija s SIEM-om).	Struktuiran i učinkovit odgovor na sigurnosne incidente minimalnim vremenom oporavka.
Visok	Račviti, dokumentirati i testirati planove kontinuiteta poslovanja (BCP) i oporavka od katastrofe (DRP) za ključnu infrastrukturu.	Osiguravanje kontinuiteta poslovanja i minimaliziranje pretrnutih usluga u slučaju katastrofe.
Srednji	Provesti očitovnu procjenu rizika za fizičke prijetnje kritične imovine (JAKS, uređaji u Zagrebu i Splitu) i uspostaviti centralizirani inventar imovina.	Identifikacija i mitigacija fizičkih rizika koji uprožavaju poslovni kontinuitet.
Srednji	Formalizirati upravljanje digitalnim identitetima i preima pristupa (političke, procesi odobrenja, periodične revizije).	Smanjenje rizika od neovlaštenog pristupa i poboljšano upravljanje korisničkim identitetima.
Srednji	Implementirati politiku mrežne sigurnosti, segmentaciju mreže i kontrole pristupa (MAC, 802.1X).	Ograničavanje širenja napadača i zaštita mrežnih resursa.
Srednji	Uspostaviti sveobuhvatnu okvir za sigurnost lanca opskrbe (političke, registar dobavljača, ugovorne klauzule, planovi odgovora na incidente).	Smanjenje rizika povezanih s trećim stranama i osiguravanje sigurnosti opskrbe.
Srednji	Uspostaviti formalni okvir sigurnog razvoja (secure by design, zero trust, kontrolni prihvaćanja sustava, sigurnost sekcije).	Integracija sigurnosti i razvojne procese i smanjenje ranjivosti i aplikacija.
Srednji	Izraditi i usvojiti Politiku fizičke sigurnosti te provesti procjenu rizika za uređ u Zagrebu i Splitu.	Zaštita fizičke imovine i zaposlenika od potencijalnih prijetnji.
Nizak	Uspostaviti sveobuhvatni sustav upravljanja informacijom imovinom (političke, popis, klasifikacija, automatizirana provjera prijenosnih medija).	Poboljšano praćenje i zaštita imovine te smanjenje rizika od gubitka i zloupotrebe.
Nizak	Ažurirati program edukacije o kibernetičkoj sigurnosti (specifični rizici za SaaS platformu, testiranje socijalnog inženjeringa).	Povećana svjest zaposlenika o sigurnosti prijenosnih kanala.
Nizak	Nadograditi alate za upravljanje rizicima (SIEM, alat za ranjivosti) i formalizirati dokumentaciju (koncepte, registar rizika).	Poboljšano upravljanje rizicima i učinkovita praćenje sigurnosnih prijetnji.
Nizak	Osigurati uniformnu sinkronizaciju vremena na svim ključnim sustavima.	Doverljive evidencije događaja i olakšano forenzičko istraživanje.

Agenda

- 9:30 • **Registracija - kava**
- 10:00 • **Kuda ide EU regulativa**
- **AI podržano upravljanje rizikom i usklađenošću**
 - Što i kako može ChatGPT
 - Kako to radi ITrevizija.hr
- **Što slijedi?**
 - From AI assisted to AI driven
- 10:45 • **Druženje – brunch**
- 11:30 • **Rezultati ankete i proglašenje pobjednika**



“Advanced AI-enabled cyber capabilities could in the near future be **weaponised** against our **critical infrastructure** and our society.””

Source: Action Plan on Cybersecurity and Artificial Intelligence
European Commission, 24 January 2024

A SAFER, MORE RESILIENT EUROPE.
THROUGH TRUSTWORTHY AI.



AI prijetnje traže AI podržano upravljanje rizicima.

AI može povezati informacije o organizaciji, imovini, ranjivostima, prijetnjama i poslovnom utjecaju — i pretvoriti ih u konkretne scenarije rizika.



ŠIRI KONTEKST

Povezuje interne i vanjske izvore znanja.



KONKRETNI SCENARIJI

Od podataka do realnih rizika.



BOLJE ODLUKE

Prioritizacija i planiranje mjera uz podršku AI-ja.

OD SLOŽENOSTI DO JASNOĆE.
UPRAVLJAJ RIZICIMA U AI DOBI.

PEOPLE
PROCESS
TECHNOLOGY
RESILIENCE

ISTI
RIZICI.
NOVA
STVARNOST.

Trevizija.hr Početna Samoprocjene Scenariji Izveštaji ACME Services Inc. [+ Generiraj scenarij uz AI](#)

Scenariji rizika

Od podataka do poslovnog utjecaja.

Svi **Visok rizik** Srednji Nizak

!	Kompromitiran korisnički račun developera Neovlašteni pristup, izmjena koda, utjecaj na proizvodnju	Visok	Tehnologija, Ljudi	12. 09. 2026.
!	Curenje osjetljivih podataka putem AI alata Neovlašćeno unošenje podataka u javne AI servise	Visok	Procesi, Ljudi	05. 09. 2026.
📦	Poremećaj u lancu dobave (dobavljač) Sigurnosni incident kod ključnog dobavljača	Srednji	Dobavljači, Procesi	28. 08. 2026.
📄	Nedostupnost ključne usluge u oblaku Poremećaj poslovanja i regulatorne posljedice	Srednji	Tehnologija, Procesi	18. 08. 2026.
👤	Zloupotreba ovlasti od strane zaposlenika Neovlašćeni pristup osjetljivim podacima	Nizak	Ljudi, Procesi	10. 08. 2026.

EVIDENCE
OVER
OPINION.

RISK MANAGEMENT

NIS2

AI GOVERNANCE

AI-supported
risk management
is something that needs
to be built **piece by piece.**



McLaren

SOME ASSEMBLY
REQUIRED:

- ☐ DOWNLOAD
- ☐ PROMPT
- ☐ ITERATE
- ☐ IMPROVE
- ☐ RACE?

Just a few
pieces...
This should
be easy!



ChatGPT



Gemini



Copilot

How do I build a McLaren F1
from Lego?



IDEAS
PROMPTS
RESULTS
...?

Good
prompts
build
great
things!

- **ChatGPT - basic**
- Pitanja i odgovori
- Znanje dolazi od utreniranog LLM-a i pristupa internetu
- Moguća je analiza pojedinačnih ili manjih skupina dokumenata
- Rezultati su solidni

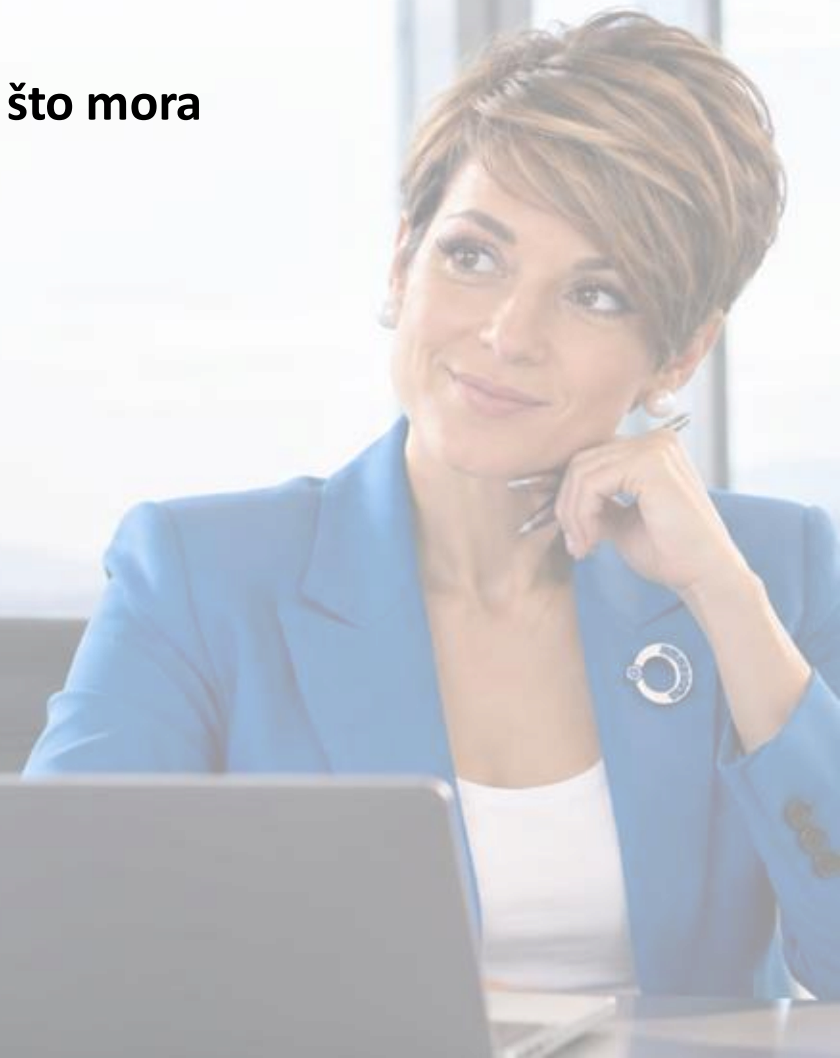


Primjer upita - ChatGPT

ACME d.o.o., Split — B2B SaaS tvrtka. Razvija cloud aplikaciju za europske korisnike. Aplikacija je u AWS-u, development koristi GitHub, Jira i Confluence, zaposlenici Google Workspace. Produkcija sadrži podatke korisnika.

Je li ACME usklađen sa zahtjevima Zakona o kibernetičkoj sigurnosti i što mora napraviti da bi se uskladio?

- **Već ima ISO 27001 što je dobar pokazatelj**
- **Implementacija 10 osnovnih mjera** (Politike analize rizika, Rješavanje incidenata, Kontinuitet poslovanja, Sigurnost lanca opskrbe, Sigurnost u nabavi, Politike i postupci za procjenu učinkovitosti mjera, Kriptografija, Sigurnost ljudskih potencijala,, Upotreba višefaktorske autentifikacije (MFA))
- **Uspostava sustava za prijavu incidenata bez odgode**
- **Edukacija i osobna odgovornost Uprave**





- **CustomGPT** (Običan AI chat +)
- "Učenje" na temelju ograničenog seta učitanih dokumenata
- Ograničeno podešavanje parametara LLM-a
- Mogućnost objavljivanja



Primjer upita - CustomGPT

ACME d.o.o., Split — B2B SaaS tvrtka. Razvija cloud aplikaciju za europske korisnike. Aplikacija je u AWS-u, development koristi GitHub, Jira i Confluence, zaposlenici Google Workspace. Produkcija sadrži podatke korisnika.

Je li ACME usklađen sa zahtjevima Zakona o kibernetičkoj sigurnosti i što mora napraviti da bi se uskladio?

- **Predanost i odgovornost osoba odgovornih za provedbu mjera**
- **Upravljanje programskom sklopovskom imovinom**
- **Upravljanje rizicima**

SOC 2 pokazuje sigurnosne politike, definirane odgovornosti, management oversight, godišnje preglede i risk management.

Formalizirati governance prema zahtjevima 1.1–1.11; usvojiti strateški akt; imenovati odgovornu osobu; uvesti formalni godišnji management report i KPI/KRI



- **MCP integracija** Custom chat +
 - Sharepoint integracija
 - Confluence integracija
 - Jira integracija
 - Google drive integracija
 - Slack integracija
 - Sentry integracija
 - ...



Koliko je to posla? Gotovo ništa.

Nekoliko klikova za svakog klijenta.
Bez razvoja. Bez integracije.

1 Napravite projekt za klijenta

Odvojen kontekst za svakog klijenta.

1 Projects

Kliknite na "New project".



Explore GPTs

Projects

+ New project

ACME

Client X

Internal

... See more

2 Naziv projekta

Upišite naziv klijenta.

Create project

ITrevizija Zagrebački holding

Homework

Writing

Health

Create project

More options

3 Project-only

Odaberite "Project-only".

Project settings

Memory

Default

Project can access memories from outside chats, and vice versa.

Project-only

Project can only access its own memories. Its memories are hidden from outside chats.

Cancel

Done

2 Povežite druge alate (MCP)

Dodajte izvore podataka iz vaših sustava.

1 Sources

Kliknite na "Sources".

Chats

Sources



Give ChatGPT more context

Upload Sources, link drives, or connect apps like Slack to give ChatGPT deeper context about your project.

Add

2 Odaberite alat

Povežite željene izvore.

Add sources

Google Drive

Microsoft OneDrive

SharePoint

Slack

GitHub

Confluence

Connect more apps



To je to.

ChatGPT sada ima odvojeni projekt i može koristiti podatke iz vaših sustava.
Nekoliko klikova. Stvarni ChatGPT. Bez razvoja. Bez integracije.

Impresivno. Ali možete li vjerovati rezultatu?

AI može analizirati vašu dokumentaciju u nekoliko sekundi.
Rezultat izgleda odlično. No je li zaista pouzdan?



ChatGPT

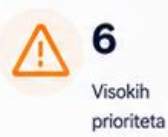
ACME – ZKS analiza ▾

23. rujna 2026. 10:24



Analiza usklađenosti sa Zakonom o kibernetičkoj sigurnosti

Na temelju dostavljenih dokumenata, sustava i procesa



Ključni nalazi



Nedovoljno definirane uloge i odgovornosti u upravljanju kibernetičkom sigurnošću
Nisu jasno dokumentirane odgovornosti za provedbu mjera.



Nema formaliziranog procesa upravljanja rizicima za dobavljače
Postupak procjene i kontinuiranog nadzora rizika dobavljača nije u potpunosti uspostavljen.



Neprovođe se redovito vježbe oporavka od kibernetičkih incidenata
Planovi postoje, ali nema evidencije o testiranjima.



Djelomično implementirana višefaktorska autentifikacija (MFA)
MFA je implementiran za ključne sustave, ali ne za sve korisničke skupine.

[Prikaži sve nalaze...](#)

 Sources

01



Je li analiza kompletna?

Kako znate da je obuhvatila sve relevantne zahtjeve, kontrole, sustave i dokaze?

02



Jesu li činjenice točne i aktualne?

Što ako su dokumenti, Jira zadaci ili tehnički podaci zastarjeli, nepotpuni ili ne odražavaju stvarno stanje?

03



Kako rješava kontradikcije?

Što kada se informacije iz različitih izvora ne podudaraju? Koju verziju uzima kao istinu?

04



Možete li rezultat ponoviti i dokazati?

Hoćete li sutra, s istim podacima, dobiti isti rezultat? Možete li lako rekonstruirati kako je nastao svaki zaključak?



Rezultat izgleda uvjerljivo.
Ali uvjerljivo nije isto što i dokazivo.

EVIDENCE
OVER
OPINION

Same
insights.
Different
outcomes.

Pretpostavimo da je analiza 100% točna.

Što sada?

Imate odlične nalaze i preporuke. Ali kako ih pretvoriti u stvarnu sigurnost?



NALAZI

Što treba riješiti?

17
nedostataka
23
preporuke



PLAN

Što prvo?
Tko je odgovoran?
Koji je rok?

- ✓ Prioriteti
- ✓ Vlasnici
- ✓ Rokovi
- ✓ Resursi



PROVEDBA

Kako to provesti
u organizaciji?

- ✓ Jira taskovi
- ✓ Projekti
- ✓ Timovi
- ✓ Praćenje statusa



DOKAZI

Je li stvarno
provedeno?

- ✓ Prikupiti dokaze
- ✓ Povezati s nalazima
- ✓ Verificirati
- ✓ Revizorska spremnost



MONITORING

Što se promijenilo?
Je li rizik smanjen?

- ✓ Kontinuirano praćenje
- ✓ Novi rizici
- ✓ Promjene u sustavima
- ✓ Promjene u regulativi



NOVA PROCJENA

Je li današnji
rezultat još uvijek
valjan?

- ✓ Reevaluacija
- ✓ Ažurirani podaci
- ✓ Novi zahtjevi
- ✓ Kontinuirani ciklus



A što ste upravo poslali u AI?

Za ovakvu analizu dijelite s vanjskim AI servisom vrlo osjetljive informacije:



Interne
politike i
procedure



Tehničke
podatke i
arhitekturu



Ranjivosti
i incidente



Organizacijsku
strukturu i
odgovornosti



Dobavljače
i ugovore



Procjene rizika
i planove

**Znate li točno gdje ti podaci odlaze, kako se obrađuju,
tko im može pristupiti i pod kojim uvjetima?**



A što ako sve ovo radite sami?

Da biste ovo pretvorili u proces, morate sami:

- ✓ Integrirati više AI alata, izvora podataka i sustava.
- ✓ Razvijati i održavati promptove i logiku.
- ✓ Rješavati promjene API-ja, modela i dozvola.
- ✓ Osigurati sigurnost i kontrolu pristupa.
- ✓ Testirati, validirati i održavati cijeli sustav.
- ✓ Uložiti vrijeme, znanje i resurse – i kontinuirano ga održavati.
- ✓ Preuzeti odgovornost kada nešto krene krivo.

**Vaš tim postaje integrator, developer
i operator AI sustava.**



Odgovor nije sustav upravljanja.

Tekstualni rezultat, čak i vrlo dobar, nije dovoljan za stvarnu sigurnost.

EVIDENCE
OVER
OPINION



77%

of users paste data into
GenAI tools,

82%

of this activity comes from
unmanaged accounts.

"The speed of GenAI adoption is outpacing an organization's ability to control where its data goes."

— LayerX Enterprise AI and SaaS Data Security Report 2025

Source: LayerX Enterprise AI and SaaS Data Security Report 2025
https://go.layerxsecurity.com/hubfs/LayerX_Enterprise_AI_and_SaaS_Data_Security_Report.pdf

EVIDENCE
OVER
OPINION.



THE WORST ENEMY OF SECURITY IS COMPLEXITY.

You can't secure what you
don't understand.

Bruce Schneier — A Plea for Simplicity, 1999

ISTI CILJ. RAZLIČIT PUT.

Isto vrijedi i za AI u upravljanju kibernetičkom sigurnošću.



Možete ga složiti sami.



Zabavno i edukativno



Zahtijeva vrijeme i trud



Rezultat ovisi o vašem iskustvu



Možda izgleda dobro,
ali neće uvijek biti pouzdano

Pitanje nije
možete li sami
složiti rješenje.

**Pitanje je koliko će biti
pouzđano kada vam
stvarno zatreba.**



Ili koristiti nešto što je napravljeno za profesionalnu utrku.



Brzo do rezultata



Testirano i pouzdano



Tim stručnjaka iza rješenja



Fokus na ono što je zaista važno



OSVOJITE LEGO® TECHNIC McLAREN

Skenirajte svoj osobni QR kod na akreditaciji i sudjelujte u anketi.

ZNANJE
POKREĆE
SIGURNIJU
BUDUĆNOST.

Hvala što proizvod gradimo zajedno.

Posebno hvala timovima
Međunarodne zračne luke Zagreb
i **Oktal Pharmer**.

Vaše intenzivno korištenje, pitanja, ideje i otvoreni feedback pomažu nam da ITrevizija.hr svakim danom bude bolji proizvod.



Stvarni korisnici



Stvarni scenariji



Stvarni feedback



Bolji proizvod za sve

ITrevizija.hr

Početna

Samoprocjena

Dokumenti

Rizici

Preporuke

Projektni plan

Izveštaji

Poslovanje

Početna

Upravlajte sigurnošću.
Dokazujte usklađenost.

✓ Analiza dokumentacije

✓ Identifikacija rizika

Preporuke i akcijski plan

Premno za audit

ITrevizija.hr
OSTENDOL CONSUMERS
Hvala na povjerenju!

Vaši podaci. Vaša kontrola.

Sigurnost, privatnost i usklađenost ugrađene su u arhitekturu ITrevizije.



AES-256 enkripcija

Korisnički podaci šifrirani su na razini pojedinačnih polja u bazama podataka i datoteka.



Vaši enkripcijski ključevi

Ključevi ostaju pod kontrolom korisnika. Bez vaše autorizacije nema pristupa zaštićenim podacima.



Bez trećih strana s pristupom vašim podacima

Vaši povjerljivi podaci ne dijele se s vanjskim AI providerima niti drugim trećim stranama radi AI obrade.



AI ne trenira na vašim podacima

Vaši podaci ne postaju dio zajedničkog AI modela. AI gradi privatno znanje o vašoj organizaciji kojim u potpunosti upravljate vi.



EU infrastruktura

Usluga i obrada podataka odvijaju se unutar Europske unije, u skladu s europskim regulativama (GDPR, NIS2 i dr.).



Enkriptirane sigurnosne kopije

Zaštita podataka obuhvaća i backup — ne samo produkcijske baze i datoteke. Sve sigurnosne kopije su šifrirane i zaštićene.



Razvijeno u Hrvatskoj

Vlastiti proizvod i razvojni tim.
Bez outsourcinga ključnih komponenti.

**Ni mi ne možemo čitati
vaše podatke bez vašeg odobrenja.**



Ljudi



Znanje



Tehnologija



Veća otpornost

ITrevizija – AI pod kontrolom.

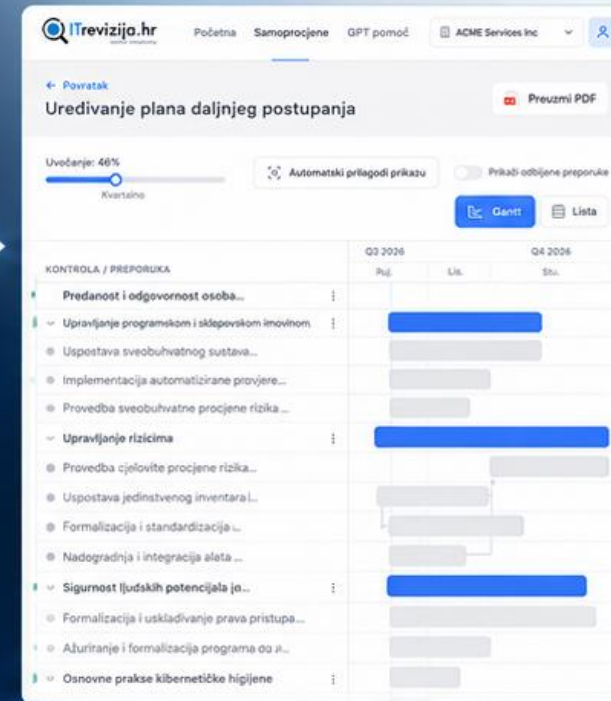
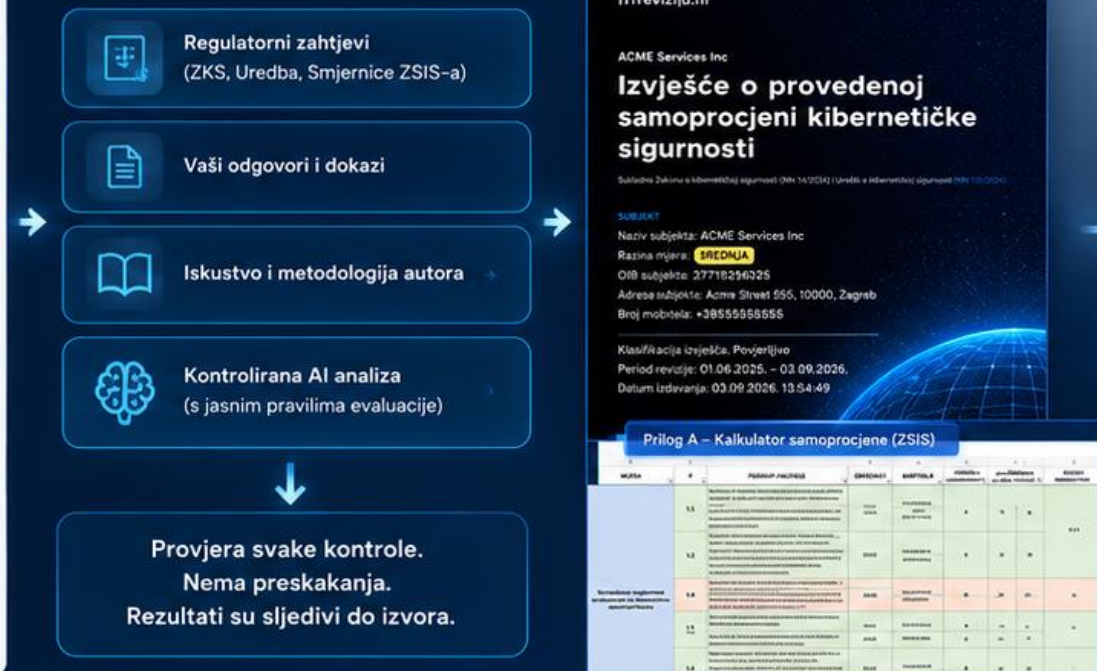
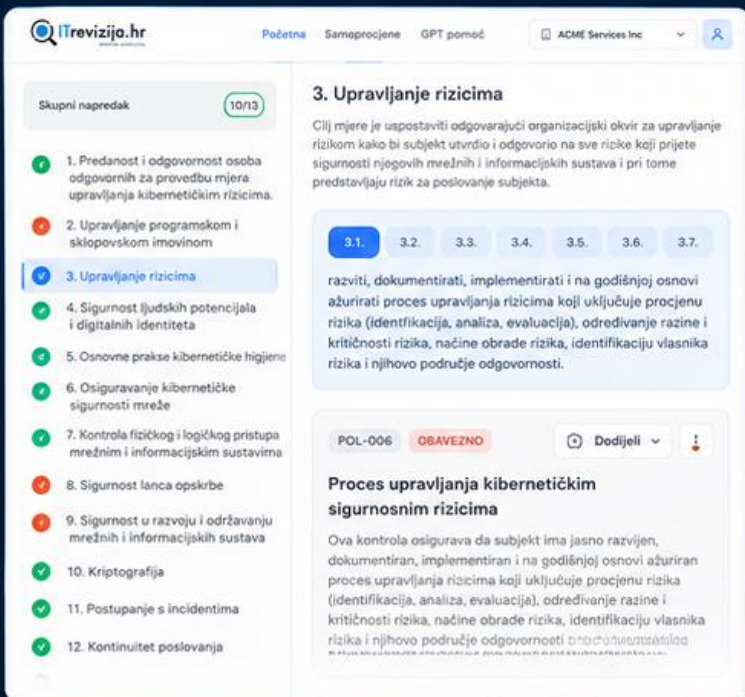
Od regulatornih zahtjeva do konkretnih i provjerljivih rezultata.

1 Svi zahtjevi regulative
 Sustavno obrađene sve mjere i kontrole iz ZKS-a i Smjernica ZSIS-a.

2 Kontrolirana AI procjena
 AI analizira odgovore, dokaze i primjenjuje regulatorna pravila i metodologiju autora.

3 Službeni rezultati
 Generira se točno izvješće i Prilog A u formatu koji traže ZSIS Smjernice.

4 Plan daljnjeg postupanja
 Preporuke se pretvaraju u aktivnosti s rokovima i prati se provedba.



Ništa se ne preskače.
 Sustavno se prolaze sve primjenjive mjere i kontrole.



Metodologija je ugrađena u sustav.
 Pravila evaluacije, kriteriji i iskustvo autora osiguravaju točnost i dosljednost.



Tim ljudi kontinuirano ga poboljšava.
 Iskustva svih klijenata ugrađuju se u sustav – za sve korisnike.

AI daje inteligenciju. ITrevizija osigurava proces.

SIGURNIJA ORGANIZACIJA.
 OTPORNIJE DRUŠTVO.

Dosta slajdova. Pogledajmo kako to stvarno radi.

Od unosa podataka do procjene, izvješća i plana
— u jednom procesu.



Unos podataka
Odgovori, dokazi
i dokumentacija



AI pod kontrolom
Sustavna i
transparentna procjena



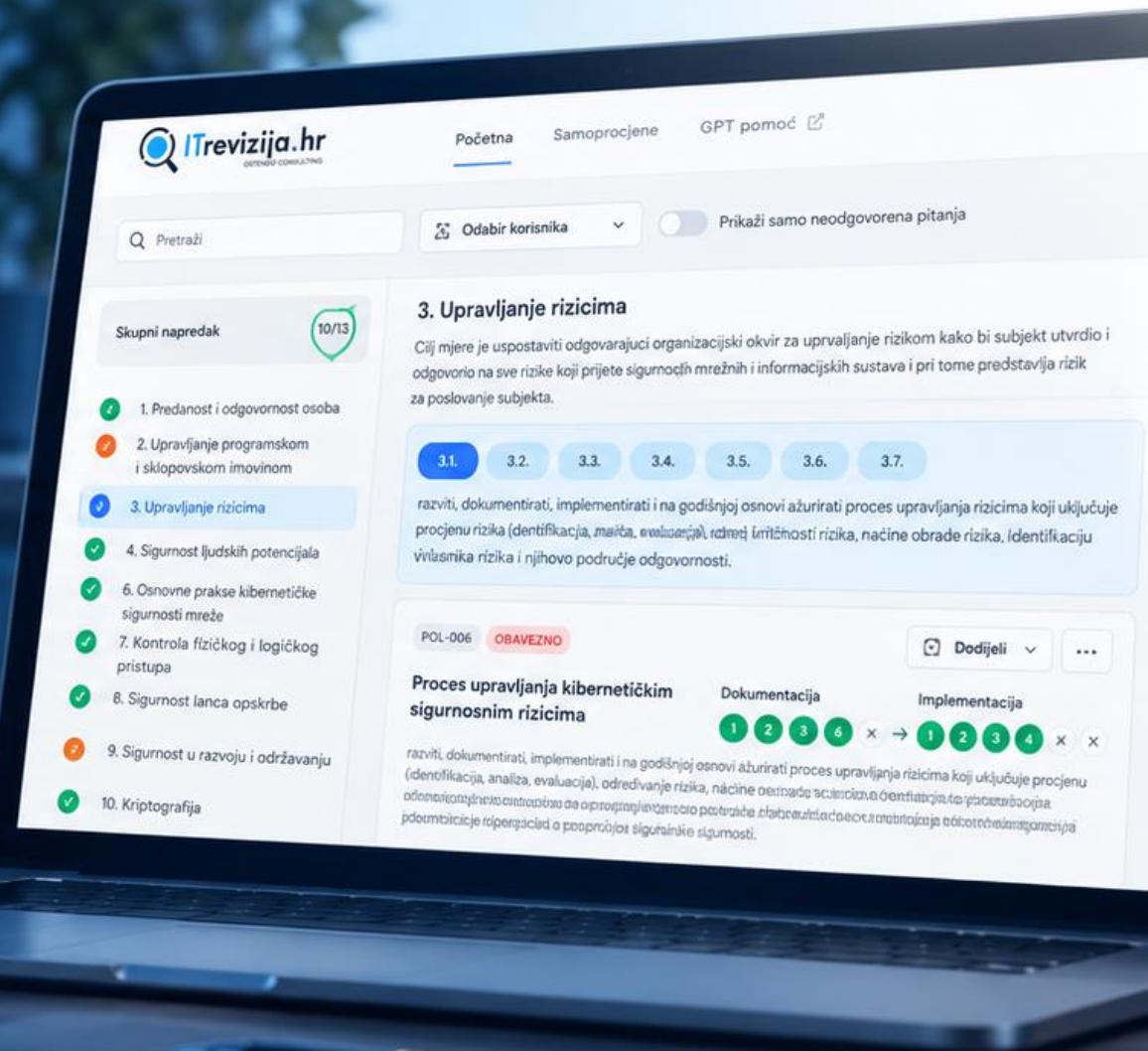
Rezultati
Prilog A i Izvješće
o samoprocjeni



**Plan daljnjeg
postupanja**
Preporuke u aktivnosti
i praćenje provedbe



Pogledajmo ITreviziju.hr u stvarnom radu.



Što smo naučili?

Vrijedno iskustvo iz stvarne primjene ITrevizija rješenja.

Danas: korisnik vodi AI do dokaza

Korisnik mora sam proći kroz sva pitanja i pripremiti dokaze.

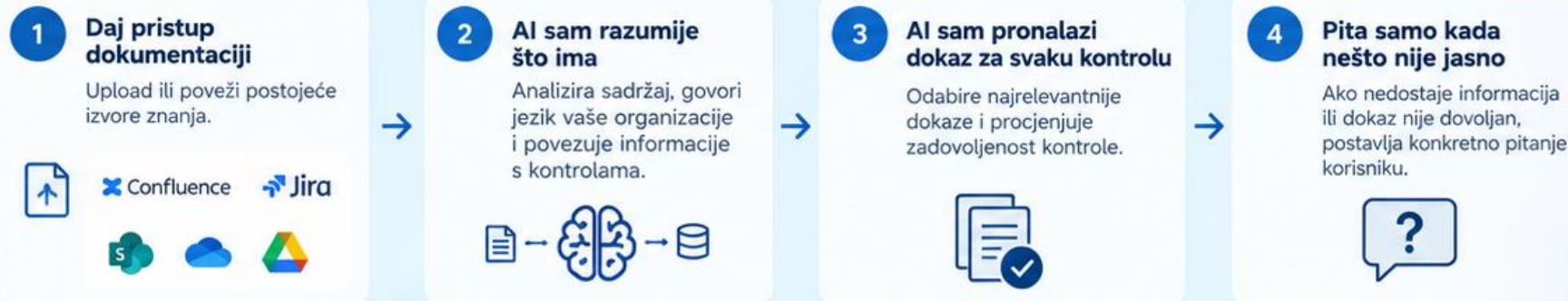


! AI radi **analizu**. Ali čovjek još uvijek radi velik dio posla da bi AI znao što analizirati.

*Previše
ručnog posla...*

A što ako okrenemo proces?

Korisnik daje pristup znanju i dokazima organizacije, a AI radi ostatak.



*AI radi posao.
Ja se bavim
onim što je važno.*



Ne pitamo korisnika da dokazuje svaku kontrolu.
Sustav traži dokaze — i pita korisnika samo ono što ne može sam utvrditi.

RAZUMIJEVANJE
UMJESTO MAPIRANJA.

A smarter path to a more resilient tomorrow.

FROM REQUIREMENTS TO REAL RESILIENCE

1

AI assisted compliance

TURN REQUIREMENTS
INTO ACTION

2

Understanding Systems & Processes

FROM INFORMATION
TO REAL CONTEXT

3

AI powered risk management

FROM INSIGHT
TO RESILIENCE



Q&A

- **info@itrevizija.hr**