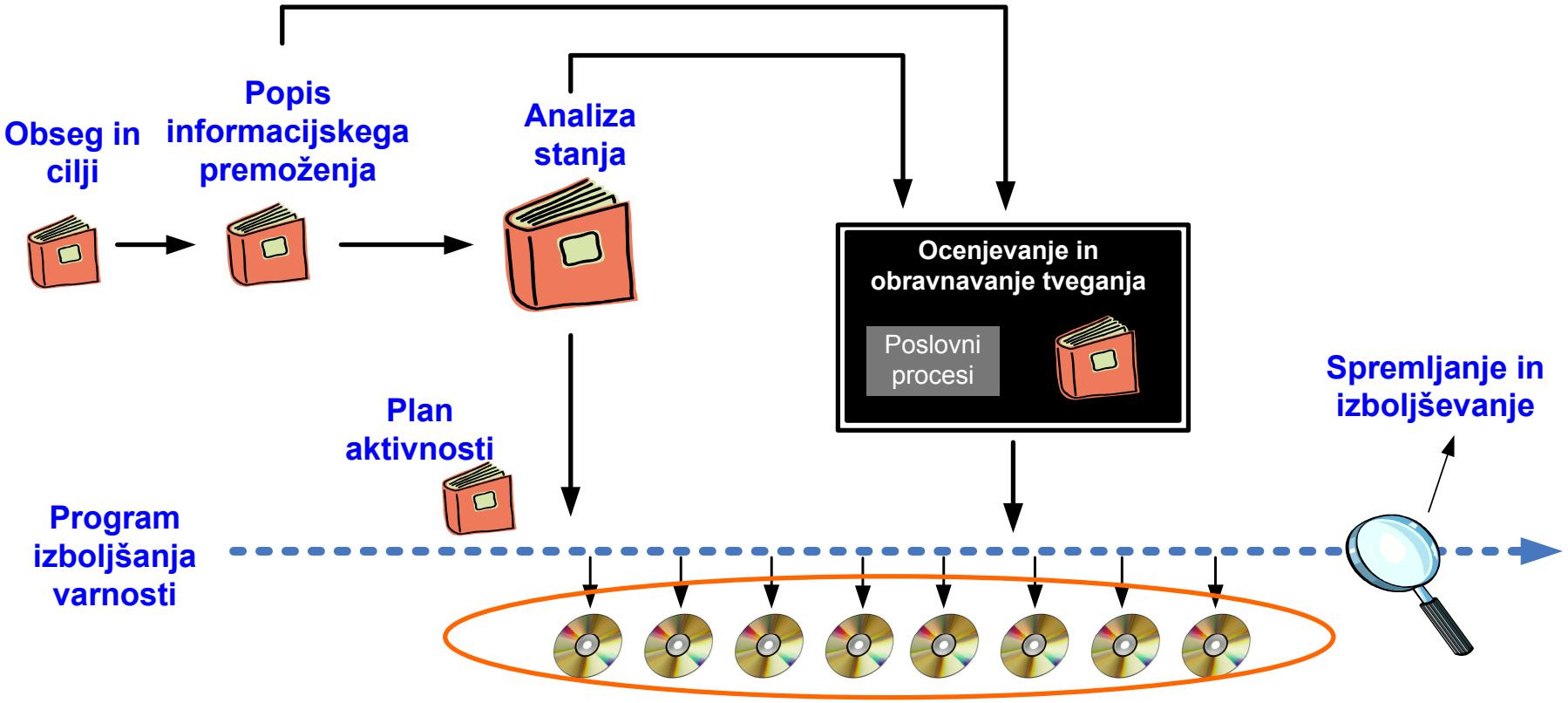
Programska podpora za učinkovito izvedbo analize tveganja

dr. Mina Žele,
vodilna presojevalka ISO/IEC 27001,
preizkušeni revizor informacijskih sistemov

Vloga analize tveganja pri vzpostavitvi optimalne varnosti

SVVI-sistem vodenja varovanja informacij



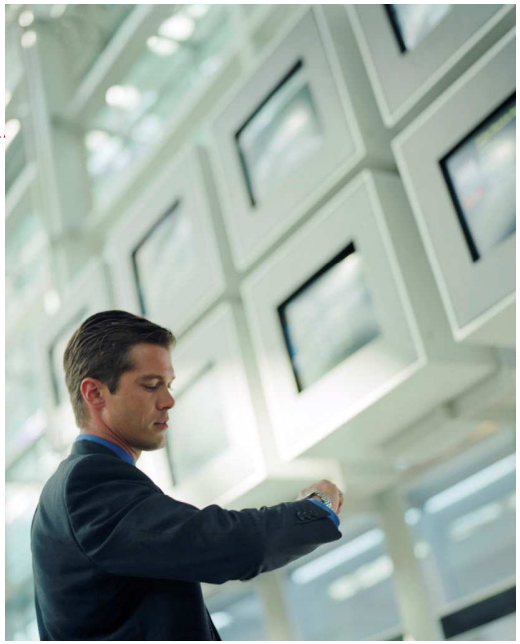
Vloga analize tveganja pri vzpostavitvi optimalne varnosti

- ***Z analizo tveganja ugotovimo varnostne zahteve***

Kaj moramo varovati? Kakšna je vrednost informacijskih sredstev

Kakšno je še sprejemljivo tveganje?

Kakšna je vrednost smiselnih investicij?



Katerim grožnjam so izpostavljena informacijska sredstva?

Katere so ranljivosti informacijskih sredstev?

Analiza tveganja

Sistematičen in celovit pristop k identifikaciji najbolj kritičnih varnostnih pomanjkljivostih v organizaciji

- Trakovi z varnostnimi kopijami podatkov se shranjujejo v omari v sistemski sobi
- Nimamo načrta ponovne vzpostavitve delovanje v primeru odpovedi diska
- V sistemsko sobo imajo dostop vsi zaposleni v informatiki
- Nimamo videonadzora na vhodu v sistemsko sobo
- Pomanjkanje nadzora nad aktivnosti administratorja podatkovne baze
- Vsi zaposleni v sektorju imajo vpogled v bazo podatkov
- Ni bil še izveden zunanji varnostni pregled informacijskega sistema
- Papirni dokumenti so shranjeni v nezaklenjenih omarah

Analiza tveganja

Namen analize tveganja je identificirati grožnje in oceniti, kako visoko tveganje predstavljajo za organizacijo.

Tveganja ocenimo iz :

- verjetnosti uresničitve grožnje
- stopnje posledic grožnje in
- stopnje ranljivosti
- učinkovitosti uporabljanih ukrepov

Tveganja se razvrsti glede na velikost –ugotovimo, katere varnostne pomanjkljivosti so najbolj kritične.

Analiza tveganja

Kako lahko nesprejemljiva tveganje zmanjšamo?

- **uvedbo/spremembo postopka, npr.:**
  - Postopek dodelitve in odvzema pravic uporabniku
  - Postopek neprekinjenega poslovanja v primeru odpovedi IT virov
  - Politika varnostnega kopiranja

- **uvedbo/izboljšavo tehničnih mehanizmov, npr.:**
  - uvedba mehanizma za spremljanje in nadzor aktivnosti administratorjev
  - sistem za odkrivanje in preprečevanje vdorov

Izzivi pri izvedbi analize tveganja

- Izbira ustrezne metodologije
  - Priporočila standarda ISO/IEC 27005:2008
  - Rangiranje vhodnih podatkov (kvalitativne ocene)
  - Enostavna uporaba
  - Preglednost rezultatov

- Kako zbrati, obdelati in analizirati veliko količino podatkov
  - Sistematičen pristop k zbiranju potrebnih podatkov
  - Uporaba namenskih programskih orodij

Izvedba analize tveganja

- Določitev procesov in zahtev
  - Katere aplikacije, strežnike in procese potrebujemo za izvajanje aktivnosti procesa?
  - Kakšna je stopnja zaupnosti informacij?
  - Kakšen je toleriran čas nedelovanja procesa?
  - Koliko časa lahko izvajamo aktivnosti v primeru izpada IS, interneta, elektronske pošte?
  - Kakšne so posledice nedelovanja procesa za poslovanje organizacije?
  - …

Izvedba analize tveganja

Popis informacijskih sredstev

- Informacije v elektronski obliki
- Informacije v fizični
- Osebje
- Strojna oprema
- Programska oprema
- Prenosni računalniški nosilci podatkov
- Komunikacije
- Infrastruktura
- Prostori

Izvedba analize tveganja

- **Uporabljeni varnostni ukrepi**

Kontrole standarda ISO 27002

Izvedba analize tveganja

- Vrednotenje posledic uresničitve groženj
- Katere posledice lahko ocenimo kot visoke, srednje in majhne??
  - Izguba ugleda
  - Kršenje zakonskih in pogodbenih obveznosti
  - Finančna izguba
  - Odpoved storitve (toleriran čas nedelovanja)
  - Razkritje zaupnih informacij
  - Razkritje internih informacij
  - Izguba celovitosti finančnih podatkov

Posledice groženj mora ovrednotiti najvišje vodstvo.

Orodje za podporo analize tveganja

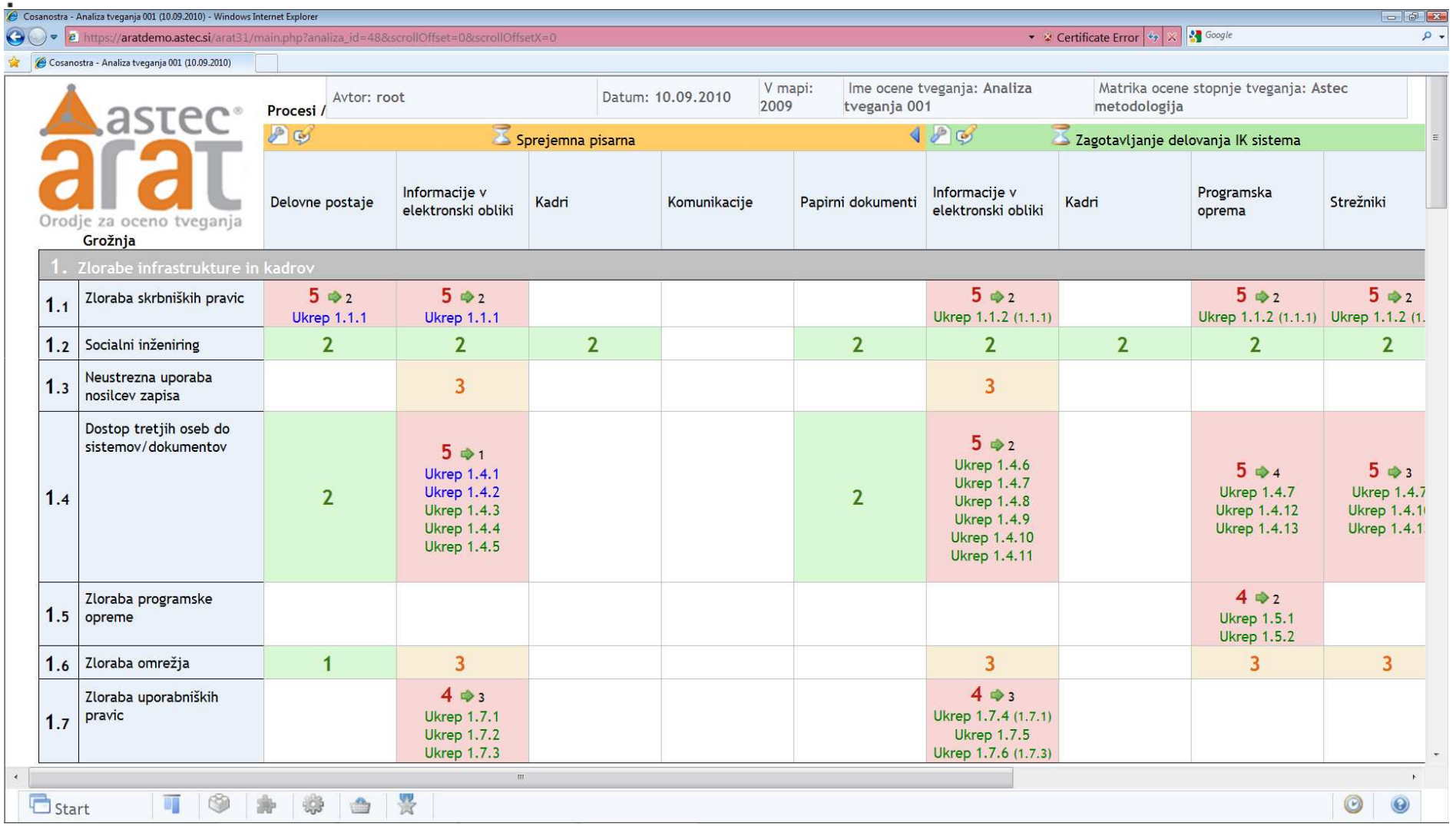
Funkcionalnosti:

- vsebuje katalog groženj in ranljivosti, seznam ISO/IEC 27002 kontrol
- možnost dodajanja novih groženj in informacijskih sredstev
- široke možnosti prilagajanja
- preglednica ukrepov (z ISO/IEC 27002 kontrolami in oceno stroškov izvedbe varnostne rešitve)
- vodenje ukrepov (status, odgovornosti, roki, potrjevanje)
- potrjevanje tveganj in ukrepov
- dostop z različnimi pravicami

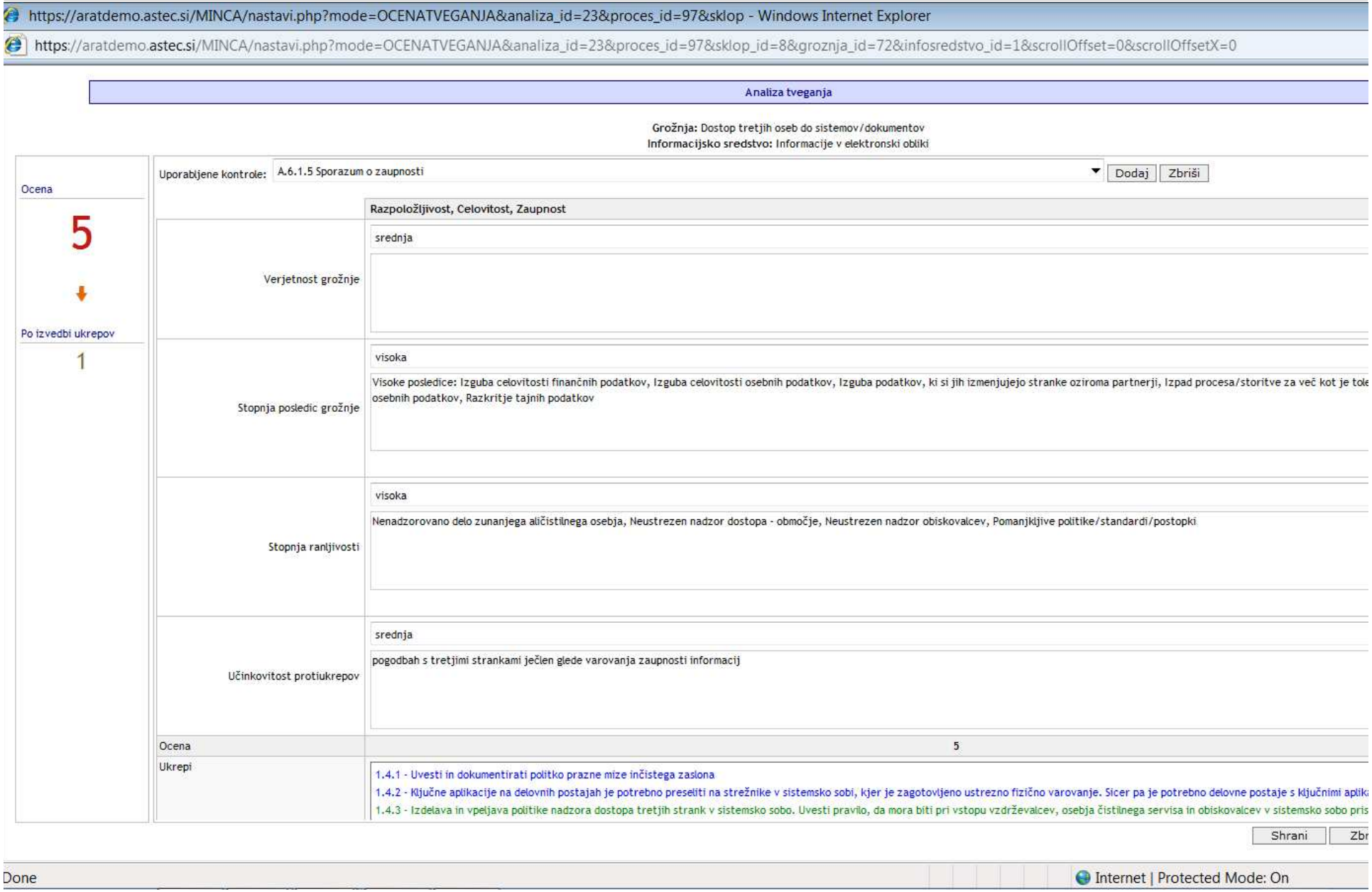
Prednosti:

- enostavna izdelava analize tveganja po procesih
- preglednost rezultatov
- enostavno posodabljanje

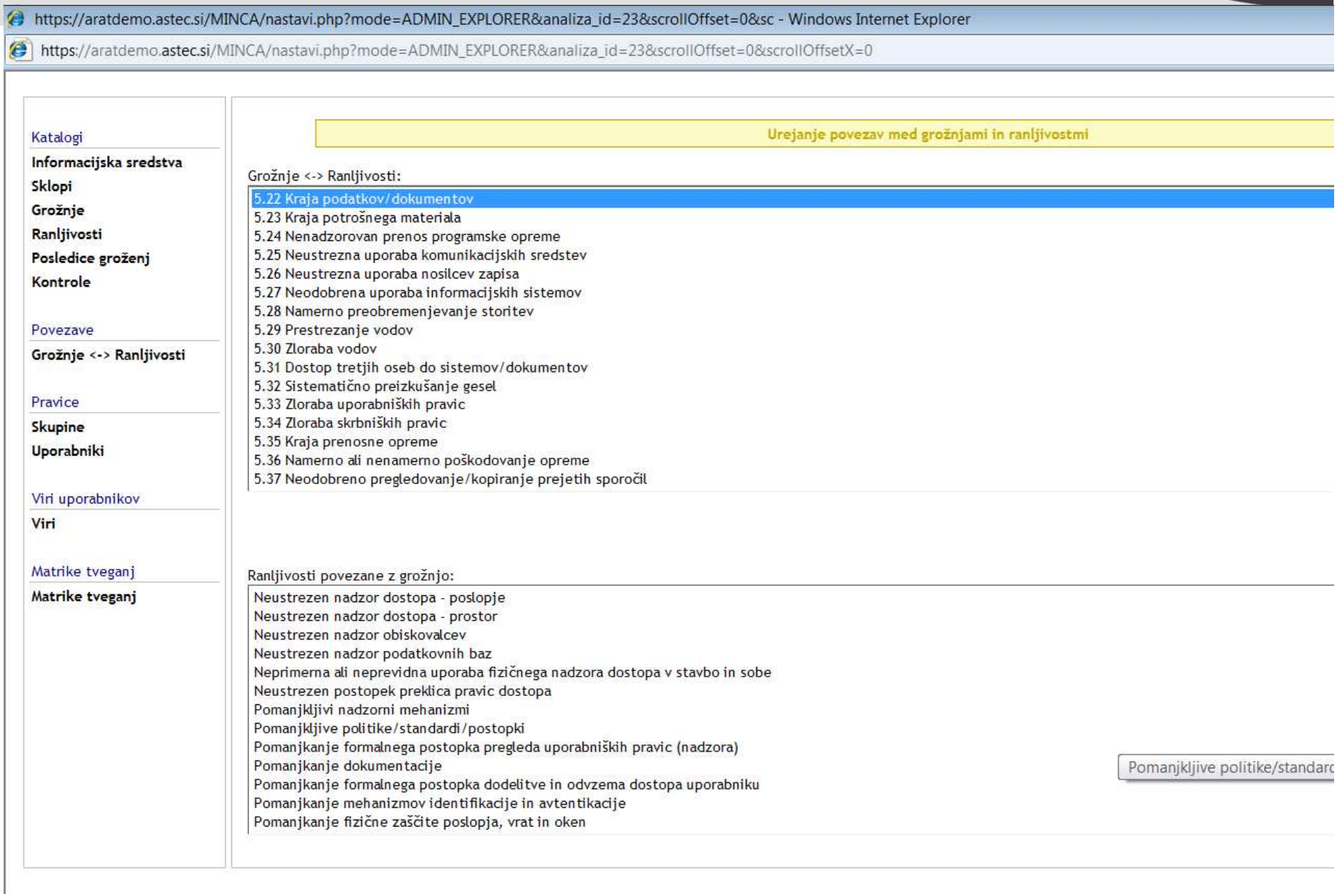
ARAT- Orodje za podporo analize tveganja



ARAT- Orodje za podporo analize tveganja



ARAT- Orodje za podporo analize tveganja



ARAT- Orodje za podporo analize tveganja

https://aratdemo.astec.si/DIU/nastavi.php - Windows Internet Explorer

https://aratdemo.astec.si/DIU/nastavi.php

Residual risk	Ser. No.	Threat	Information assets	Action	Costs	Controls	Responsible person	Due date	Implementation date	State
Proces: Main office										
5	1.1.1	1.1 Abuse of administrator rights	Electronic information Workstations	Implementation of SIEM (Security Information and Event Management) system.		A.10.10.2 Monitoring system use		30.7.2010		accomplished
5	1.4.1	1.4 Third-party access to systems / documents	Electronic information	Implement and document clear desk and clear screen policy.		A.11.3.3 Clear desk and clear screen policy			15.12.2009	accomplished
5	1.4.2	1.4 Third-party access to systems / documents	Human resources Electronic information	Critical applications installed in workstations should be migrated to servers in the server room, where appropriate physical protection is provided. However, the workstations with critical applications should be protected to prevent unauthorized physical access, and disaster recovery procedures must be ensured in case of physical damage.		A.9.1.4 Protecting against external and environmental threats			15.12.2009	accomplished
5	1.4.3	1.4 Third-party access to systems / documents	Electronic information	Develop and implement a policy for third parties access control to the server room. Implement the rule that an authorized person should supervise visitors, maintenance and cleaning staff while entering the service room.		A.9.1.5 Working in secure areas				in implementati
5	1.4.4	1.4 Third-party access to systems / documents	Electronic information	Draw up the confidentiality and non-disclosure agreement that must be signed by all third parties having logical or physical access to information, applications, or systems.		A.6.1.5 Confidentiality agreements				in implementati
5	1.4.5	1.4 Third-party access to systems / documents	Electronic information	Removable media with back-up copies should be stored in locked fire resistant cupboards.		A.10.5.1 Information back-up				in implementati
4	1.6.1	1.6 Abuse of user rights	Electronic information	A formal procedure to review user access rights should be introduced.		A.11.2.4 Review of user access rights				in implementati
4	1.6.2	1.6 Abuse of user rights	Electronic information	Define disciplinary procedure in case of security incidents.		A.13.2.1 Responsibilities and procedures				in implementati
4	1.6.3	1.6 Abuse of user rights	Electronic information	Provide employees with regular information security awareness training.		A.8.2.2 Information security awareness, education, and training				in implementati
Proces: Provision of information system services										
5	1.1.2	1.1 Abuse of administrator rights	Electronic information Servers --DNS server --Data server --Mail server --www server	Implementation of SIEM (Security Information and Event Management) system.		A.10.10.1 Audit logging				in implementati

Done

Internet | Protected Mode: On

100%

Astec d. o. o.
Stegne 31

W: www.astec.si
T: +386 1 2008300
F: +386 1 2008310

mina.zele@astec.si
041 787 395