# OCENA TVEGANJA V PROCESU CERTIFICIRANJA PO ZAHTEVAH ISO/IEC 27001

Jernej Potočnik, Henrik Udovč

Portorož, april 2012

# Cilji predstavitve

- Predstaviti potek projekta SUVI
- Opozoriti na probleme, na katere smo naleteli na projektu in pri izvedbi ocene tveganja
- Predstaviti praktične rešitve s pomočjo programskega orodja

# Uvod

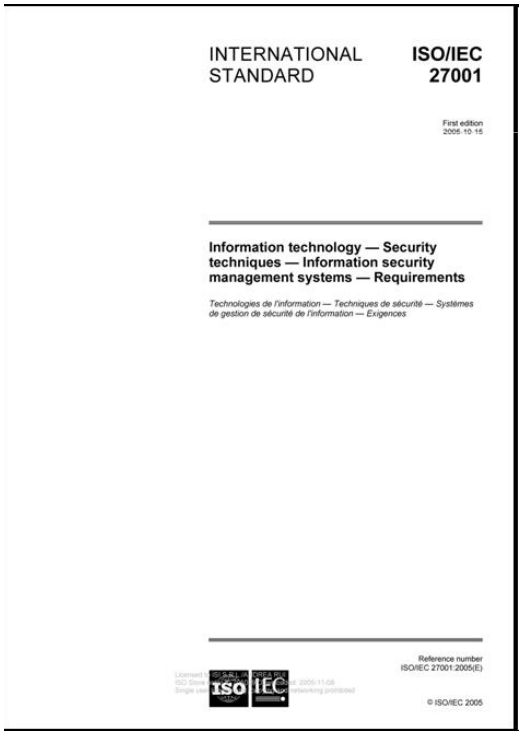
- Informacije imajo iz dneva v dan večjo vrednost.
- Potrebno jih je primerno varovati.
- Zaradi narave našega dela smo se tega zavedali.
- Problematiko smo obravnavali predvsem s tehničnega vidika.

# Vodstvo in SUVI

- Vodstvo je ugotovilo naslednje:
  - tak pristop k varovanju ne zadošča več našim potrebam,
  - tak pristop k varovanju ne izpolnjuje več pričakovanj naših strank,
  - varovanja informacij se je potrebno lotiti sistematično na upravljavskem nivoju,
  - zmanjševati je potrebno tveganja v zvezi z varovanjem informacij.

# Odločitev za vzpostavitev SUVI

- Odločitev za vzpostavitev in certificiranje sistema upravljanja varovanja informacij (SUVI).
- Izbrali smo standard ISO/IEC 27001.


INTERNATIONAL STANDARD

ISO/IEC 27001

First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

*Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences*

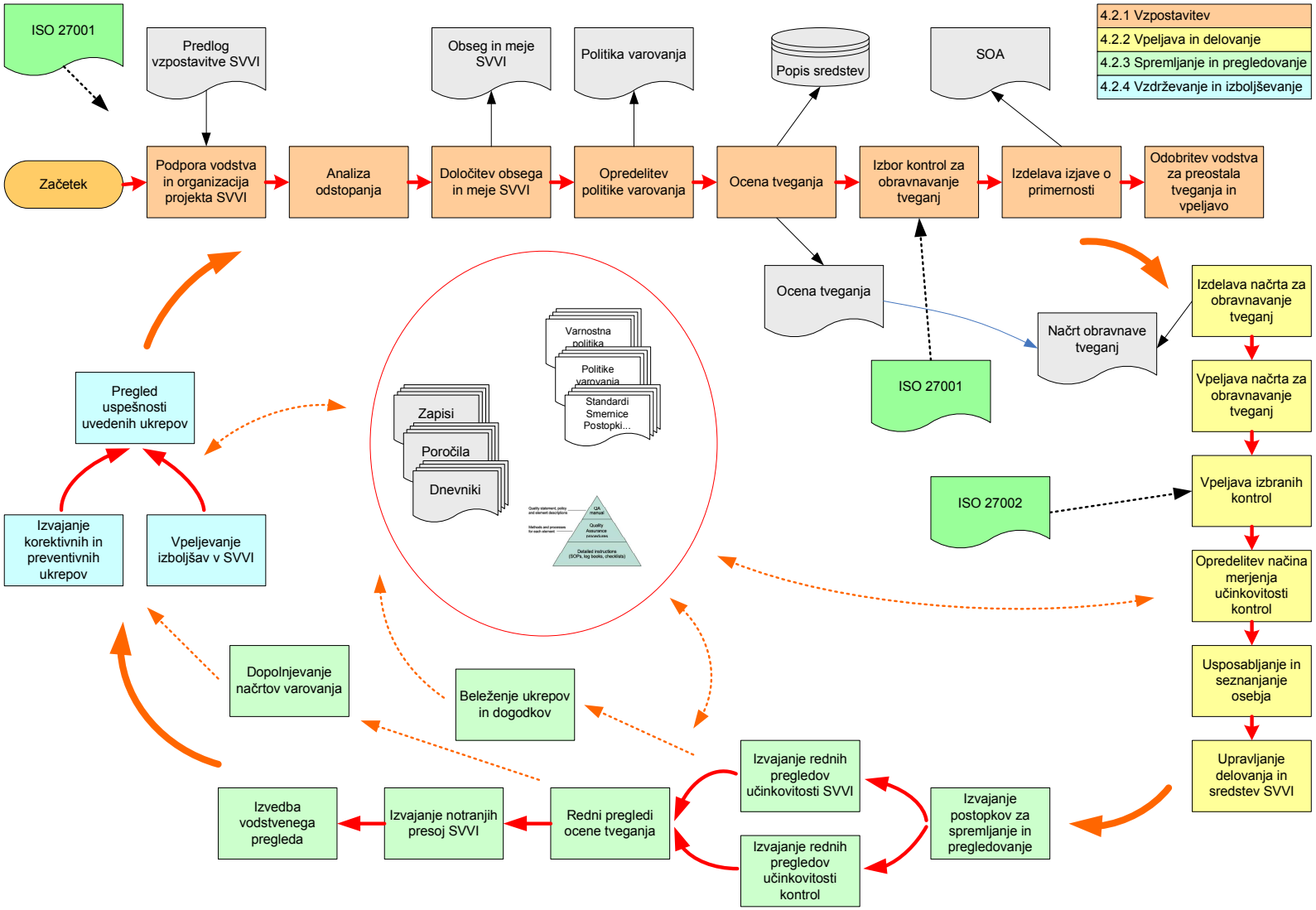
Reference number
ISO/IEC 27001:2005(E)

© ISO/IEC 2005

# Projekt vzpostavitve SUVI

- Standard ISO/IEC 27001 zahteva, da SUVI deluje po principu Demingovega kroga nenehnega izboljševanja (PDCA), ki vključuje faze načrtovanja, uvedbe in izvajanja, nadzora, analiziranja ter ukrepanja

# Potek projekta SUVI



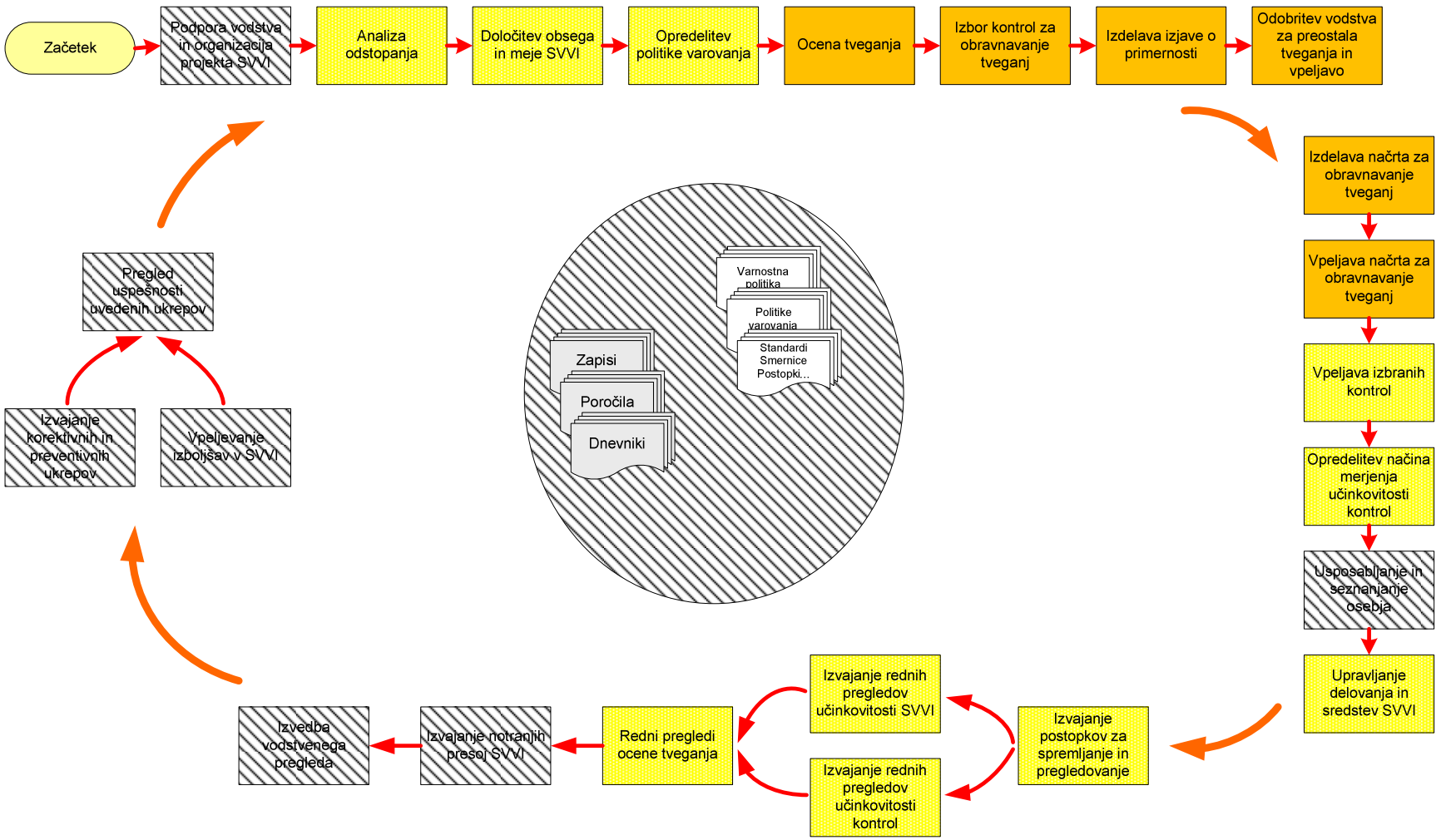
# ISO/IEC 27001 in ISO 9001

- Pred leti smo vzpostavili in certificirali naš sistem vodenja kakovosti (SVK) po ISO 9001
- Že na začetku projekta SUVI smo ugotovili, da imamo princip PDCA že vzpostavljen.

# Prednosti zaradi že vzpostavljenega SVK po ISO 9001

- Že na začetku projekta SUVI  smo izpolnjevali nekatere zahteve standarda ISO/IEC 27001:
  - podporo vodstva in organizacijo,
  - obvladovanje dokumentov in zapisov,
  - obvladovanje procesov,
  - notranje presoje,
  - vodstvene preglede,
  - izboljšave ter korektivne in preventivne ukrepe,
  - definiranje odgovornosti,
  - usposabljanje zaposlenih...

# Pokritost SUVI z elementi SVK



# Obseg dela pri vzpostavitvi SUVI

- Na projektu SUVI je potrebno na novo izvesti proces vzpostavitve (česar standard ISO 9001 ne zahteva) ter vpeljave sistema.
- Zaradi vzpostavljenega SVK je bil obseg dela na projektu SUVI bistveno manjši.
- Obseg dela pa je bil manjši tudi zato, ker smo že imeli vzpostavljene tehnične mehanizme zagotavljanja varnosti.

# Ocena tveganja in projekt SUVI

- Ocena tveganja je ena od najbolj pomembnih, pa tudi zahtevnih in obsežnih aktivnosti projekta SUVI.
- Ocenili smo, da bo izvedba ocene tveganja in ostalih aktivnosti predstavljala več kot 50% vsega dela.

# Ocena tveganja

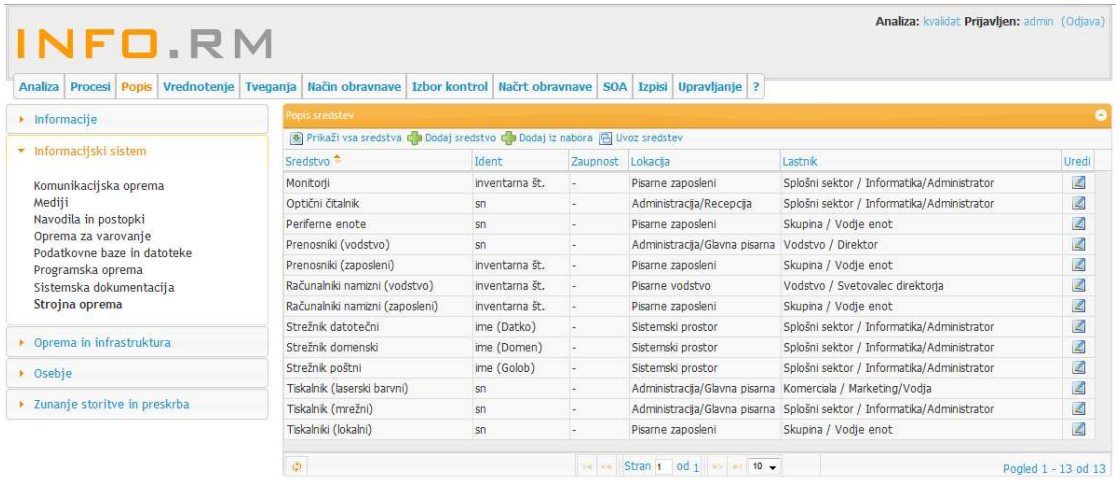
- V splošnem obsega naslednje glavne faze:
  - izbor ustrezne metodologije ocenjevanja tveganj,
  - izdelava popisa sredstev,
  - vrednotenje sredstev,
  - določitev groženj za posamezna sredstva,
  - ocena vpliva in verjetnosti posameznih groženj ter ranljivosti posameznega sredstva,
  - določiti način obravnave tveganj,
  - izbrati ustrezne kontrole za zmanjševanje tveganj,
  - pripraviti izjavo o uporabnosti (SOA),
  - izdelati načrt obravnave tveganj.

# Problemi pri izvedbi ocene tveganja

- Izvesti moramo veliko aktivnosti.
- Obvladovati moramo veliko število podatkov.
- Potrebno je izvesti izračune tveganja za množico kombinacij sredstvo/groženja.
- Po izboru primernih kontrol dobimo še večjo množico kombinacij sredstvo/grožnja/kontrola.
- Z uporabo MS Excel-a nismo je postalo vse skupaj preobsežno in nepregledno.

# Orodje za podporo ocene tveganja

- Razvili smo programsko orodje.
- Omogočilo je učinkovito izvedbo ocene tveganja.
- Podprlo je ostale aktivnosti, ki jih zahteva standard.
- Izdelali smo lahko vse potrebne dokumente in izpise.
- Omogočeno je sodelovanje vseh lastnikov sredstev.



# Programsko orodje in metodologija

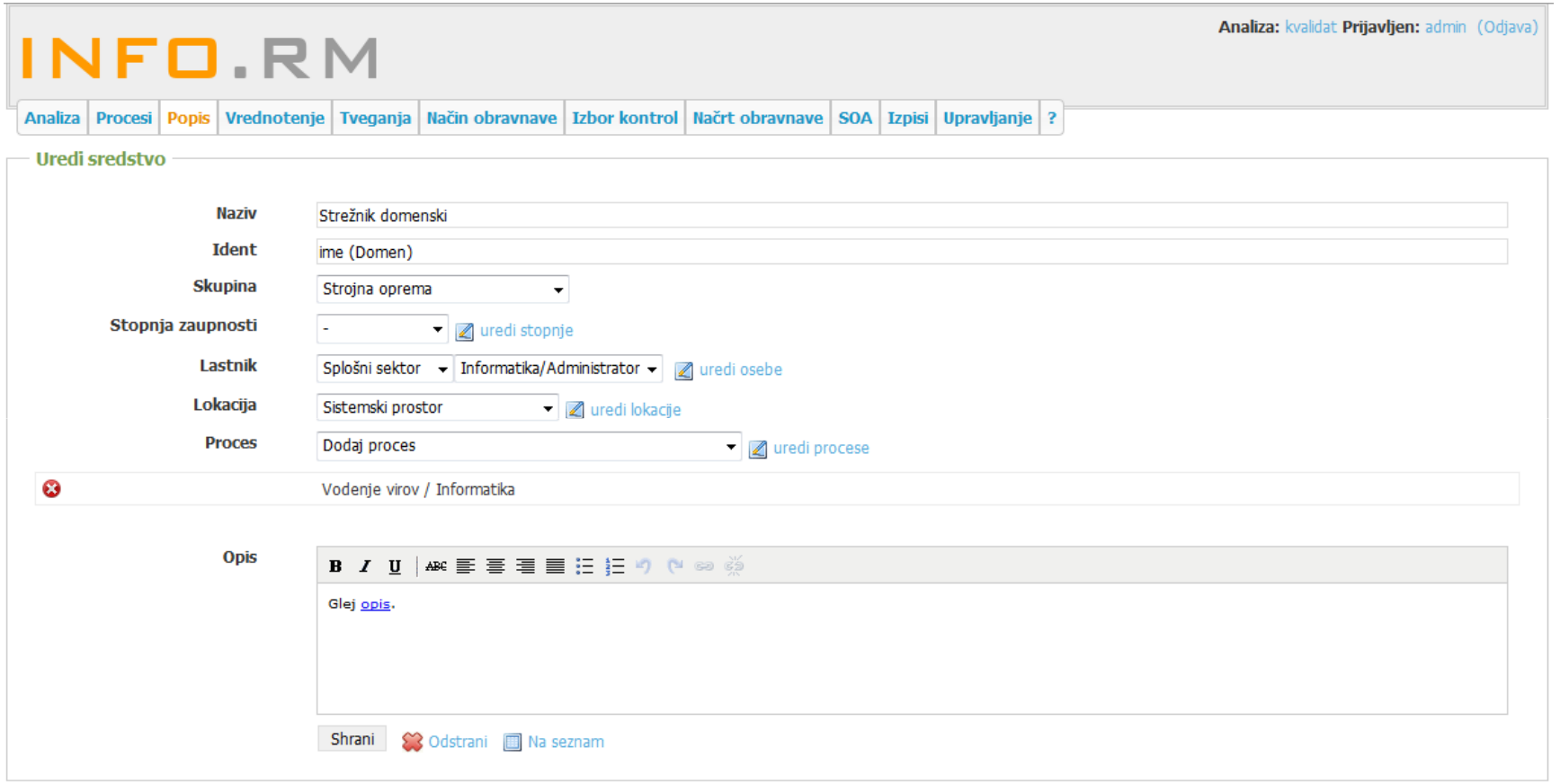
- Metodologija je že vgrajena v izbrano programsko orodje.
- Je skladna z najboljšimi praksami.
- Je skladna z zahtevami ISO/IEC 27001.

| Ranljivost | Vrednost | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vpliv | | 1 | | | | | 2 | | | | | 3 | | | | | 4 | | | | | 5 | | | | |
| Verjetnost | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 1 | 2 | 3 | 4 | 5 | 2 | 3 | 4 | 5 | 6 | 3 | 4 | 5 | 6 | 7 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 |
| | 2 | 2 | 3 | 4 | 5 | 6 | 3 | 4 | 5 | 6 | 7 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 |
| | 3 | 3 | 4 | 5 | 6 | 7 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 |
| | 4 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 |
| | 5 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 |
| 2 | 1 | 2 | 3 | 4 | 5 | 6 | 3 | 4 | 5 | 6 | 7 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 |
| | 2 | 3 | 4 | 5 | 6 | 7 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 |
| | 3 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 |
| | 4 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 |
| | 5 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 |
| 3 | 1 | 3 | 4 | 5 | 6 | 7 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 |
| | 2 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 |
| | 3 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 |
| | 4 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 |
| | 5 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 | 11 | 12 | 13 | 14 | 15 |
| 4 | 1 | 4 | 5 | 6 | 7 | 8 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 |
| | 2 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 |
| | 3 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 |
| | 4 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 | 11 | 12 | 13 | 14 | 15 |
| | 5 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 | 11 | 12 | 13 | 14 | 15 | 12 | 13 | 14 | 15 | 16 |
| 5 | 1 | 5 | 6 | 7 | 8 | 9 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 |
| | 2 | 6 | 7 | 8 | 9 | 10 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 |
| | 3 | 7 | 8 | 9 | 10 | 11 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 | 11 | 12 | 13 | 14 | 15 |
| | 4 | 8 | 9 | 10 | 11 | 12 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 | 11 | 12 | 13 | 14 | 15 | 12 | 13 | 14 | 15 | 16 |
| | 5 | 9 | 10 | 11 | 12 | 13 | 10 | 11 | 12 | 13 | 14 | 11 | 12 | 13 | 14 | 15 | 12 | 13 | 14 | 15 | 16 | 13 | 14 | 15 | 16 | 17 |

# Popis sredstev

- Sredstva združimo v skupine sredstev istega tipa.
- Večja preglednost popisa sredstev.
- Določimo lastnike posameznih sredstev.
- Določimo procese in lokacije, v katerih sredstvo nastopa.
- Možna različna obravnava tveganj za sredstvo glede na proces ali lokacijo.

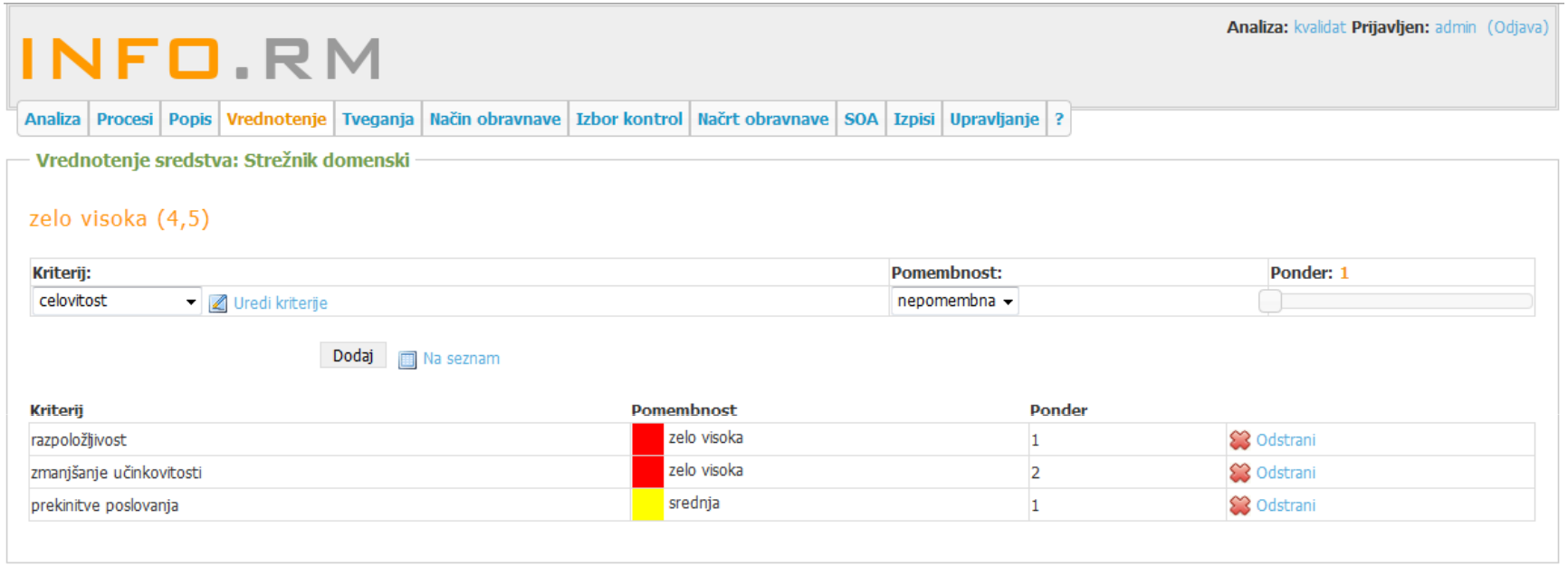
# Popis sredstev



# Vrednotenje sredstev

- Določimo vrednost sredstva glede na kriterije.
- Poleg običajnih kriterijev (celovitost, razpoložljivost, zaupnost) lahko upoštevamo druge kriterije:
  - poslovni interesi, finančne izgube, zmanjšanje učinkovitosti, prekinitve poslovanja, zakonske kršitve, zahteve regulative, ugled organizacije, varnost osebja, osebni podatki, družba in okolje, izguba naklonjenosti, javni red in mir...
- Dobimo bolj uporabno sliko vrednosti sredstva.
- Vrednost sredstva se upošteva pri izračunu tveganj, posledično dobimo realnejšo vrednost tveganja.

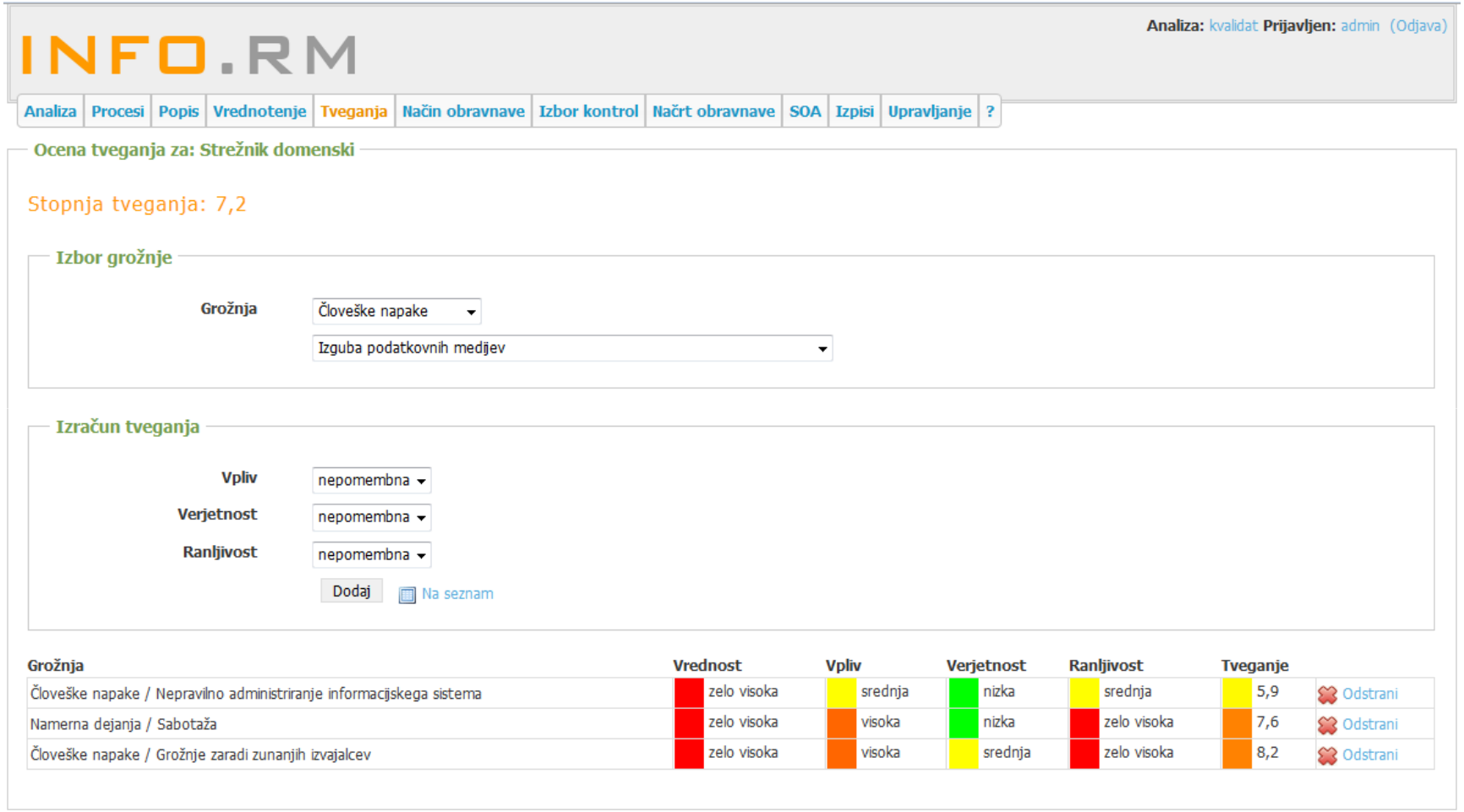
# Vrednotenje sredstev



# Izračun tveganja

- Orodje vsebuje obsežen in strukturiran nabor možnih groženj.
- Hitro in enostavno izberemo primerne grožnje.
- Dobimo kmalu zelo veliko število kombinacij sredstvo/grožnja, ki jih enostavno obvladujemo.
  - Ocenimo vpliv posamezne grožnje na sredstvo.
  - Ocenimo realno verjetnost dogodka.
  - Ocenimo ranljivost sredstva.
- Algoritem je že vgrajen v programsko orodje.
- Ni potrebno razbirati vrednosti tveganja iz matrike.

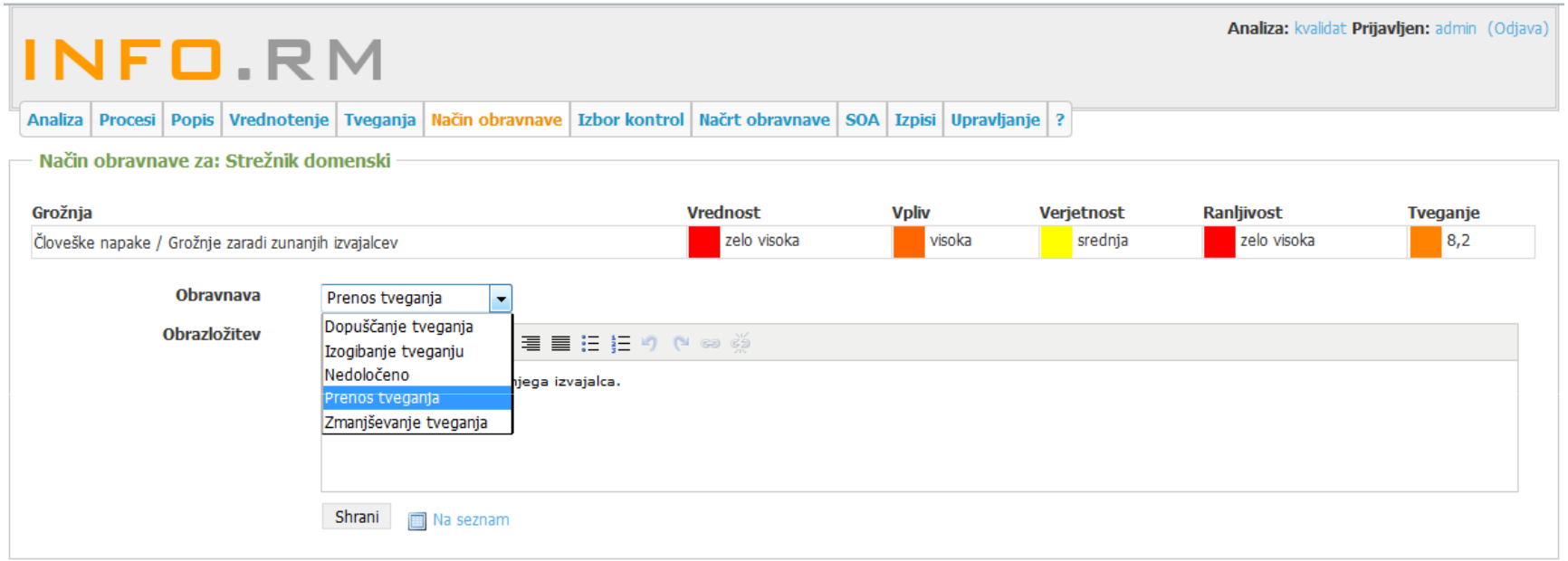
# Izračun tveganja



# Določitev načina obravnave tveganj

- Določimo sprejemljivi nivo tveganja.
- Za nižjo vrednost, kot je sprejemljivi nivo tveganj, se avtomatično določi status »Dopuščanje tveganj«.
- Določimo ostale načine obravnave tveganja:
  - Prenos tveganja
  - Izogibanje tveganju
  - Zmanjševanje tveganja
- V nadaljevanju obravnavamo le najbolj pomembna tveganja.

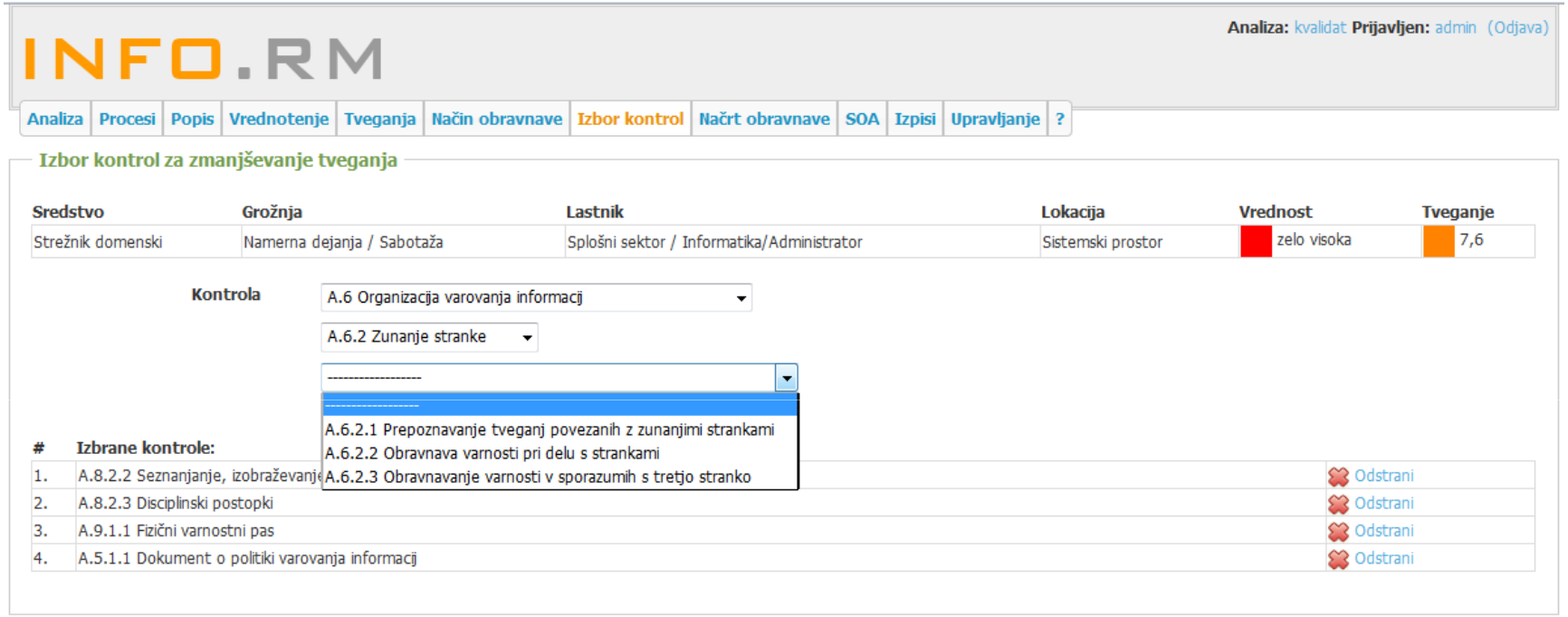
# Določitev načina obravnave tveganj



# Izbor kontrol za obravnavo tveganj

- Že vsebuje vse kontrole, ki so predpisane v prilogi A standarda ISO/IEC 27001.
- Omogoča pregleden in enostaven način izbora ustrezne kontrole.
- Izberemo lahko eno ali več primernih kontrol.
- Omogoča izdelavo podrobnejšega načrta obravnave tveganj.

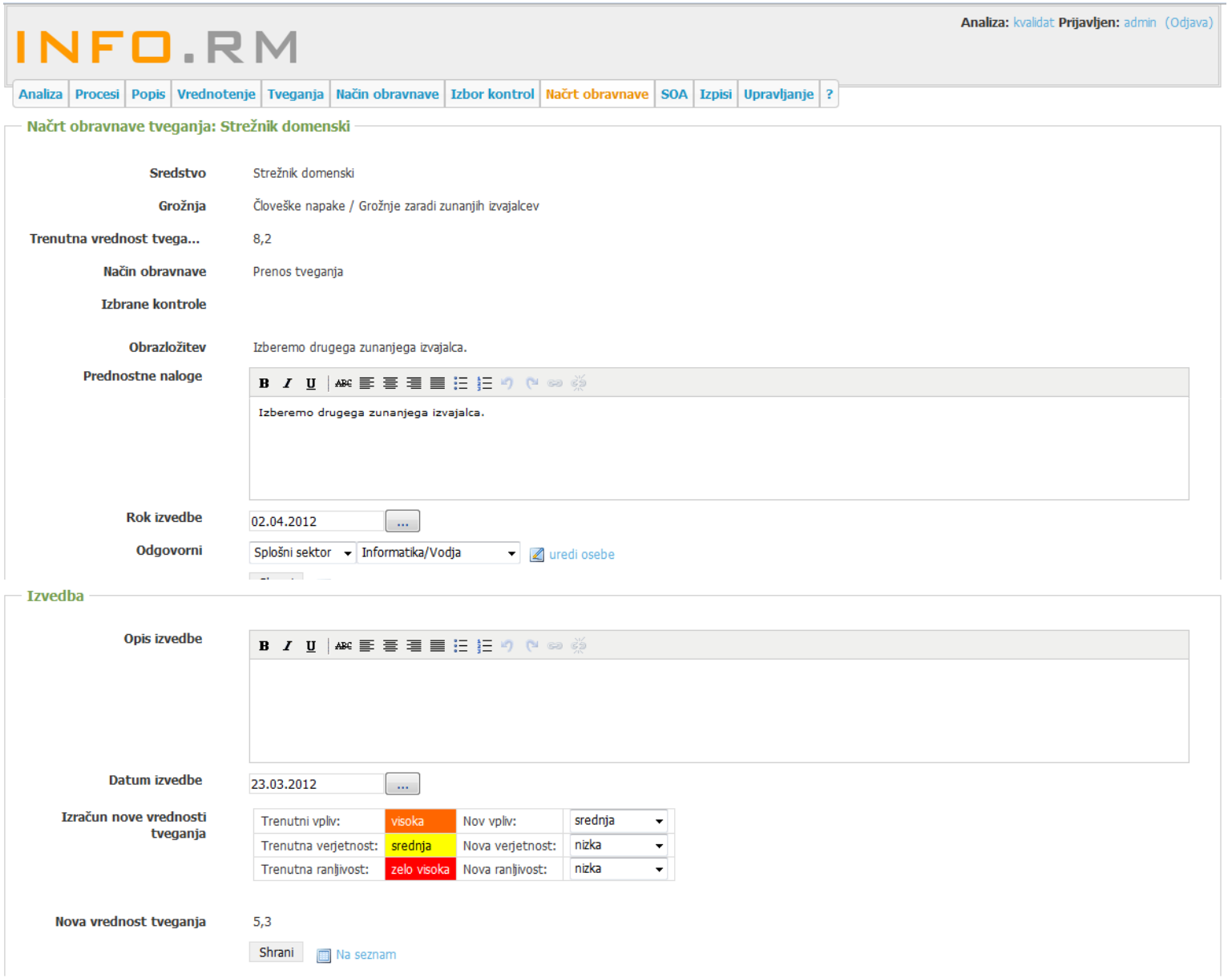
# Izbor kontrol za obravnavo tveganj



# Izdelava načrta obravnave tveganj

- Omogoča izdelavo podrobnega načrta za obravnavo tveganj.
- V načrtu določimo ukrepe za vpeljavo izbranih kontrol.
- Določimo, odgovornosti in naloge oziroma aktivnosti.
- Spremljamo realizacijo načrta obravnave tveganj.

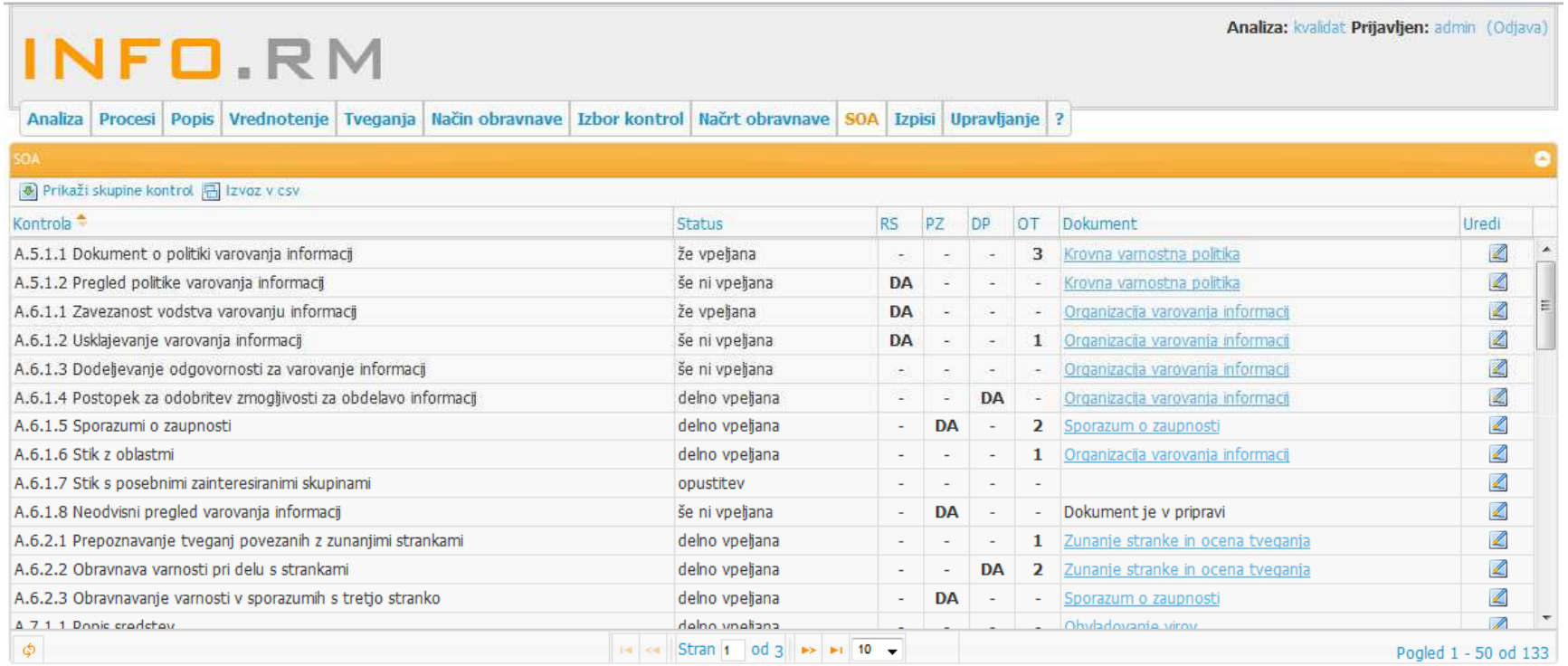
# Izdelava načrta obravnave tveganj



# Priprava izjave o uporabnosti (SOA)

- Omogoča avtomatično izdelavo kompleksnega dokumenta »Izjava o uporabnosti« (SOA).
- Določimo status izbrane kontrole.
- Definiramo razloge za izbor kontrole in navedemo pripadajoče dokumente, ki opisujejo način vpeljave izbrane kontrole.
- V kolikor kontrole ne izberemo, definiramo razloge za opustitev.

# Priprava izjave o uporabnosti (SOA)



INFO.RM

Analiza: kvalidat Prijavljen: admin (Odjava)

Analiza | Procesi | Popis | Vrednotenje | Tveganja | Način obravnave | Izbor kontrol | Načrt obravnave | SOA | Izpisi | Upravljanje | ?

SOA

Prikaži skupine kontrol | Izvoz v csv

| Kontrola | Status | RS | PZ | DP | OT | Dokument | Uredi |
|---|---|---|---|---|---|---|---|
| A.5.1.1 Dokument o politiki varovanja informacij | že vpeljana | - | - | - | 3 | Krovna varnostna politika | |
| A.5.1.2 Pregled politike varovanja informacij | še ni vpeljana | DA | - | - | - | Krovna varnostna politika | |
| A.6.1.1 Zavezanost vodstva varovanju informacij | že vpeljana | DA | - | - | - | Organizacija varovanja informacij | |
| A.6.1.2 Usklajevanje varovanja informacij | še ni vpeljana | DA | - | - | 1 | Organizacija varovanja informacij | |
| A.6.1.3 Dodeljevanje odgovornosti za varovanje informacij | še ni vpeljana | - | - | - | - | Organizacija varovanja informacij | |
| A.6.1.4 Postopek za odobritev zmogljivosti za obdelavo informacij | delno vpeljana | - | - | DA | - | Organizacija varovanja informacij | |
| A.6.1.5 Sporazumi o zaupnosti | delno vpeljana | - | DA | - | 2 | Sporazum o zaupnosti | |
| A.6.1.6 Stik z oblastmi | delno vpeljana | - | - | - | 1 | Organizacija varovanja informacij | |
| A.6.1.7 Stik s posebnimi zainteresiranimi skupinami | opustitev | - | - | - | - | | |
| A.6.1.8 Neodvisni pregled varovanja informacij | še ni vpeljana | - | DA | - | - | Dokument je v pripravi | |
| A.6.2.1 Prepoznavanje tveganj povezanih z zunanjimi strankami | delno vpeljana | - | - | - | 1 | Zunanje stranke in ocena tveganja | |
| A.6.2.2 Obravnava varnosti pri delu s strankami | delno vpeljana | - | - | DA | 2 | Zunanje stranke in ocena tveganja | |
| A.6.2.3 Obravnavanje varnosti v sporazumih s tretjo stranko | delno vpeljana | - | DA | - | - | Sporazum o zaupnosti | |
| A.7.1.1 Popis sredstev | delno vpeljana | - | - | - | - | Obvladovanje virov | |

Stran 1 od 3 | 10 | Pogled 1 - 50 od 133

**RS** - Regulativa,standardi **PZ** - Pogodbene zahteve **DP** - Dobra praksa **OT** - Zaradi ocene tveganja

# Zaključek

- Predstavili potek projekta vzpostavitve SUVI.
- Obseg potrebnega dela je bistveno manjši, če imamo vzpostavljen SVK.
- Izvedba ocene tveganja obsega najmanj 50% vloženega truda.
- Smiselna je uporaba programskega orodja.
- Na enostaven način pridemo  do vseh potrebnih dokumentov.
- Je dobra osnova za obravnavo ostalih poslovnih tveganj.

# Vprašanja?

# Viri


- [1] KOŠIR Aleš, OREL Andrej: Pregled in primerjava orodij za podporo obvladovanju tveganj, ISACA, 2010
- [2] BSI (2005a). BS ISO/IEC 27001:2005 Information technology – Security techniques - Information security management systems – Requirements, British Standard Institution
- [3] BSI (2005). BS ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management, British Standard Institution
- [4] ISO 31000:2009 Risk management -- Principles and guidelines, ISO, 2009
- [5] BSI (Bundesamt für Sicherheit in der Informationstechnik), IT Baseline Protection Manual, 2004
- [6] THOMSON - Knowledgenet Certified Information Systems Security Professionals Cissp Student Guide v1.0 -.2006