

# UPORABA PROGRAMSKEGA ORODJA ZA PODPORO OBVLADOVANJU TVEGANJ

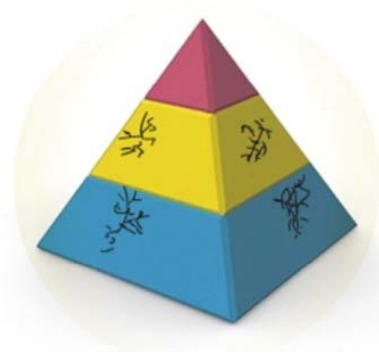
Jernej Potočnik, Henrik Udovč  
Portorož, april 2011

## Cilji predstavitve

- Predstaviti temeljne zahteve standarda ISO/IEC 27001 glede izvedbe ocene tveganja.
- Predstaviti možne praktične rešitve s pomočjo primernega programskega orodja.
- Opozoriti na možne probleme, na katere lahko naletimo pri izvedbi ocene tveganja.

# Zakaj vzpostaviti SUVI?

- Zagotoviti:

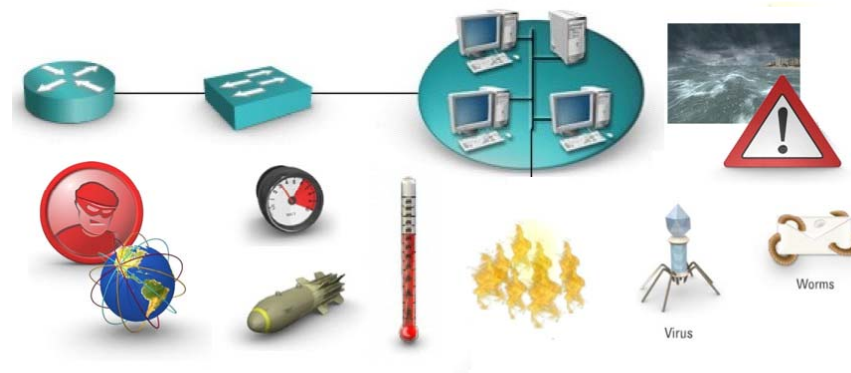


Zaupnost

Celovitost

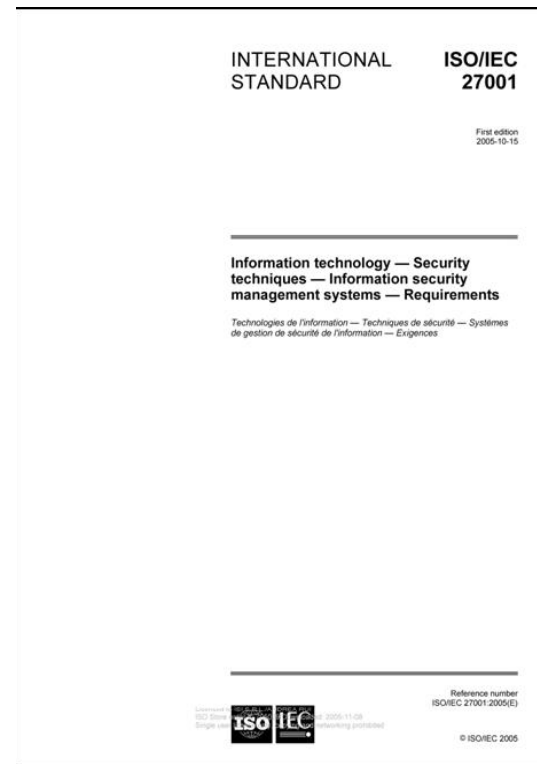
Razpoložljivost

- Zmanjšati tveganja:



# Modeli vzpostavitve SUVI

- Obstaja veliko različnih modelov vzpostavitve SUVI.
- Najbolj aktualen model je standard ISO/IEC 27001.



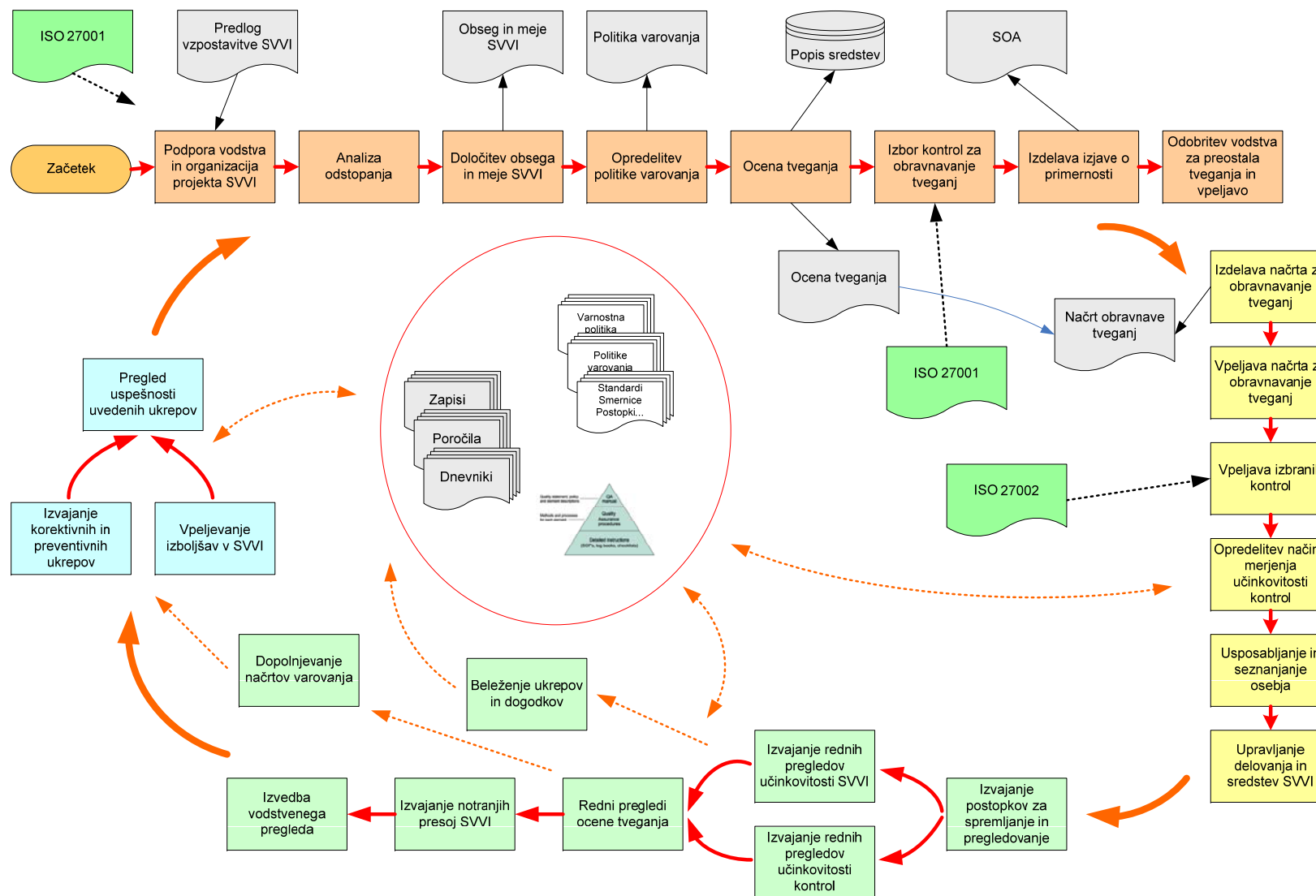
## Vzpostavitev SUVI

- Uspešna vzpostavitev SUVI:
  - izvesti veliko aktivnosti, ki si sledijo po fazah v duhu PDCA (Plan, Do, Check, Act).



- Princip PDCA je eden temeljnih principov SUVI.

# Potek vzpostavitve SUVI



## Ocena tveganja

- Ena od najbolj pomembnih, pa tudi zahtevnih in obsežnih aktivnosti pri vzpostavitvi SUVI, je izvedba ocene tveganja.



# Faze ocene tveganja

- Ocena tveganja obsega:
  - izbor metodologije,
  - izdelava popisa sredstev,
  - vrednotenje sredstev,
  - določitev groženj,
  - ocena vpliva in verjetnosti groženj,
  - ocena ranljivosti sredstva.





## Dodatne faze ocene tveganja

- Da bi lahko imeli korist od izvedene ocene tveganja, je potrebno izvesti še naslednje aktivnosti:
  - določiti način obravnave tveganj,
  - izbrati ustrezne kontrole za zmanjševanje tveganj,
  - pripraviti izjavo o uporabnosti (SOA),
  - izdelati načrt obravnave tveganj.



# Pristopi k izvedbi ocene tveganja

- Odločimo se lahko za različne pristope k izvedbi ocene tveganja:
  - enostavni pristop,
  - zelo podroben pristop,
  - kombinirani pristop.



# Metodologija ocenjevanja tveganj

- Izbrana metodologija mora zagotoviti, da bodo izvedene ocene tveganja dale primerljive rezultate.

Ranjivost	Vrednost																									
		1					2					3					4					5				
Vpliv																										
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

## Orodje za podporo izvedbi ocene tveganja

- Izkazalo se je za primerno in smiselno, da uporabimo ustrezno programsko orodje.
- Na razpolago imamo veliko število primernih programskih orodij za podporo ocene tveganja.



# Orodje za podporo izvedbi ocene tveganja

- Programsko orodje mora omogočiti enostavno in učinkovito obravnavo vseh informacij o tveganjih.

Analiza: kvalidat Prijavljen: admin (Odjava)

**INFO.RM**

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

Informacije

▼ Informacijski sistem

- Komunikacijska oprema
- Mediji
- Navodila in postopki
- Papirnata dokumentacija
- Podatkovne baze in datoteke
- Programska oprema
- Sistemska dokumentacija
- Strojna oprema**
- Uporabniški priročniki

► Oprema in infrastruktura

► Osebe

► Test\_Skupina

► Zunanje storitve in preskrba

Popis sredstev

▼ Prikaži vsa sredstva + Dodaj sredstvo Uvoz sredstev

Sredstvo	Ident	Lokacija	Lastnik	Uredi
Dlančniki	sn	Celotno podjetje	Skupina / Zaposleni	<a href="#">Uredi</a>
Monitorji	inventarna št.	Pisarne zaposleni	Splošni sektor / Informatika/Administ	<a href="#">Uredi</a>
Optični čitalnik	sn	Administracija/Recepcija	Administracija / Recepcija/Vodja	<a href="#">Uredi</a>
Periferne enote	sn	Pisarne zaposleni	Skupina / Vodje enot	<a href="#">Uredi</a>
Prenosniki (vodstvo)	sn	Pisarne vodstvo	Vodstvo / Direktor	<a href="#">Uredi</a>
Prenosniki (zaposleni)	inventarna št.	Pisarne zaposleni	Skupina / Vodje enot	<a href="#">Uredi</a>
Računalniki namizni (vodstvo)	inventarna št.	Pisarne vodstvo	Vodstvo / Direktor	<a href="#">Uredi</a>
Računalniki namizni (zaposleni)	inventarna št.	Pisarne zaposleni	Skupina / Vodje enot	<a href="#">Uredi</a>
Strežnik datotečni	ime (Datko)	Sistemske prostor	Splošni sektor / Informatika/Administ	<a href="#">Uredi</a>
Strežnik domenski	ime (Domen)	Sistemske prostor	Splošni sektor / Informatika/Administ	<a href="#">Uredi</a>
Strežnik poštni	ime (Golob)	Sistemske prostor	Splošni sektor / Informatika/Administ	<a href="#">Uredi</a>
Tiskalnik (laserski barvni)	sn	Administracija/Glavna pisarna	Administracija / Glavna pisarna/Glavna	<a href="#">Uredi</a>
Tiskalnik (mrežni)	sn	Administracija/Glavna pisarna	Splošni sektor / Informatika/Administ	<a href="#">Uredi</a>
Tiskalniki (lokalni)	sn	Pisarne zaposleni	Skupina / Vodje enot	<a href="#">Uredi</a>

Stran 1 od 1 30 Pogled 1 - 15 od 15

# Uporaba programskega orodja za oceno tveganja

- Popis sredstev

- Prednosti

- Ločene ocene tveganj po posameznih procesih. Posamezno sredstvo ima lahko za različne lastnike procesov različne vrednosti.
    - Razvrstitev sredstev v skupine sredstev omogoča večjo preglednost in enostavno obravnavo sredstev istega tipa (podobne grožnje, podobni ukrepi)

- Možnosti

- Z izvozom sredstev v datoteke formata .csv lahko izdelamo različne preglede sredstev po različnih atributih (lastnik, proces, skupina, lokacija, vrednost ... )
    - Možna je izdelava vnaprej pripravljenega nabora (template) sredstev, ki običajno nastopajo znotraj določenega poslovnega procesa, tipičnega za neko panogo. Vključevanje takih v naprej pripravljenih naborov nam lahko močno pohitri izdelavo popisa sredstev.

# Uporaba programskega orodja za oceno tveganja

- **Vrednotenje sredstev**

- Določimo vrednost sredstva glede na različne kriterije. Sami lahko definiramo ustrezne kriterije, ki so za nas pomembni pri določanju vrednosti sredstva. Pri vrednotenju sredstva lahko upoštevamo enega ali več kriterijev.
- Poleg običajnih kriterijev (celovitost, razpoložljivost, zaupnost) lahko tako upoštevamo kriterije, kot so to na primer:
  - finančne izgube
  - zmanjšanje učinkovitosti
  - prekinitve poslovanja
  - zakonske kršitve
  - zahteve regulative
  - ugled organizacije
  - varnost osebja
  - poslovni interesi
  - osebni podatki
  - družba in okolje
  - izguba naklonjenosti
  - javni red in mir

# Uporaba programskega orodja za oceno tveganja

- Določitev groženj

Analiza: Analiza 3GEN 2010 Prijavljen: sys04 (Odjava)

**INFO.RM**

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

Informacije

▼ Informacijski sistem

- Komunikacijska oprema
- Mediji**
- Navodila in postopki
- Papirnata dokumentacija
- Podatkovne baze in datoteke
- Programska oprema
- Sistemska dokumentacija
- Strojna oprema
- Uporabniški priročniki

► Oprema in infrastruktura

► Osebjje

► Zunanje storitve in preskrba

Ocena tveganja: Informacijski sistem / Mediji

📄 Prikaži vsa sredstva 📄 Izvoz v csv

Sredstvo	Ident	Lokacija	Lastnik	Vrednost sred	Stopnja tvega	Uredi
Podatkovne kasete	--	Langusova	Sistemska služba / Operativa/Oper	zelo visoka	7,5	🔗
Prenosni mediji (DVD/CD, USB ključ)	--	3GEN/Pisar Skupina / Zaposleni		visoka	6,1	🔗
Prenosni mediji (papir)	--	3GEN/Pisar Skupina / Sistemski administrator		srednja	5,9	🔗

Stran 1 od 1 30 Pogled 1 - 3 od 3



# Uporaba programskega orodja za oceno tveganja

- Ocena vpliva in verjetnosti posameznih groženj ter ranljivosti sredstva.

**INFO.RM** Analiza: Analiza 3GEN 2010 Prijavljen: sys04 (Odjava)

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

Ocena tveganja za: Podatkovne kasete

Stopnja tveganja: 7,5

Grožnja: Človeške\_napake  
Mediji: Izguba podatkovnih medijev med prenosom  
Vpliv: nepomembna  
Verjetnost: nepomembna  
Ranljivost: nepomembna

Grožnja	Vrednost	Vpliv	Verjetnost	Ranljivost	Tveganje	
Človeške_napake / Mediji: Izguba podatkovnih medijev med prenosom	zelo visoka	zelo visoka	srednja	nizka	7,1	<a href="#">Odstrani</a>
Človeške_napake / Oprema: Uničenje opreme ali podatkov zaradi malomarnosti	zelo visoka	zelo visoka	srednja	nizka	7,1	<a href="#">Odstrani</a>
Organizacijske_napake / Mediji: Neučinkovito uničenje podatkovnih medijev	zelo visoka	zelo visoka	srednja	visoka	8,2	<a href="#">Odstrani</a>

© 2010 KVALI.DAT d.o.o.

# Uporaba programskega orodja za oceno tveganja

- Določitev načina obravnave tveganj
  - Določitev največjega še sprejemljivega nivoja tveganja, ki omogoča obvladljivo število vseh kombinacij sredstvo / grožnja.
  - Avtomatična določitev statusa “dopuščanje tveganja” za tista sredstva, ki imajo nivo tveganja manjši od največjega še sprejemljivega nivoja.
  - Preostalim kombinacijam sredstvo / grožnja določimo načine obravnave s pomočjo programskega orodja.



Način obravnave: Informacijski sistem / Programska oprema						
Prikaži vsa sredstva <input checked="" type="checkbox"/> Prikaži "Dopuščanje tveganja" <input checked="" type="checkbox"/> Izvoz v csv						
Sredstvo	Grožnja	Vrednost	Tveganje	Obravnava tveganja	Ured	
Operacijski sistemi - strežniki	Organizacijske_napake / Dokumentacija: Neobstajanje ali nepopoln	zelo visoka	6,5	Zmanjševanje tveganja		
Operacijski sistemi - strežniki	Organizacijske_napake / Dokumentacija: Pomanjkljiva ali nepopoln	zelo visoka	7,1	Zmanjševanje tveganja		
Zunanja aplikativna programska oprema	Namerna_dejanja / Nepooblaščen: Uporaba računalniškega	srednja	6,5	Zmanjševanje tveganja		
Računovodski program	Splošne_grožnje / Osebj: Izguba osebj	visoka	6,5	Izogibanje tveganju		
Operacijski sistemi - strežniki	Človeške_napake / Osebj: Nepravilno administriranje dostop	zelo visoka	7,1	Izogibanje tveganju		
Računovodski program	Človeške_napake / Osebj: Prenos nepravilnih ali neželenih p	visoka	6,5	Izogibanje tveganju		
Operacijski sistemi - strežniki	Organizacijske_napake / Postopki: Neustrezno načrtovanje ni	zelo visoka	7,1	Zmanjševanje tveganja		

# Uporaba programskega orodja za oceno tveganja

- Izbor kontrol za obravnavo tveganj
  - Na pregleden in enostaven način izberemo ustrezno kontrolo iz vnaprej definiranega nabora kontrol. Za posamezno kombinacijo sredstvo / grožnja lahko izberemo eno ali več kontrol.



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

**Izbor kontrol za zmanjševanje tveganja**

Sredstvo	Grožnja	Lastnik	Lokacija	Vrednost	Tveganje
Arhivska knjižnica (NAS)	Organizacijske_napake / Arhiviranje: Neučinkovita revizija postopkov za arhiviranje	Sistemska služba / Basic System	Langusova/Sistemska soba	 zelo visoka	 6,5

**Kontrola**

**# Izbrane kontrole:**

1.	A.14.1.1 Vključevanje varovanja informacij v proces neprekinjenega poslovanja	 <a href="#">Odstrani</a>
2.	A.14.1.5 Testiranje, vzdrževanje in ponovno ocenjevanje načrtov za neprekinjeno poslovanje	 <a href="#">Odstrani</a>

# Uporaba programskega orodja za oceno tveganja

- **Priprava izjave o uporabnosti (SOA)**
- Vsaka organizacija, ki želi uskladiti svoj sistem z zahtevami standarda ISO/IEC 27001 mora pripraviti Izjavo o uporabnosti (SOA), ki predstavlja povzetek odločitev v zvezi z obravnavo tveganja. Programsko orodje omogoča enostavno izdelavo relativno zelo kompleksnega dokumenta, saj pri pripravi dokumenta avtomatično uporabi relevantne podatke iz predhodnih faz.
- S programskim orodjem določimo status izbrane kontrole, definiramo razloge za izbor kontrole in navedemo dokumente, ki opisujejo način vpeljave izbrane kontrole. V kolikor kontrole nismo izbrali, moramo definirati razloge za opustitev. Obrazložitev opustitve kontrole zagotavlja, da nobena kontrola ni bila izpuščena zaradi nepazljivosti.

# Uporaba programskega orodja za oceno tveganja

**INFO.RM**

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

- ▶ A.5 Varnostna politika
- ▶ A.6 Organizacija varovanja informacij
- ▼ **A.7 Upravljanje sredstev**
  - A.7.1 Odgovornost za sredstva
  - A.7.2 Klasifikacija informacij
- ▶ A.8 Varovanje človeških virov
- ▶ A.9 Fizična zaščita in zaščita okolja
- ▶ A.10 Upravljanje s komunikacijami in s produkcijo
- ▶ A.11 Nadzor dostopa
- ▶ A.12 Nakup, razvoj in vzdrževanje informacijskih sistemov
- ▶ A.13 Upravljanje incidentov pri varovanju informacij
- ▶ A.14 Upravljanje neprekinjenega poslovanja
- ▶ A.15 Združljivost

**SOA**

Izvoz v csv

Kontrola	Status	RS	PZ	DP	OT	Uredi
A.7.1.1 Popis sredstev	že vpeljana	DA	-	-	0	
A.7.1.2 Lastništvo sredstev	že vpeljana	DA	-	-	0	
A.7.1.3 Sprejemljiva uporaba sredstev	že vpeljana	-	-	DA	1	

Stran 1 od 1 30 Pogled 1 - 3 od 3

**RS** - Regulatorna, standardi **PZ** - Pogodbene zahteve **DP** - Dobra praksa **OT** - Ocena tveganja

## Uporaba programskega orodja za oceno tveganja

- Izdelava načrta obravnave tveganj
- Programsko orodje nam omogoča izdelavo načrta za obravnavo tveganja, ki določa ustrezne ukrepe za vpeljavo izbranih kontrol, sredstva, odgovornosti in prednostne naloge za upravljanje tveganj pri varovanju informacij.
- Ko izvedemo ukrepe, lahko s programskim orodjem izračunamo novo vrednost tveganja, kar je osnova za naslednjo izvedbo ocene tveganja.

## Uporaba programskega orodja za oceno tveganja

- Ostale prednosti in možnosti:
  - možnost sodelovanja vseh vključenih oseb, saj lahko tudi lastniki sredstev ali procesov izvedejo oceno za svoj del,
  - enostavnost uporabe tudi v primerih, ko se odločimo za zelo podroben ali pa kombiniran pristop,
  - večja natančnost, saj lahko uporabimo lestvico z več stopnjami za ocenjevanje vrednosti sredstva, verjetnosti dogodka, vpliva grožnje in ranljivosti sredstva,
  - samodejno vodenje velike količine podatkov in podrobnosti,
  - možnost izdelave različnih izpisov in poročil,
  - izvoz podatkov in njihova uporaba v drugih aplikacijah.

## Zaključek

- Predstavili smo glavne zahteve glede izvedbe ocene tveganja.
- Predstavili smo glavne prednosti, ki nam jih prinaša uporaba namenskega programskega orodja, pa tudi slabosti in možnosti za naprej.
- Z uporabo orodja si lahko zelo poenostavimo delo in skrajšamo čas izvedbe ocene tveganja.
- Izvedemo lahko bolj natančno in poglobljeno analizo in definiramo takšne ukrepe, ki dejansko vodijo k izboljšanju SUVI.
- Za resno uporabo orodja kljub temu potrebujemo znanja s področja obvladovanja tveganj in informacijske varnosti.



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