

**Departman za
poslediplomske studije**

**INŽENJERSKI MENADŽMENT
MASTER STUDIJSKI PROGRAM**

Master rad

**ZAHTEVI STANDARDA ISO 27001 ZA BEZBEDNOST INFORMACIJA I
UPRAVLJANJA RIZIKOM PRIMENOM STANDARDA ISO 27000**

Mentor:

Prof.dr. Dragan Cvetković

Student:

Vuk Tatić

Br. indeksa: 411195/2012

Beograd, avgust 2013.godina

SADRŽAJ

Uvod	3
1. Metodologija naučnog istraživanja	6
1.1 Cilj istraživanja	6
1.2 Predmet istraživanja	6
1.3 Hipotetički okvir	6
1.4 Metode i tok istraživačkog procesa	6
1.5 Struktura rada	6
2. Uopšteno o standardu ISO 27001 i njegov značaj	7
2.1 Istorijat	7
2.2 Definicije i termini	8
2.3 Struktura serije standarda ISO 27001	10
2.4 Značaj standarda	12
3. Procesni pristup	14
3.1 PDCA model	14
4. Sistem menadžmenta bezbednošću informacija	15
4.1 Opšti zahtevi	15
4.1.2 Plan (Uspostavljanje ISMS-a)	15
4.1.3 Do (Implementacija i primena ISMS)	17
4.1.4 Check (Praćenje i preispitivanje ISMS-a)	18
4.1.5 Act (Održavanje i poboljšavanje ISMS-a)	19
5. Interne provere ISMS	19
6. Preispitivanje ISMS od strane rukovodstva	20
7. Poboljšavanje ISMS-a	21
8. Iskustva u primeni i praktični aspekti	21
9. Uopšteno o standardu ISO 27002	28
9.1 Istorijat	28
9.2 O Standardu ISO 27002	28
9.3 Definicije i termini	28
9.4 Struktura standarda	30
10. Upravljanje rizicima	31
10.1 Opšte	31
10.2 Priprema za procesa upravljanja rizikom	34
10.3 Identifikovanje opasnosti	13
10.4 Određivanje verovatnoće nastanka rizičnog događaja	35
10.5 Određivanje posledica nastanka opasnosti	

rizičnog događaja	35
10.6 Ocenjivanje rizika	35
10.7 Definisanje granica za prihvatanje rizika	35
10.8 Definisanje zaštitnih mera (kontrola)	36
10.9 Učinak delovanja zaštitnih mera	37
10.10 Uvođenje zaštitnih mera u svakodnevni rad	37
11. Kategorije sigurnosti	38
12. Politika sigurnosti informacije	38
13. Organizovanje sigurnosti informacija	40
13.1 Interno organizovanje	41
13.2 Eksterno organizovanje	41
14. Upravljanje imovinom	41
14.1 Odgovornost za imovinu	42
14.2 Klasifikovanje informacija	42
15. Sigurnost ljudskih resursa	42
15.1 Radnje koje prethode zapošljavanju	42
15.2 Obaveze u toku zaposlenja	42
15.3 Prestanak ili promena zaposlenja	43
16. Fizicka sigurnost ili sigurnost u okruženju	44
16.1 Sigurne oblasti	45
16.2 Sigurnost opreme	45
17. Upravljanje komunikacijama i radom	45
17.1 Radne procedure I odgovornosti	45
17.2 Upravljanje pružanjem usluge preko treće strane	45
17.3 Planiranje i prihvatanje sistema	45
17.4 Zaštita od malicioznog i mobilnog koda	46
17.5 Rezervne kopije	47
17.6 Upravljanje sigurnošću u mrežama	47
17.7 Postupanje sa medijumima	47
17.8 Razmena informacija	47
17.9 Usluge elektronske trgovine	47
17.10 Nadgledanje	48
18. Kontrola pristupa	48
18.1 Poslovni zahtevi za kontrolu pristupa	49
18.2 Upravljanje pristupom korisnika	49
18.3 Odgovornosti korisnika	49
18.4 Kontrola pristupa na mrežu	49
18.5 Kontrola pristupa operativnim sistemima	50
18.6 Kontrola pristupa aplikacijama i informacijama	50
18.7 Mobilno računarstvo i rad sa udaljenosti	50

19. Nabavka, razvoj i održavanje informacionih sistema	51
19.1 Zahtevi za sigurnost informacionih sistema	52
19.2 Ispravna u obrada u aplikacijama	53
19.3 Kriptografske kontrole	53
19.4 Sigurnost sistemskih datoteka	53
19.5 Sigurnost u procesima razvoja i podrške	53
19.6 Upravljanje tehničkim ranjivostima	53
20. Upravljanje incidentima narušavanja sigurnosti informacija	54
20.1 Izveštavanje o događajima u vezi sa sigurnošću Informacija i o slabostima	54
20.2 Upravljanje incidentima narušavanja sigurnosti informacija i poboljšanja	54
21. Upravljanje kontinuitetom poslovanja	55
21.1 Aspekti sigurnosti informacija kod upravljanja kontinuitetom poslovanja	55
22. Usklađenost	56
22.1 Usklađenost za zakonskim odredbama	57
22.2 Usklađenost sa politikama i standardima sigurnosti i tehnička usklađenost	57
22.3 Razmatranje provere informacionih sistema	57
23. Zaključak	57
Literatura	59

UVOD

Znanje, kao najznačajniji resurs svakog čoveka, pa i društva u celini, može se definisati kao „*Obim informacija, opažanja ili razumevanja koja poseduje neka osoba*“

Krajem dvadesetog veka, industrijski period razvoja tehnologija i mašina, zamenjen je razvojem informatičkih tehnologija koje u centar interesovanja stavljaju informacije kao izvor znanja. Nagli razvoj informacionih tehnologija izaziva velike promene u poslovanju svih činioca društva, pa se već početkom 21. veka savremena informatička rešenja koriste u svim društvenim procesima.

Informacije postaju dobro koje, kao i druga društvena dobra, imaju vrednost koju treba adekvatno zaštititi.

Imajući u vidu da je čuvanje znanja, resursa od suštinskog značaja za društvo, jasno je koliko je bezbednost informacija važna. U današnjim uslovima globalizacije tržišta, informacije posebno veliki značaj imaju u poslovnom svetu, često od raspoloživosti i tačnosti informacija zavisi opstanak na tržištu.

Britanski Institut za standardizaciju (BSI) je početkom devedesetih godina postavio osnovu za razvoj standarda za bezbednost informacija.

Prva verzija teksta ovog standarda BS 7799 se usvaja 1995. godine, a 1998. godine dobija svoju prvu zvaničnu reviziju. BSI nedugo po objavljivanju prvog, prateći brz razvoj interneta, objavljuje i drugi deo standarda BS 7799.

Zbog sve izraženijih potreba organizacija u svetu, razvoj ovog standarda podignut je na međunarodni nivo u okviru ISO (*International Organization for Standardization*).

Međunarodna organizacija za standardizaciju ISO prihvata BS standarde i u junu 2005. godine objavljuju drugu verziju standarda koja se zvala ISO 17799 Informacione tehnologije - bezbednost tehnike - Načela upravljanja bezbednošću informacija.

Standard ISO 27001 se objavljuje u oktobru 2005. godine pod nazivom Informacione tehnologije - Sistemi upravljanja bezbednošću informacija - Zahtevi.

Standard 27001 je posvećen bezbednosti informacija i specificira zahteve i daje okvir na koji način organizacija treba da pristupe zaštiti informacija.

Standard ISO 27001 je značajan za sve organizacije koje imaju potrebu za menadžment informacijama, bez obzira čime se bave, tj. da li posluju u oblasti informacionih tehnologija ili se bave proizvodnjom ili pružanjem usluga.

Međunarodna organizacija za standardizaciju ISO i Međunarodna elektrotehnička komisija IEC čine specijalizovani sistem svetske standardizacije. Radi delovanja u pojedinim oblastima tehničke aktivnosti, nacionalna tela koja su članovi ISO-a ili IEC-a, učestvuju u razvoju međunarodnih standarda preko tehničkih komiteta koje je osnovala odgovarajuća organizacija.

Kontrola se može definisati kao sredstvo za upravljanje rizikom, uključujući smernice, prakse, procedure ili organizacionu strukturu koja može biti tehničke, rukovodne, administrativne ili zakonske prirode.

1. METODOLOGIJA NAUČNOG ISTRAŽIVANJA

1.1. Cilj istraživanja

Cilj istraživanja je da se dokumentuje Sistem za bezbednost informacija jedne inženjering organizacije koja se bavi realizacijom investicionih projekata saglasno zahtevima standarda ISO 27001:2005, tako da se izrađena dokumentacija može primeniti za razvoj, implementaciju i sertifikaciju Sistema, kao i proučavanje i primena kontrola standarda ISO IEC 27002 u organizacijama i smanjenja rizika sa kojim se organizacija suočava na minimum.

1.2. Predmet istraživanja

Analiza i proučavanje zahteva standarda 27001:2005 u specifičnom poslovnom okruženju inženjering organizacije koja se odlikuje razuđenošću poslovnog sistema kroz postojanje matične organizacije i projekata. U takvom okruženju bezbednost informacija ima dodatne izazove, jer se mnoge aktivnosti obavljaju na privremenim lokacijama izvan matične organizacije - na gradilištima. U drugom delu rada predmet istraživanja su analiza i proučavanje kontrola standarda 27000 u raznim tipovima organizacija, gde bezbednost informacija ima dodatni izazov, s obzirom na različite delatnosti organizacija.

1.3. Hipotetički okvir

Opšta hipoteza: Moguće je uspostaviti bezbednost informacija u razuđenom poslovnom sistemu inženjering organizacije koji će zadovoljiti zahteve standarda ISO 27001:2005, kao i da je sa kontrolama koje se nalaze u standardu 27002 moguće svesti rizike na prihvatljiv nivo.

1.4 Metode i tok istraživačkog procesa

Imajući u obzir specifičnost i obim proučavanog predmeta istraživanja, u ovom radu će pored opštih segmenata standarda ISO 27001 biti prikazani i pojedini segmenti standarda ISO 27002 primenjeni u razuđenom poslovnom sistemu inženjering organizacije u matičnoj organizaciji i na gradilištima, kao i opšti segmenti standarda ISO 27002 i pojedinačne kontrole za snižavanje rizika za svaku logičku grupu kontrola.

1.5 Struktura rada

U prvom poglavlju je opisana metodologija i tok naučnog istraživanja. U drugom poglavlju je pisano uopšteno o standardu i njegovom značaju, opisan je istorijat, dati su termini i definicije i prikazana je struktura standarda. U trećem poglavlju je prikazak procesni pristup i PDCA model. U četvrtom poglavlju je opisan sistem menadžmenta bezbednošću informacija, gde su prikazani opšti zahtevi, uspostavljanje, implementacija, praćenje i preispitivanje i održavanje i poboljšavanje ISMS-a. U petom poglavlju opisane su interne provere ISMS-a, u šestom poboljšavanja, dok su u sedmom, koje je ujedno i poslednje poglavlje, prikazani praktični aspekti ovog standarda.

2. UOPŠTENO O STANDARDU ISO 27001 I NJEGOV ZNAČAJ

Standard ISO 27001 ima za cilj obezbeđenje poverljivosti, integriteta i dostupnosti informacija zainteresovanim i ovlašćenim stranama kroz postavljanje mehanizama - kontrola zaštite informacija.

U današnjoj eri informacionih tehnologija, informacija je postala lako dostupna, ali u isto vreme i veoma ugrožena. Informacija je dobro koje, kao i druga vredna poslovna dobra ima vrednost za organizaciju i potrebu da bude odgovarajuće zaštićena.

Danas, kada se gotovo kompletno poslovanje obavlja preko računarskih poslovnih sistema, bezbednost informacija postaje veoma važna. Zbog pretnji iz raznih izvora, zaštita informacija je neophodna.

U uslovima visoke konkurentnosti, pravovremena i prava informacija je novac, opstanak i prestiž na tržištu. Podatak koji je ažuran, pravovremeno dostavljen do korisnika postaje informacija.

Sa aspekta bezbednosti informacije uočavamo tri dimenzije: bezbednost podataka, bezbednost kanala distribucije podataka i bezbednost korišćenja informacije.

Bezbednost informacija čine sledeća tri elementa:

- ✓ Poverljivost: informacija nije dostupna neovlašćenim osobama, organizacijama i procesima, što se u velikom broju slučajeva stavlja u prvi plan;
- ✓ Integritet: zaštita tačnosti i kompletnosti informacije;
- ✓ Pristupačnost: omogućavanje pravovremene dostupnosti informacijama osobama sa ovlašćenjem i u vremenu kada je to potrebno na mestu gde je predviđeno.

Pretnje po bezbednost informacija dolaze i iznutra i spolja. Možemo ih podeliti u namerne i slučajne. Namerne su osmišljene akcije fokusirane na informacije, a slučajne su neplanirani upadi u sistem spolja i neadekvatno rukovanje informacijama od strane zaposlenih. Upravljanjem rizicima upravljamo bezbednošću informacija.

U pravcu ostvarenja bezbednosti informacija usvojen je standard ISO 27001. U standardu su specificirani zahtevi koje organizacija treba da ispuni da bi zaštitila informacije. Ovaj standard je primenjiv za sve tipove organizacija.

2.1 Istorijat

Krajem dvadesetog veka na poslovnu scenu veliki trag je ostavio nagli razvoj informacionih tehnologija.

Britanski Institut za standardizaciju (BSI) je početkom devedesetih godina postavio osnovu za razvoj standarda za bezbednost informacija. Zbog sve izraženijih zahteva organizacija u svetu, razvoj ovog standarda je značajno podstaknut .

Prva verzija teksta ovog standarda BS 7799 se usvaja 1995. godine, a 1998. godine dobija svoju prvu zvaničnu reviziju. BSI nedugo po objavljivanju prvog, prateći brz razvoj interneta, objavljuje i drugi deo standarda BS 7799.

Međunarodna organizacija za standardizaciju ISO prihvata ove standarde i u junu 2005. godine objavljuje drugu verziju standarda koja se zvala ISO 17799 Informacione tehnologije - bezbednost tehnike - Načela upravljanja bezbednošću informacija. Standard ISO 27001 se objavljuje u oktobru 2005. godine pod nazivom Informacione tehnologije - Sistemi upravljanja bezbednošću informacija - Zahtevi.

Standard ISO 27001 je značajan za sve organizacije koje se bave uslugama koje su povezane sa Informacionim tehnologijama i imaju potrebu za očuvanjem poverljivosti informacija.

2.2 Definicije i termini

U daljem tekst prikazani su termini i definicije koje se primenjuju u standardu ISO 27001.

✓ Imovina (*asset*)

Sve ono što ima vrednost za organizaciju.

[ISO/IEC 13335-1:2004]

✓ Raspoloživost (*availability*)

Svojstvo dostupnosti i upotrebljivosti na zahtev ovlašćenog entiteta.

[ISO/IEC 13335-1:2004]

✓ Poverljivost (*confidentiality*)

Svojstvo da informacija ne može biti dostupna ili vidljiva neovlašćenim osobama, entitetima ili procesima.

[ISO/IEC 13335-1:2004]

✓ Bezbednost informacija (*information security*)

Očuvanje integriteta, poverljivosti i raspoloživosti informacija. Druga svojstva su verodostojnost, pouzdanost, nadležnost i neporecivost.

[ISO/IEC 17799:2005]

- ✓ Događaj u vezi sa bezbednošću informacijama (*information security event*)

Pojava u sistemu, usluzi ili stanju na mreži koja ukazuje na moguće narušavanje politike bezbednosti informacija ili na otkaz zaštite ili situacija koja prethodno nije bila poznata i koja se može odnositi na bezbednost

[ISO/IEC TR 18044:2004]

- ✓ Incident narušavanja bezbednosti informacija (*information security incident*)

Jedan ili niz neočekivanih događaja u vezi sa bezbednošću informacija za koje postoje znatni izgledi da će kompromitovati poslovne aktivnosti i zapretiti bezbednosti informacija.

[ISO/IEC TR 18044:200

- ✓ Sistem menadžmenta bezbednošću informacija (*information security*

management system)

Deo ukupnog sistema menadžmenta, koji se zasniva na pristupu poslovnom riziku, uspostavljanje, implementiranje, primenjivanje, praćenje, preispitivanje, održavanje i poboljšavanje bezbednosti.

- ✓ Integritet (*integrity*)

Svojstvo zaštite ispravnosti i kompletnosti imovine.

[ISO/IEC 13335-1:2004]

- ✓ Preostali rizik (*residual risk*)

Rizik koji ostaje nakon postupanja sa rizikom.

[ISO/IEC Guide 73:2002]

- ✓ Prihvatanje rizika (*risk acceptance*)

Odluka da se rizik prihvati.

[ISO/IEC Guide 73:2002]

- ✓ Analiza rizika (*risk analysis*)

Sistematsko korišćenje informacija da bi se identifikovali izvori i procenio rizik.

[ISO/IEC Guide 73:2002]

✓ Ocenjivanje rizika (*risk assessment*)

Sveobuhvatni proces analize i vrednovanja rizika.

[ISO/IEC Guide 73:2002]

✓ Vrednovanje rizika (*risk evaluation*)

Proces upoređivanja procenjenog rizika u odnosu na kriterijume rizika kako bi se odredio značaj tog rizika.

[ISO/IEC Guide 73:2002]

✓ Menadžment rizikom (*risk management*)

Koordinisane aktivnosti usmeravanja i kontrolisanja u nekoj organizaciji u vezi sa rizicima.

[ISO/IEC Guide 73:2002]

✓ Postupanje sa rizikom (*risk treatment*)

Proces izbora i implementacije mera-kontrola kako bi se rizik modifikovao.

[ISO/IEC Guide 73:2002]

Napomena: U ovom standardu termin "kontrola" se koristi kao sinonim za "mera".

✓ Izjava o primenljivosti (*statement of applicability*)

Dokumentovana izjava koja opisuje ciljeve kontrola i kontrole koju su relevantne i primenjive na ISMS organizacije.

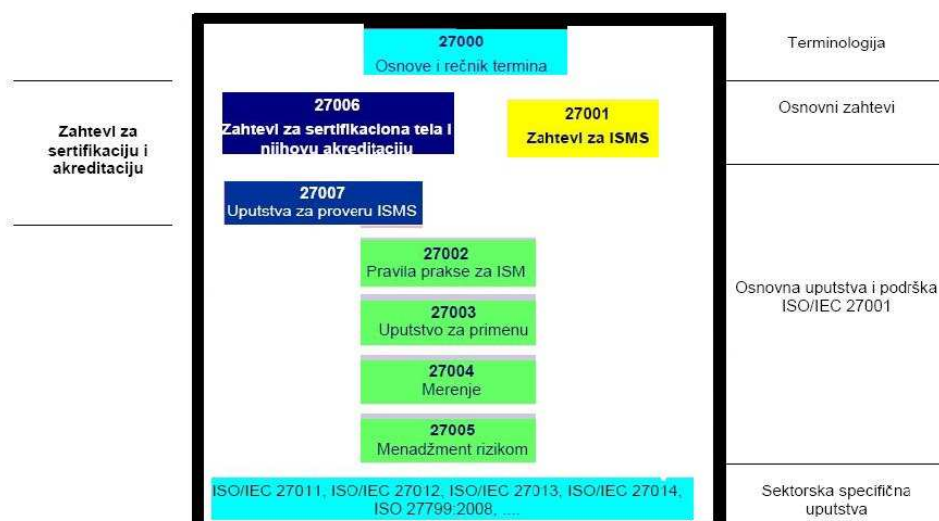
2.3 Struktura serije standarda ISO 27001

Međunarodna organizacija za standardizaciju (ISO) i Međunarodna elektrotehnička komisija (IEC) su osnovali zajednički tehnički komitet JTC1 u okviru koga radi stalni komitet SC 27 (ISO/IEC JTC1/SC 27 „IT Security Technique“) koji se bavi razvojem standarda u oblasti sigurnosti IT sistema. Ovaj komitet razvija seriju standarda ISO/IEC 27000.

Ovu seriju čine standardi:

- ✓ ISO/IEC 27000 ISMS - Osnove i rečnik pojmova
- ✓ ISO/IEC 27001 ISMS – zahtevi
- ✓ ISO/IEC 27002 - Kodeks postupaka za upravljanje sigurnosti informacija
- ✓ ISO/IEC 27003 - Uputstvo za implementaciju
- ✓ ISO/IEC 27004 - Merenja u menadžmentu sigurnosti informacija
- ✓ ISO/IEC 27005 - Menadžment rizika sigurnosti informacija

- ✓ ISO/IEC 27006 - Zahtevi za akreditaciju za sertifikaciona tela koja sertifikuju ISMS
- ✓ ISO/IEC 27007- Obezbeđuje uputstva za interne i eksterne provere ISMS
- ✓ ISO/IEC 27011 - Zahtevi za sektor telekomunikacija
- ✓ ISO 27799 - Bezbednosni zahtevi u zdravstvu korišćenjem standarda ISO/IEC 27002



Slika 1 Struktura serije standarda ISO 27000

Struktura standarda ISO 27001 sastavljena je iz 8 poglavlja:

- ✓ Poglavlje 1 ...
- ✓ Poglavlje 2 ...
- ✓ Poglavlje 3 ...
- ✓ Poglavlje 4: Sistem menadžmenta bezbednošću informacija (ISMS)
- ✓ Poglavlje 5: Odgovornost rukovodstva
- ✓ Poglavlje 6: Interna provera ISMS
- ✓ Poglavlje 7 : Preispitivanje ISMS od strane rukovodstva
- ✓ Poglavlje 8: Unapređenje ISMS.

Struktura standarda ISO 27001 tretira bezbednost informacija sa tri aspekta:

✓ Fizičkog: fizička kontrola pristupa, evidencija zaposlenih, zaštita radnih prostorija.

- ✓ Administrativnog: definiše jasna uputstva, politiku i procedure za stvaranje

informacija , njihovu distribuciju i čuvanje.

- ✓ Informatičkog: analizira i definiše performanse IT opreme, lozinke, prava pristupa, kriptovanje, protokole i politike sa aspekta pojave rizika po bezbednost podataka i informacija.

2.4 Značaj standarda

Standard ISO 27001 primenjuje se u različitim područjima u cilju razlikovanja mogućih procesa u organizaciji koji su povezani sa upravljanjem kontrole sigurnosti kao sto su: politika sigurnosti, sigurnost organizacije, kontrola i klasifikacija izvora, sigurnost osoblja, sigurnost materijalnih dobara i životne sredine, operativno upravljanje i komunikacija, kontrola pristupa, razvoj i održavanje raznih sistema i upravljanje kontinuitetom poslovanje.

Koristi i prednosti primene i sertifikacije ISMS-a mogu se podeliti u dva dela:

- ✓ Zaštita i bezbednost informacija i *know-how* organizacije, kroz sistematski

pristup za identifikovanje i borbu protiv niza potencijalnih rizika kojima je organizacija izložena. Upravljanje rizikom po bezbednost informacija, u mnogome se smanjuje verovatnoća pojave situacija koje nisu predviđene.

- ✓ Zaštita i bezbednost podataka i informacija klijenata sa kojima organizacija

dolazi u kontakt prilikom instaliranja opreme, izvođenja obuke, projektovanja i montaže itd. Posedovanjem sertifikata o implementiranom ISMS po zahtevima standarda ISO 27001, organizacija pruža klijentu dokaz da su njegove informacije i *know-how* bezbedni i zaštićeni od raznih zloupotreba. Takav sistem predstavlja kompetitivnu prednost organizacije u odnosu na konkurente.

Koristi i prednosti ISO 27001, koje primenom Sistema menadžmenta bezbednošću informacija (ISMS) i njegova sertifikacija saglasno zahtevima ISO 27001, donose organizaciji, mogu biti sledeće:

- ✓ *Just-in-time* efekat – prava informacija – na pravom mestu – u pravo vreme
- ✓ Zaštita i očuvanje kompanijskog *Know-How*-a
- ✓ Povećanje efektivnosti i efikasnosti Informacionog sistema
- ✓ Povećanje poslovnog kredibiliteta i poverenja od strane klijenata i partnera
- ✓ Prodor na zahtevno međunarodno tržište
- ✓ Mogućnost dugoročnog interesnog umrežavanja sa drugim kompanijama
- ✓ Ušteda vremena racionalizacijom količine i sadržine informacija

- ✓ Optimizacija resursa potrebnih za distribuciju i čuvanje podataka
- ✓ Rana identifikacija ranjivosti, pretnji i potencijalnih negativnih uticaja na

poslovanje

- ✓ Smanjenje rizika od zapošljavanja ljudi koji bi mogli naštetiti organizaciji
- ✓ Postizanje sinergetskog efekta timskog rada
- ✓ Usklađenost sa zakonskom regulativom
- ✓ Dostupnost klijentima kroz e-poslovanje
- ✓ Brži protok informacija između zaposlenih
- ✓ Stvaranje preduslova za delegiranje odgovornosti
- ✓ Smanjenje nesporazuma kod zaposlenih usled „ukrštanja informacija“
- ✓ Međunarodna verifikacija vaše dobre poslovne prakse
- ✓ Kod potencijalnih ili postojećih korisnika se stvara poverenje u informacioni

sistem u organizaciji čime se sa korisnicima ostvaruju poverljivije i čvršće relacije,

- ✓ Obezbeđuje se da organizacija ima potpuno komplementaran sistem sa

pravnom regulativom koja je vezana za informacione tokove jer se radi o standardu koji ima jasnu fleksibilnost u tom pravcu

- ✓ Obezbeđuje se sistem koji je usmeren na jasna kontinualna poboljšavanja procesa kojima se obezbeđuje informaciona sigurnost
- ✓ Ovim sistemom se ostvaruje transparentnost u pružanju usluga i menadžment na visokom nivou
- ✓ Obezbeđuje se i sistem koji je posebno orijentisan na upravljanje rizikom i kroz

upravljačke aktivnosti, smanjenje rizika na dozvoljenu i minimalnu meru

- ✓ Obezbeđuje se naprednije razumevanje informacionih tokova u organizaciji čime se ostvaruje značajna dobit i u delu razumevanja i poboljšavanja poslovnih procesa
- ✓ Ostvaruje se mehanizam za jasno vidljive i opipljive dokaze o smanjenju troškova kroz bolji menadžment rizikom i smanjenje značaja uzročnika grešaka u organizaciji
- ✓ Ostvaruje se bolja analiza troškovi/dobiti
- ✓ Ostvaruje se lakši proces monitoringa kroz smanjenje radnih napora i primenu

recimo sistema samo provere

- ✓ Moguće je povećati preventivno dejstvo kroz na primer smanjenje »uskih grla«

u mreži ili kroz analizu zaštićenih i sačuvanih ranijih podataka o procesima

- ✓ Smanjenje incidenata i bolje razumevanje uzročnika
- ✓ Razvija se svest zaposlenih u smislu značaja zaštite informacija
- ✓ Obezbeđuje se jasan protok i raspoloživost informacija i dr.

3. PROCESNI PRISTUP

Standard ISO 27001 usvaja procesni pristup za uspostavljanje, implementaciju, rad, praćenje, preispitivanje, održavanje i poboljšavanje ISMS-a u organizaciji.

Radi efektivnog funkcionisanja organizacija mora da upravlja mnogim aktivnostima . Skup aktivnosti koje koriste resurse i kojima se upravlja da bi se ostvarila transformacija ulaznih elemenata u izlazne može se nazvati procesom.

Procesni pristup se može okvalifikovati kao primena sistema procesa unutar organizacije, sa identifikacijom i međusobnim delovanjem procesa i menadžmentom njima.

3.1 PDCA model

Standard ISO 27001 razvijen je na bazi PDCA modela (planirati-uraditi-proveriti-delovati). ISMS procesi su struktuirani primenom PDCA modela.



Slika 2. ISO 27001 i PDCA model

Planirati(ustpostaviti ISMS) Planiranje (<i>Plan</i>) je opisano u tački 4.1.2	Uspostavljanje ISMS politike, ciljeva, procesa i procedura, koje su bitne za menadžment rizikom i poboljšanje bezbednosti informacija da bi bili postignuti rezultati u skladu sa ukupnom politikom i ciljevima organizacije.
Uraditi(implementirati i primenjivati ISMS) Uraditi (<i>Do</i>) je opisano u tački 4.1.3	Implementiranje i primenjivanje ISMS politike, procesa, procedura i kontrola.
Proveriti(pratiti i preispitivati ISMS) Proveriti (<i>Check</i>) je opisano u tački 4.1.4	Ocenjivanje i merenje performansi procesa u odnosu na politiku, ciljeve i iskustvo u praksi i izrada izveštaja koji se odnose na preispitivanje od strane rukovodstva.
Delovati (održavati i poboljšavati ISMS) Delovati (<i>Act</i>) je opisano u tački 4.1.5	Preduzimanje korektivnih i preventivnih mera, zasnovanih na rezultatima internih provera ISMS i preispitivanjima od strane rukovodstva ili drugim informacijama radi postizanja stalnog poboljšavanja ISMS-a.

4. SISTEM MENADŽMENTA BEZBEDNOŠĆU INFORMACIJA

4.1 Opšti zahtevi

Organizacija je dužna da uspostavi, implementira, primenjuje, prati, preispituje, održava i poboljšava dokumentovani ISMS u kontekstu svoje ukupne poslovne aktivnosti i rizika sa kojima se suočava. PDCA model se koristi za potrebe ovog standarda koji je prikazan na slici 2.

4.1.2. *Plan* (ustpostavljanje ISMS-a)

Organizacija je dužna da:

- ✓ Definiše područje primene ISMS-a u odnosu na delatnost organizacije i njenu

organizacionu strukturu, lokaciju, imovinu i tehnologiju.

Za inženjering organizaciju područje primene je u maticnoj organizaciji i na projektima u zemlji i inostranstvu.

- ✓ Definiše politiku ISMS-a u odnosu na karakteristike poslovanja, organizaciju, njenu lokaciju, tehnologiju i imovinu koja:
 - 1) je u okviru za postavljanje ciljeva i određivanja opšteg pravca i principa za aktivnosti u pogledu bezbednosti informacija.
 - 2) uzima u obzir poslovanje, zahteve i propise iz zakona i ugovorne obaveze koje se odnose na bezbednost.
 - 3) je usaglašena sa menadžmentom rizika u organizaciji u kojoj će uspostaviti i održavati ISMS.
 - 4) uspostavi kriterijume u odnosu na koje će se proceniti rizik

5) je odobrena od strane rukovodstva.

U prilogu 3 dat je primer izjave o politici ISMS-a u inženjering organizaciji

✓ Definiše ocenjivanje rizika u organizaciji:

- 1) Uspostavlja metodologiju ocenjivanja rizika koja odgovara ISMS-u i da identifikuje poslovnu bezbednost informacija, zahteve zakona i propisa.
- 2) Razvije kriterijume za prihvatanje rizika i identifikuje prihvatljive nivoe rizika.

U prilogu 1 je dat primer metodologije za ocenjivanje rizika i kriterijumi za njihovo prihvatanje.

✓ Identifikuje rizike.

- 1) Identifikuje imovinu unutar područja primene ISMS (imovinu organizacije) i vlasnike imovine
- 2) Identifikuje pretnje za tu imovinu
- 3) Identifikuje ranjivosti koje mogu nastati usled pretnji
- 4) Identifikuje uticaje koje gubitak poverljivosti, integriteta i raspoloživosti mogu imati na imovinu.

U prilogu 2 dat je primer popisa imovine u inženjering organizaciji.

✓ Analizira i procenjuje rizike

- 1) Ocenjuje poslovne uticaje na organizaciju koji mogu da proisteknu iz otkaza bezbednosti, imajući u vidu posledice gubitka poverljivosti, integriteta i raspoloživosti imovine.
- 2) Ocenjuje realnu verovatnoću pojave otkaza bezbednosti uzimajući u obzir preovlađujuće pretnje i ranjivosti, uticaje povezane sa tom imovinom i implementirane kontrole.
- 3) Proceni nivoe rizika
- 4) Odrediti kada su rizici prihvatljivi ili se zahteva postupanje sa njima tako što će se koristiti uspostavljeni kriterijumi za prihvatanje rizika.

✓ Identifikuje i proceni opcije za postupanje sa rizicima

Moguće mere obuhvataju:

- 1) Primenu odgovarajućih kontrola
- 2) Prihvatanje rizika objektivno i sa punim znanjem, obezbeđujući da oni jasno zadovoljavaju politiku organizacije i kriterijume za prihvatanje rizika
- 3) Izbegavanje rizika
- 4) Prenos pratećih rizika poslovanja na ostale učesnike npr. isporučioce.

- ✓ Izabere ciljeve kontrola i kontrole za postupanje sa rizicima

Ciljevi kontrola i kontrole moraju biti implementirani tako da ispune zahteve koji su identifikovani prilikom ocenjivanja rizika i postupanja sa rizikom. Prvenstveno se moraju uzeti u obzir kriterijumi za prihvatanje rizika, pa i zahtevi propisa, zakona i ugovora. Mogu se izabrati i dodatni ciljevi kontrola i kontrole.

- ✓ Dobiće odobrenje rukovodstva za predloženi preostali rizik
- ✓ Dobiće autorizaciju rukovodstva za implementaciju i primenu ISMS
- ✓ Primeni izjavu o primenljivosti.

U tabeli ispod je prikazan primer izjave o primenljivosti u inženjering organizaciji

- ✓ Izjava o primenljivosti mora biti pripremljena tako da obuhvati sledeće:

1) Ciljeve kontrola i kontrole

2) Ciljeve kontrola i kontrole koji su već implementirani

Izjava o primenljivosti je skup odluka koje se odnose na postupanje sa rizikom. Ako se neka od kontrola izostavi mora se obezbediti opravdanje radi provere da nijedna kontrola nije nehotice izostavljena.

4.1.3. Do (Implementacija i primena ISMS)

Kod implementacije i primene ISMS organizacija je dužna da :

- ✓ Napravi plan postupanja sa rizikom u kojem su identifikovane odgovarajuće mere rukovodstva, resursi, odgovornosti i prioriteti za upravljanje rizicima po bezbednost informacija.
- ✓ Da implementira plan postupanja sa rizikom da bi se dostignu ciljevi kontrola, koji obuhvata razmatranje finansiranja i podelu uloga i odgovornosti
- ✓ Da uspostavi kontrole da bi se ispunili ciljevi kontrola.
- ✓ Definiše kako se meri efektivnost izabranih kontrola ili grupa, specificira kako se ta merenja koriste da bi se ocenila efektivnost kontrola i da bi se postigli uporedivi i ponovljivi rezultati.

Rukovodstvo i zaposleni određuju koliko dobro kontrole postižu planirane ciljeve kontrola pomoću merenja efektivnosti.

- ✓ Uspostavlja programe obuke i podizanja svesti
- ✓ Upravlja primenom ISMS-a

- ✓ Upravlja resursima za ISMS
- ✓ Uspostavlja procedure i kontrole koje su odgovarajuće za omogućavanje trenutnog otkrivanja događaja u vezi sa bezbednošću i odgovore na incidente narušavanja bezbednosti.

4.1.4 Check (Praćenje i preispitivanje ISMS-a)

Kod praćenja i preispitivanja ISMS organizacije je dužna da:

- ✓ Sprovede procedure za praćenje i preispitivanje i ostale kontrole zbog:
 - 1) brzog otkrivanja grešaka u rezultatima procesa
 - 2) brzog uočavanja pokušaja i uspešnih narušavanja bezbednosti i incidenata
 - 3) omogućava rukovodstvu da odredi da li se bezbednosne aktivnosti odvijaju kako se očekuje, koje su dodeljene ljudima ili one koje implementiraju informacione tehnologije.
 - 4) da pomaže u otkrivanju događaja u vezi sa bezbednošću i na osnovu toga, koristeći pokazatelje, sprečava incidente narušavanja bezbednosti.
 - 5) određuje da li su mere koje su preduzete za rešavanje narušavanja bezbednosti bile efektivne.
- ✓ Redovno preispituje efektivnost ISMS, uzimajući u obzir rezultate provera bezbednosti, incidente, rezultate merenja efektivnosti, predloge i povratne informacije od svih zainteresovanih strana.
- ✓ Meri efektivnost kontrola zbog verifikacije da su zahtevi za bezbednost ispunjeni.
- ✓ Preispituje ocenjivanje rizika u planiranim intervalima, preispituje preostali rizik i uočava prihvatljive nivoe rizika uzimajući u obzir promene koje se odnose na:
 - 1) organizacije
 - 2) tehnologije
 - 3) ciljeve poslovanja i procesa
 - 4) uočenih pretnji
 - 5) efektivnosti primenjenih kontrola
 - 6) spoljašnjih događaja: promene zakona i propisa, promenjene ugovorne obaveze i promene u društvu.
- ✓ Sprovodi interne provere ISMS-1 u planiranim intervalima.

- ✓ Preduzima redovno preispitivanje ISMS-a od strane rukovodstva da bi se obezbedilo da područje primene ostane odgovarajuće i da se uoče poboljšanja procesa ISMS-a.
- ✓ Ažurira planove bezbednosti uzimajući u obzir rezultate praćenja i preispitivanja.
- ✓ Zapisuje aktivnosti i događaje koji mogu imati uticaj na efektivnost ili performanse ISMS-a.

4.1.5 Act (Održavanje i poboljšavanje ISMS-a)

Da bi se održavao i poboljšavao ISMS organizacija je dužna da:

- ✓ Implementira i uoči poboljšanja u ISMS-u
- ✓ Preduzima odgovarajuće korektivne i preventivne mere i primenjuje znanja stečena iz sopstvenih iskustava i iz iskustava o bezbednosti drugih organizacija .
- ✓ Saopšti mere i poboljšanja svim zainteresovanim stranama onoliko detaljno koliko to odgovara okolnostima i ako je odgovarajuće, utvrđuje kako nastaviti te aktivnosti.
- ✓ Osigurava da poboljšavanja dostignu predviđene ciljeve

5. INTERNE PROVERE ISMS-a

Interne provere ISMS-a, organizacija mora da sprovodi u planiranim intervalima da bi odredila da li su ciljevi kontrola, kontrole, procesi i procedure ISMS-a :

- ✓ Usaglašeni sa zahtevima ovog međunarodnog standarda i odgovarajućih zakona ili propisa
- ✓ Usaglašeni sa identifikovanim zahtevima za bezbednost informacija
- ✓ Efektivno implementirani i održavani
- ✓ Izvedeni kako se očekuje

Program provere se planira razmatranjem statusa važnosti procesa i oblasti koje se proveravaju, kao i rezultata prethodnih provera. Definišu se kriterijumi provere, područje primene, učestalost i metode. Proverivači moraju biti objektivni i nepristrasni kod procesa provere i ne smeju proveravati sopstveni rad.

Odgovornosti i zahtevi za planiranje i izvođenje provera, kao i za izveštavanje o rezultatima i održavanju zapisa, definišu se u dokumentovanoj proceduri.

Rukovodstvo koje je odgovorno za oblast koja se proverava mora da osigura da će bez nepotrebnog odlaganja preduzeti mere za otklanjanje neusaglašenosti koje su utvrđene tokom provere.

6. PREISPITIVANJE ISMS OD STRANE RUKOVODSTVA

Rukovodstvo mora da preispituje ISMS organizacije u planiranim intervalima (najmanje jedanput godišnje), da bi se obezbedila njegova stalna pogodnost, adekvatnost i efektivnost. To preispitivanje mora da obuhvati proverene mogućnosti za poboljšavanje i potrebu za promenama ISMS-a, uključujući politiku bezbednosti informacija i ciljeve bezbednosti informacija. Rezultati preispitivanja moraju biti jasno dokumentovani i zapisi se moraju održavati. Definisani su ulazni i izlazni elementi preispitivanja.

Ulazni elementi preispitivanja moraju da sadrže:

- ✓ Rezultate provera ISMS-a i preispitivanja
- ✓ Reagovanje zainteresovanih strana
- ✓ Procedure, proizvode i tehnike koje mogu da se koriste u organizaciji za poboljšanje performansi i efektivnosti ISMS-a
- ✓ Status preventivnih i korektivnih mera
- ✓ Rezultate merenja efektivnosti
- ✓ Dodatne mere koje su proistekle iz prethodnih preispitivanja od strane rukovodstva
- ✓ Bilo koje izmene koje bi mogle uticati na ISMS
- ✓ Preporuke za poboljšanje

Izlazni elementi preispitivanja od strane rukovodstva moraju da sadrže sve aktivnosti i odluke koje se odnose na :

- ✓ Poboljšanje efektivnosti ISMS-a
- ✓ Ažuriranje ocenjivanja rizika i plana postupanja sa rizikom
- ✓ Izmene kontrola i procedura koje imaju uticaj na bezbednost informacija, kada je potrebno, radi reakcije na unutrašnje i spoljašnje događaje koji mogu uticati na ISMS, uključujući promene:

- 1) Zahteva poslovanja
- 2) Zahteva za bezbednost
- 3) Zahteva iz zakona i propisa
- 4) Ugovornih obaveza
- 5) Nivoa rizika i/ili kriterijuma za prihvatanje rizika

- ✓ Potrebne resurse
- ✓ Poboljšanje načina na koji se meri efektivnost kontrola

7. POBOLJŠAVANJE ISMS-a

7.1 Stalno poboljšavanje ISMS-a

Organizacija mora stalno da poboljšava efektivnost ISMS-a pomoću politike bezbednosti informacija, ciljeva bezbednosti informacija, rezultata provera, korektivnih i preventivnih mera i preispitivanja od strane rukovodstva.

Korektivne mere su mere koje organizacija mora da preduzima radi otklanjanja uzroka neusaglašenosti, i radi sprečavanja ponavljanja tih neusaglašenosti.

Dokumentovana procedura za korektivne mere mora da definiše zahteve za:

- ✓ Identifikovanja neusaglašenosti
- ✓ Određivanje uzroka neusaglašenosti
- ✓ Vrednovanje potrebe za merama koje će osigurati da se neusaglašenosti ne ponove
- ✓ Određivanje i sprovođenje potrebnih korektivnih mera
- ✓ Zapisivanje rezultata preduzetih mera
- ✓ Preispitivanje preduzetih korektivnih mera

Preventivne mere su mere koje organizacija sprovodi radi otklanjanja uzroka potencijalnih neusaglašenosti da bi se sprečilo njihovo pojavljivanje. Preuzete mere moraju da budu odgovarajuće uticaju potencijalnih problema. Dokumentovana procedura za preventivne mere mora da definiše zahteve za:

- ✓ Utvrđivanje potencijalnih neusaglašenosti i njihovih uzroka
- ✓ Vrednovanje potrebe za merom da bi se sprečilo pojavljivanje neusaglašenosti
- ✓ Određivanje i uspostavljanje potrebne preventivne mere
- ✓ Zapisivanje rezultate preduzete mere
- ✓ Preispitivanje preduzete preventivne mere

Organizacija mora da identifikuje izmene rizika i identifikuje zahteve za preventivne mere usredsređujući pažnju na značajno izmenjene rizike. Prioritet preventivnih mera se određuje na osnovu rezultata ocenjivanja rizika.

8. ISKUSTVA U PRIMENI I PRAKTIČKI ASPEKTI

Neki od primera praktičnih aspekata u inženjering organizaciji dati su u daljem tekstu:

- ✓ Pristup kadrovskim i drugim ličnim podacima mora biti restriktivan
- ✓ U slučaju novozaposlenog, promene radnog mesta ili napuštanja organizacije vrši se korekcija prava pristupa, njihova dodela, promena i/ili ukidanje.

- ✓ Kroz PKU i lične ugovore o radu treba utvrditi obavezu vezanu za bezbednost informacija
- ✓ Kroz ugovore sa trećom stranom treba uključiti NDA (*Non Disclosure Agreement*) klauzule, kao obavezu čuvanja i nesaopštavanja do kojih mogu doći (klijenti, servis, podizvođači, održavanje)
- ✓ U zaštićenim prostorima ni pod kojim uslovima ne smeju se ostavljati bez nadzora lica sa strane
- ✓ Kada se oprema ostavlja van nadzora treba predvideti tehničke i/ili organizacione mere *Screen Saver*, *Hard Lock*, zaključavanje prostorija itd.
- ✓ Obezbediti redovan back up informacija uključujući i dokumentaciju na projektima, kako tekuću tako i nakon završetka i isporuke projekata
- ✓ Sva oprema sa informacijama pri rashodovanju mora biti podvrgnuta postupku uklanjanja informacija koje se mogu zloupotrebiti, kroz low level formatiranje i sl.
- ✓ Treba biti veoma oprezan kada su u pitanju zlonamerni softveri - virusi i sl.
- ✓ Periodično preispitivanje prava pristupa i periodična promena lozinki
- ✓ Politika „praznog stola i praznog ekrana“ – sa stola treba ukloniti sve što nije potrebno za rad, sa ekrana računara ukloniti sve ikonice koje vode direktno ka nekim dokumentima koji su vezani za ponude i ugovore, planove realizacije i sl.
- ✓ Zaposleni koji zaduže laptop da potpišu odgovarajuću izjavu da su upoznati sa obavezama čuvanja informacija.

Prilog 1. Primer imovine u inženjering organizaciji

Br.	Mesto	Opis imovine	Vlasnik	Forma		Napomena
				Na papiru	Elektronska	
1. INFORMACIJE / PODACI						
	Sekretarijat direktora	Ulazna/izlazna pošta		+		
		Ulazni/izlazni faksovi			+	

		Arhiva ugovora (originali)		+	+	
		Opšta dokumentacija dir. i pom. dir.				
	Finansijski sektor	Finansijska dokumentacija		+	+	
	Komercijalni sektor	Komercijalna dokumentacija		+	+	
	Plan i analiza	Dokumentacija		+	+	
	Kadrovska služba	Osnivačka i opšta dokumentacija preduzeća		+	+	
		Kartoteka		+	+	
		Evidencija radnog vremena		+	+	
		Obračuni i evidencije rada i g.o.		+	+	
	PIP	Reference		+	+	
		Ponude		+	+	
		Razni podaci		+	+	
	Mašinski i elektro sektor	Kataloška dokumentacija		+	+	
		Kalkulacije za ponude		+	+	
		Podaci o realizaciji projekata		+	+	
2. FIZIČKA IMOVINA						
	2.1. Računarska oprema					
		Serveri				
		Komunikaciona oprema (kablovi, svičevi, ruteri, wireless antene i oprema)				
		Računari - desk-top				
		Računari - lap-top				
		I/O uređaji (štampači, skeneri itd)				
	2.2. Telekomunikaciona oprema					

		Telefonska centrala				
		Telefoni - fiksni				
		Telefoni - mobilni				
		Telefaks				
	2.3. Ostala oprema					
	2.4. Zgrade					
		Poslovna zgrada - Mihaila Pupina 12				
		Magacin i lim. radionica - Vuka Vrčevića b.b.				
3. SOFTVERSKA IMOVINA						
	3.1. Sistemski i aplikativni softver					
		<u>Serveri:</u> - Windows Server 2008, - - Exchange, - Antivirus, - TMG - server, - DSM - server, - SQL, - Baze podataka				
		<u>Računari:</u> - OS - Windows 7, Windows XP, - aplikativni softver (Office, AutoCAD, Adobe, MS Project, Primavera, specijalistički programi)				
	3.2. Utilities					
		- Mrežni alati				
4. SERVISI						
	4.1. Računarski servisi					
		Servis za autentifikaciju korisnika (AD)				
		Servis za autentifikaciju računara (DHCP, DNS)				
		E-mail servis				
		Internet servis				

		FTP - servis				
		File - server				
		IIS - servis (EPOQ)				
		OWA (Outlook Web Access)				
	4.2. Telekomunikacioni servis					
		Telefonija - fiksna				
		Telefonija - mobilna				
	4.3. Opšte usluge					
		Električna energija (iz lokalne trafostanice) - osvetljenje i napajanje el. uređaja				
		Električna energija (UPS) - za napajanje servera				
		Električna energija (havarijsko napajanje - dizel generator) - selektivno: osvetljenje i napajanje el. uređaja				
		Grejanje, ventilacija i klimatizacija (opšte za zgradu)				
		Grejanje i klimatizacija (za prostoriju sa serverima)				
5. LJUDI I NJIHOVE KVALIFIKACIJE, VEŠTINE ISKUSTVA						
6. NEMATERIJALNA IMOVINA						
		Poslovna reputacija				
		Imidž				

Prilog 2 primer metodologije za ocenjivanje rizika i kriterijumi za njihovo prihvatanje.

Tabela 1: Vrednost informacione imovine (A)

	Opis	A
1.	Vrlo visoka	5
2.	Visoka	4
3.	Srednja	3
4.	Umerena	2
5.	Niska	1

Tabela 2: Verovatnoća nastajanja neželjenog događaja (P)

	Opis	P
1	Izuzetno čest događaj (više puta mesečno)	5
2	Velika verovatnoća – prilično čest događaj (jednom mesečno)	4
3	Moguć događaj – čest događaj (jednom u 6 meseci)	3
4	Mala verovatnoća - redak događaj (jednom godišnje)	2
5	Ekstremno mala verovatnoća – ekstremno redak događaj (jednom u 3 godine)	1

Tabela 3: Uticaj po bezbednost informacija (I)

	Opis	I
1	Veliki uticaj - veoma ozbiljne posledice	4
2	Srednji uticaj - znatne posledice	3
3	Mali uticaj - male posledice	2
4	Veoma mali uticaj - zanemarljive posledice	1

$$NR = A * P * I$$

Tabela 4: Nivo rizika (NR)

P	I	NR=A*P*I				
		A=1	A=2	A=3	A=4	A=5
5	4	20	40	60	80	100
4	4	16	32	48	64	80
5	3	15	30	45	60	75
4	3	12	24	36	48	60
3	4	12	24	36	48	60
5	2	10	20	30	40	50
3	3	9	18	27	36	45
4	2	8	16	24	32	40
2	4	8	16	24	32	40
3	2	6	12	18	24	30
2	3	6	12	18	24	30
5	1	5	10	15	20	25
4	1	4	8	12	16	20
2	2	4	8	12	16	20
1	4	4	8	12	16	20
3	1	3	6	9	12	15
1	3	3	6	9	12	15
2	1	2	4	6	8	10
1	2	2	4	6	8	10
1	1	1	2	3	4	5

Prilog 3. Primer izjave o politici IMS-a u inženjering organizaciji

ENERGOPROJEKT

ENTEL a.d.



IZJAVA O POLITICI IMS

Energoprojekt-Entel (ENTEL) opredeljen je da stalno unapređuje svoje poslovanje kako bi obezbedio da ga njegovi tradicionalni i novi naručioci stalno rangiraju među vrhunske svetske organizacije koje se bave projektovanjem i konsultantskim uslugama u oblastima energetike, vodoprivrede, telekomunikacija, zaštite životne sredine i upravljanja projektima. U tom cilju ENTEL uspostavlja i unapređuje sopstveni integrisani sistem menadžmenta (IMS) koji obuhvata menadžment kvalitetom (usaglašen sa ISO 9001:2008), menadžment zaštitom životne sredine (usaglašen sa ISO 14001:2004), menadžment bezbednošću i zdravljem na radu (usaglašen sa OHSAS 18001:2007), energetske menadžment (usaglašen sa ISO 50001:2011) i menadžment bezbednošću informacija (usaglašen sa ISO 27001:2005). Svoj integrisani sistem menadžmenta ENTEL stavlja u funkciju stalnog nastojanja da u svom poslovanju što potpunije, efikasnije, efektivnije i pouzdanije zadovoljava zahteve, potrebe i očekivanja, kako naručilaca svojih proizvoda, tako i svih zaposlenih, poslovnog sistema Energoprojekt, vlasnika, isporučilaca, šire društvene zajednice i države.

Sve svoje poslovne aktivnosti ENTEL usklađuje sa primenljivim zahtevima zakonske regulative u oblasti zaštite životne sredine, bezbednosti i zdravlja na radu, energetske efikasnosti i bezbednosti informacija, utvrđuje programe zaštite životne sredine, bezbednosti i zdravlja na radu, energetske efikasnosti i bezbednosti informacija i angažuje se na njihovom doslednom sprovođenju – kroz projektna rešenja, specifikacije za nabavku opreme i materijala i metode realizacije projekata ugrađujemo tehničko-tehnološka rešenja koja sprečavaju ili minimizuju zagađenje životne sredine, odnosno rizike po bezbednost i zdravlje ljudi i bezbednost opreme, postrojenja i informacija i vode računa o primeni energetske efikasne proizvoda, identifikujemo, analiziramo i vrednujemo rizike u oblastima zaštite životne sredine, bezbednosti i zdravlja ljudi, bezbednosti opreme, postrojenja i informacija, odnosno energetske efikasnosti prema uspostavljenim kriterijumima i pomažemo našim klijentima u procesu usaglašavanja sa zakonskom regulativom u ovim oblastima.

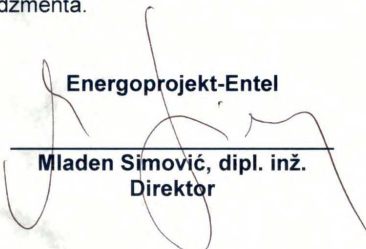
Najviše rukovodstvo ENTEL-a organizuje i stalno prati, preispituje i usmerava aktivnosti svih organizacionih delova, službi i pojedinaca kako bi ova politika IMS bila u potpunosti ostvarivana na svakom poslu. U tom smislu, obaveza najvišeg rukovodstva je da svi zaposleni budu potpuno upoznati sa utvrđenom politikom, da jasno prepoznaju svoje zadatke i odgovornosti na ostvarivanju te politike kroz svakodnevne aktivnosti, da im obezbedi raspoloživost informacija i resursa i da ih maksimalno motiviše za stalno postizanje njenih ciljeva.

Utvrđena politika IMS u okviru ENTEL-a predmet je stalnog preispitivanja od strane najvišeg rukovodstva, koje je obavezno da tu politiku neprekidno usavršava i blagovremeno prilagođava svim nastalim promenama u poslovnom i društvenom okruženju, kao i da tako usavršenu i prilagođenu politiku IMS efikasno sprovodi uz pomoć integrisanog sistema menadžmenta.

U Beogradu, 30. septembra 2012.

Izdanje 3; K-

Energoprojekt-Entel


Mladen Simović, dipl. inž.
Direktor

9. UOPŠTENO O STANDARDU ISO 27002

9.1 Istorijat

ISO/IEC 27002 je nastao iz standarda BS779 90-tih godina prošlog veka. Standard BS779 je objavila BSI grupa (British Standards Institutions) 1995. godine. Kao međunarodni standard prihvaćen je 2000. godine pod imenom ISO 17799, a revidiran je 2005. godine. 2007 godine promenjen je u ISO/IEC 27002, kako bi se uskladio sa ostalim standardima iz serije 27000.

9.2 O Standardu ISO 27002

Standard ISO 27002 prikazuje više od sto potencijalnih kontrola i kontrolnih mehanizama koji se, u skladu sa uputstvima, mogu uspostaviti unutar ISO 27001. Kontrole su namenjene za rešavanje specifičnih zahteva koji su identifikovani preko formalne procene rizika. ISO 27002 nije upravljački standard i po njemu se ne može sertifikovati. Pod upravljačkim standardom se podrazumeva da se njime određuje način upravljanja sistemom, kao što je u standardu ISO 27001 upravljanje sistemom bezbednosti informacija (ISMS). Kontrole u standardu ISO 27002 imaju iste nazive kao i one u 27001, samo što je razlika u količini detalja.

Primer 1. Razlika u količini detalja između ISO 27002 i 27001

ISO 27001	A.6.1.8	Nezavisno preispitivanje sigurnosti informacija	1 rečenica
ISO 27002	6.1.8	Nezavisno preispitivanje sigurnosti informacija	1 strana

U prethodnoj tabeli vidimo da je u standardu ISO 27001 kontrola opisana samo u jednoj rečenici, dok je u standardu ISO 27002 opisana na jednoj strani. Standard ISO 27002 ne razlikuje sigurnosne mere prema primenljivosti u određenoj organizaciji, dok 27001 propisuje da se mora sprovesti procena rizika kako bi se utvrdilo da li je neka mera potrebna za umanjivanje rizika. Mere koje su navedene u aneksu A standarda ISO 27001 ne bi bilo moguće sprovesti bez detalja koji su u standardu ISO 27002.

9.3 Definicije i termini

U daljem tekstu biće prikazani termini i definicije koje su zastupljene u standardu ISO 27001.

✓ **Kontrola** (control)

Sredstvo za upravljanje rizikom, uključujući politike, procedure, smernice, prakse ili organizacionu strukturu koja može biti administrativne, tehničke, rukovodne ili zakonske prirode

✓ **Imovina** (asset)

Sve ono što za određenu organizaciju ima neku vrednost.

✓ **Uputstvo** (guideline)

Opis koji pojašnjava šta i kako bi trebalo uraditi da bi se ostvarili ciljevi postavljeni u politikama

✓ **Sredstva za obradu informacija** (information processing facilities)

Svaki sistem za obradu informacija, usluga ili infrastruktura, ili fizičke lokacije u kojima su oni smešteni

✓ **Sigurnost informacija** (information security)

Očuvanje poverljivosti, celovitosti i raspoloživosti informacija: pored toga mogu takođe biti obuhvaćena i druga svojstva, kao što su verodostojnost, nadležnost, neporečivost i pouzdanost

✓ **Događaj u vezi sa sigurnošću informacija** (informational security event)

Događaj u vezi sa sigurnošću informacija predstavlja svaka identifikovana pojava u sistemu, usluzi ili stanju na mreži koja ukazuje na moguće narušavanje politike sigurnosti ili otkaz zaštite, ili situacija koja prethodno nije bila poznata i koja se može odnositi na sigurnost.

✓ **Incident narušavanja sigurnosti informacija** (information security incident)

Na incident narušavanja sigurnosti informacija ukazuje pojedinačni i neželjeni ili neočekivani događaj narušavanja sigurnosti informacija ili niz takvih događaja za koje postoje znatni izgledi da će kompromitovati poslovne aktivnosti i zapretiti sigurnosti informacija.

✓ **Politika** (policy)

Ukupne namere i pravac, onakve kakve ih je formalno iskazao menadžment.

✓ **Rizik** (risk)

Kombinacija verovatnoće nastanka nekog događaja i njegovih posledica Efekat neizvesnosti u odnosu na ciljeve.

✓ **Analiza rizika** (risk analysis)

Sistematsko korišćenje informacija da bi se identifikovali izvori i proceio rizik

✓ **Ocenjivanje rizika** (risk assessment)

Sveobuhvatni proces analize i vrednovanja rizika

✓ **Vrednovanje rizika** (risk evaluation)

Proces upoređivanja procenjenih rizika u odnosu na kriterijume rizika, kako bi se odredio značaj tog rizika

✓ **Upravljanje rizicima** (risk management)

Koordinirane aktivnosti usmeravanja i kontolisanja u nekoj organizaciji u vezi sa rizicima.

✓ **Razmatranje rizika** (risk treatment)

Proces izbora i implementacije mera da bi se rizik modifikovao

✓ **Treća strana** (third party)

Osoba ili telo koje su nezavisno priznale strane koje su angažovane na predmetu o kojem se radi

✓ **Pretnja** (threat)

Potencijalni uzrok nekog neželjenog incidenta koji može dovesti do štete na sistemu ili organizaciji

✓ **Ranjivost** (vulnerability)

Slabost neke imovine ili grupe dobara koju neka pretnja može da iskoristi

2.4 Struktura standarda

Standard 27002 sadrži 11 tačaka o sigurnosnim kontrolama koje zajedno sadrže 39 glavnih kategorija sigurnosti i jednu uvodnu tačku kojom se uvode ocenjivanje i postupanje sa rizicima.

Svaka tačka sadrži više glavnih kategorija sigurnosti. Navedenih 11 tačaka su:

- ✓ Politika sigurnosti
- ✓ Organizovanje sigurnosti informacija
- ✓ Upravljanje imovinom
- ✓ Sigurnost ljudskih resursa
- ✓ Fizička sigurnost i sigurnost okruženja
- ✓ Upravljanje komunikacijama i radom
- ✓ Kontrola pristupa
- ✓ Nabavka, izrada i održavanje informacionih sistema
- ✓ Upravljanje incidentima narušavanja sigurnosti
- ✓ Upravljanje kontinuitetom poslovanja
- ✓ Usklađenost

Svaka glavna kategorija sigurnosti sadrži:

- ✓ Cilj kontrole kojim se navodi ono što treba ostvariti
- ✓ Jednu ili više kontrola koje se mogu primeniti kako bi se cilj kontrole ostvario

Opisi kontrola su klasifikovani na sledeći način:

- ✓ **Kontrola**
Definiše se specifičan izveštaj kontrole da bi se ispunio cilj kontrolisanja
- ✓ **Smernice za implementaciju**
Za podršku uspostavljanja određene kontrole i ispunjenja ciljeva te kontrole obezbeđuju se detaljnije informacije. Neke od ovih smernica možda neće biti pogodno u svim slučajevima, tako da će možda biti pogodniji neki drugi način implementacije te kontrole.
- ✓ **Ostale informacije**
Obezbeđuju se dalje informacije koje mogu biti uzete u obzir, kao što su na primer pravni aspekti i pozivanja na druge standarde.

10. UPRAVLJANJE RIZICIMA

10.1 Opšte

Upravljanje rizicima je proces sistematske indentifikacije rizika, analiza i ocena njihovih uticaja i izrada i realizacija kompleksnih rešenja za upravljanje njima. Koncept upravljanja rizicima je našao siroku primenu u raznim sferama ljudske delatnosti, tako i u upravljanju bezbednošću informacija.

Termin „rizik“ je uveo američki ekonomista Frenk Najt 1921. godine i on označava onu neodređenost koja se kvantitativno može izmeriti. Termin rizik ima više različitih značenja, kao što su:

- ✓ Verovatnoća nastanka štete ili gubitka, opasnost
- ✓ Faktor, elemenat ili bilo šta u čemu je sadržana neizvesna opasnost
- ✓ Verovatnoća gubitaka ili povreda, podvrgaivanje -izlaganje opasnostima

Veza između pojmova „rizik“ i „pretnja“ sastoji se u tome što je rizik kombinacija pretnje i ranjivog mesta informacionog sistema.

Pretnja bez ranjivog mesta, kao i ranjivo mesto bez pretnje ne daju rizik. Jedna od glavnih osobina koja karakteriše rizik je pojava gubitka i postojanje verovatnoće i realizacije pretnje.

Temelj upravljanja rizicima čine:

- ✓ Predviđanja koji sve rizični događaji mogu nastati i kakve posledice ti događaji mogu imati
- ✓ Pokušaji da sprečimo nastanak rizičnih događaja jer oni izazivaju neželjene posledice
- ✓ Pokušaji da umanjimo posledice od nastajanja rizičnih događaja

Najveći problem kod upravljanja rizicima je taj što se mogućnost nastajanja i posledice rizičnih događaja ne mogu u potpunosti eliminisati, već se svode na prihvatljiv nivo.

Pošto se o rizicima govori uvek kada postoji mogućnost da se nešto dogodi ili ne dogodi, evidentno je da svaki rizik ima dve osnovne komponente:

- ✓ Jedna komponenta rizika je verovatnoća da se realizuje rizični događaj
- ✓ Druga komponenta rizika je težina posledica usled nastanka rizičnog događaja

Opis rizika sadrži:

- ✓ Izvor rizika (risk source) - objekat ili aktivnost (element) koji sam ili u kombinaciji sa drugim, ima potencijal /u stanju je/ ima mogućnost da izazovu rizik, da poveća rizik. Izvor rizika može biti materijalni ili nematerijalni.
- ✓ Događaj (event) - pojavljivanje ili promena niza specifičnih okolnosti/ uslova. Događaj može biti jedan ili ih može biti više (pojedinačni ili višestruki) i događaj može da ima jedan ili nekoliko uzroka. Događaj može biti određen ili neodređen. Događaj se može nazvati kao „incident“, „opasan događaj“ ili „nesrećni slučaj“. Događaj bez posledica može se nazvati kao „pretnja nastanku opasnog događaja“, „slučajno izbegnuto“, „pretnja incidentu“, „gotovo opasno ili štetno“, „skoro se dogodilo“, „pretnja nastanku havarijske situacije“.
- ✓ Posledica (consequence) - rezultat delovanja nekog događaja na ciljeve/ objekat.
- ✓ Verovatnoća nastanka rizičnog događaja

Što je verovatnoća nastanka rizičnog događaja veća, rizik je veći.

Za verovatnoću nastanka rizičnog događaja uvek se koristi broj koji ima vrednost između 0 (nemoguć događaj) i 1 (događaj koji će se sigurno realizovati).

- ✓ Posledice usled nastanka rizičnog događaja

Što su posledice usled nastanka rizičnog događaja teže, rizik je veći.

Posledice rizičnog događaja uvek izazivaju probleme u poslovanju.

Mernu jedinicu i vrednost za posledice nastanka rizičnih događaja prilično je teško odrediti.

Najlakše je ako je posledica nastajanja rizičnog događaja isključivo finansijske prirode, odnosno kada se može izraziti u nekoj valuti.

Veličina rizika bezbednosti informacija dobija se kao proizvod:

$$NR=A \cdot P \cdot I$$

A-Vrednost informacione imovine

	Opis	A
1.	Vrlo visoka	5
2.	Visoka	4
3.	Srednja	3
4.	Umerena	2
5.	Niska	1

Tabela 1. Vrednost informacione imovine

P-Verovatnoća nastajanja neželjenog događaja

	Opis	P
1.	Izuzetno čest događaj (više puta mesečno)	5
2.	Velika verovatnoća- prilično čest događaj (jedno mesečno)	4
3.	Moguć događaj-čest događaj (jednom u 6 meseci)	3
4.	Mala verovatnoća-redak događaj(jednom godišnje)	2
5.	Ekstremno mala verovatnoća-ekstremno redak događaj (jednom u tri godine)	1

Tabela 2. Verovatnoća nastajanja neželjenog događaja

I-Uticaj po bezbednosti informacija

	Opis	P
1.	Veliki uticaj- veoma ozbiljne posledice	4
2.	Srednji uticaj- znatne posledice	3
3.	Mali uticaj- male posledice	2
4.	Veoma mali uticaj – zanemarljive posledice	1

Tabela 3.Uticaj po bezbednosti informacija

P	I	NR=A*P*I				
		A=1	A=2	A=3	A=4	A=5
5	4	20	40	60	80	100
4	4	16	32	48	64	80
5	3	15	30	45	60	75
4	3	12	24	36	48	60
3	4	12	24	36	48	60
5	2	10	20	30	40	50
3	3	9	18	27	36	45
4	2	8	16	24	32	40
2	4	8	16	24	32	40
3	2	6	12	18	24	30
2	3	6	12	18	24	30
5	1	5	10	15	20	25
4	1	4	8	12	16	20
2	2	4	8	12	16	20
1	4	4	8	12	16	20
3	1	3	6	9	12	15
1	3	3	6	9	12	15
2	1	2	4	6	8	10
1	2	2	4	6	8	10
1	1	1	2	3	4	5

Tabela 4. Ocenjivanje rizika

10.2 Priprema za proces upravljanja rizikom

Pre početka upravljanje rizikom potrebno je pripremiti tim koji će sprovoditi ovaj proces, pri čemu posebnu pažnju treba obratiti na sastav tima (moraju biti pokriveni svi aspekti procesa/ aktivnosti u okviru kojih se želi upravljati rizikom).

Mora se sprovesti obuka i proveriti znanje koje poseduju članovi tima iz oblasti upravljanje rizikom.

Potrebno je precizno definisati:

Koji su to procesi/ aktivnosti u kojima se želi upravljati rizikom ? (Navesti procese i aktivnosti)

Koji su ciljevi koji treba da se ostvare realizacijom procesa/ aktivnosti ? (Navesti ciljeve)

10.3 Identifikovanje opasnosti

Prvi pravi korak u procesu upravljanja rizikom jeste identifikovanje opasnosti, odnosno pojava koje se mogu dogoditi i izazvati posledice po realizaciju neke aktivnosti/ procesa.

Koliko god se neko trudio da identifikuje sve opasnosti, uvek će se ispostaviti da postoje opasnosti koje nisu identifikovane. Stalno se javljaju nove opasnosti ili eskaliraju postojeće, pa se identifikovanje mora periodično ponavljati.

Važno je da se formira dokumentacija koja precizno opisuje koji su procesi/ aktivnosti ili pojave analizirani i koje opasnosti su identifikovane. Ovo je dragoceni izvor podataka pri kasnijem preispitivanju opasnosti.

10.4 Određivanje verovatnoće nastanka rizičnog događaja

Uporedo sa identifikovanjem opasnosti, potrebno je ustanoviti i verovatnoću nastupanja - nastanka opasnosti - rizičnog događaja.

Najbolje bi bilo ukoliko bi se za svaku opasnost odredila precizna verovatnoća njenog nastanka. Na žalost, ovo najčešće nije moguće, tako da se u tom slučaju pribegava kvalitativnoj proceni odgovarajuće verovatnoće.

Svaka organizacija mora za sebe da definiše model za određivanje verovatnoće nastanka opasnosti - rizičnog događaja (Tabela 2).

10.5 Određivanje posledica nastanka opasnosti - rizičnog događaja

Kada je proces identifikovanja opasnosti završen, potrebno je ustanoviti kakav uticaj svaka od identifikovanih opasnosti ima na definisane ciljeve sprovođenja postupka upravljanja rizikom, odnosno kakve su posledice tog uticaja. Potrebno je proveriti svaku kombinaciju "identifikovana opasnost – definisan cilj". Kao i sve prethodne aktivnosti, i ova aktivnost zahteva dokumentovanje svih rezultata, zbog potrebe naknadnog preispitivanja sistema upravljanja rizikom.

10.6 Ocenjivanje rizika

Vrši se ocenjivanje rizika (množenjem verovatnoće i posledica) i određuje se njihova prihvatljivost prema tabeli 4.

10.7 Definisanje granica za prihvatanje rizika

Kada je izvršeno ocenjivanje rizika potrebno je odrediti granice prihvatljivosti rizika.

Ocena za rizik (Verovatnoća x Težina) posledice	Nivo rizika	Prihvatljivost rizika	Delovanje na rizik
do 10	Mali	Prihvatljiv rizik	Ne primenjuju se zaštitne mere.
10 – 30	Umeren	Prihvatljiv rizik	Primenjuju se zaštitne mere u vidu nadzora - kontrolisanja.
preko 30	Visok	Neprihvatljiv rizik	Obavezno preduzimanje zaštitnih mera za ublažavanje rizika radi svođenja na prihvatljiv nivo.

Tabela 5. - Granice prihvatljivosti rizika

10.8 Definisanje zaštitnih mera (kontrola)

Kada je sve prethodno sprovedeno, sledeći korak je definisanje zaštitnih mera koje će umanjiti verovatnoću nastanka posledice od opasnog događaja ili umanjiti težinu posledice od nastanka opasnog događaja, i u takvoj meri da utvrđeni rizik pređe u oblast prihvatljivog rizika. Nekada ovo može da znači definisanje dve, tri, pa i više različitih zaštitnih mera, kako bi utvrđeni rizik postao prihvatljiv. Kod ovakvog pristupa se krije opasnost da uvođenje zaštitnih mera ne stvori uslove za pojavu novog, ranije neidentifikovanog rizika. Stoga je potrebno svaku zaštitnu meru dobro proučiti i proveriti da li ona može imati posledice po postavljene ciljeve. Prilikom definisanja zaštitne mere potrebno je koristiti iskustva drugih, kao i vršenje simulacija i praktičnih eksperimenata.

Aktivnosti i donete odluke se dokumentuju kada se završi definisanje zaštitnih mera, kojim su svi neprihvatljivi rizici prevedeni u prihvatljive. Dokumentovanje se primenjuje sa ciljem da se olakša posao kasnijeg preispitivanja rezultata primene zaštitnih mera i radi provere da li je došlo do promene nekih uslova ili eskalacije nekog opasnog događaja ili čak i pojave novih opasnih događaja.

Pri dokumentovanju zaštitnih mera, potrebno je navesti:

- ✓ Opasni događaj / posledicu na koji se odnosi zaštitna mera, ko je definisao i odobrio zaštitnu meru
- ✓ Opis definisane zaštitne mere (ko, šta, kada, kako, čime)
- ✓ Očekivano delovanje zaštitne mere na verovatnoću i težinu posledica opasnog događaja
- ✓ Očekivani novi, niži nivo verovatnoće i težine posledice posle primene zaštitne mere
- ✓ Podatke i pretpostavke na kojima je zasnovana primena zaštitne mere
- ✓ Način na koji će se proveravati uspešnost delovanja zaštitne mere, ko i u kojim intervalima.
- ✓ Podatke koji se zapisuju pri proveravanju delovanja zaštitne mere

10.9 Učinak delovanja zaštitnih mera

Učinak delovanje zaštitnih mera je različit i može se definisati pomoću koeficijenta delovanja zaštitnih mera čiji je primer dat u tabeli.

Delovanja zaštitne mere na rizik	Koeficijent delovanja	Opis situacije
Snažno	0,3	Zaštitna mera je odgovarajuća i primenjuje se.
Zadovoljavajuće	0,5	Zaštitna mera je uspostavljena, ima nedostataka, ali poboljšanja zaštitne mere nisu neophodna.
Nezadovoljavajuće	0,7	Zaštitna mera je uspostavljena, ali su potrebna značajna poboljšanja.
Simbolično	0,9	Zaštitna mera je neodgovarajuće, ima značajne nedostatke. Definirati i primeniti novu zaštitnu meru.

Tabela 6. - Učinak delovanja zaštitnih mera

Koeficijent delovanja se primenjuje za izračunavanje preostalog (rezidualnog) rizika na sledeći način:

$$R_r \text{ (rezidualni rizik)} = R_i \text{ (inherentni rizik)} \times K_d \text{ (koeficijent delovanja zaštitne mere)}$$

gde je

- R_r - Rezidualni rizik, vrednost rizika koji je preostao posle primene jedne ili više zaštitnih mera
- R_i - Inherentni rizik, izvorno utvrđena vrednost rizika bez delovanja bilo kakvih zaštitnih mera
- K_d - Koeficijent delovanja jedne ili više zaštitnih mera gde je $K_d = K_{d1} \times K_{d2} \times K_{dn}$
- K_{d1} do K_{dn} - Koeficijent delovanja prve, druge, n-te zaštitne mere

Ukoliko rezidualni rizik nije prihvatljiv mora se pristupiti definisanju i primeni zaštitnih mera sve dok rezidualni rizik ne postane prihvatljiv.

10.10 Uvođenje zaštitnih mera u svakodnevni rad

Kada je sve pripremljeno i dokumentovano, prelazi se na sledeći korak, koji spada u jedan od najtežih: uvođenje zaštitnih mera u upotrebu, njihova primena.

Ovo podrazumeva obuku svih izvršilaca za obavljanje svojih radnih aktivnosti na novi način, sa objašnjenjima zašto treba primeniti zaštitne mere.

Izvršiocima je potrebno objasniti šta je bio razlog za promenu načina rada i koji efekti se očekuju od novog načina rada. Kao i prilikom svake promene načina rada potrebno je praćenje da li izvršioci uredno primenjuju novi način rada ili rade u skladu sa starim navikama. Promene načina rada zahtevaju i promene u načinu razmišljanja zaposlenih, samim tim se menja i kultura unutar organizacije.

Kultura zasnovana na upravljanju rizikom podrazumeva svest o postojanju rizika i odlučivanje na osnovu rizika. Promena kulture podrazumeva da je svaki zaposleni upoznat sa svim identifikovanim opasnostima, nastankom mogućih posledica,

znacima koji pokazuju razvijanje opasnih događaja, kao i merama koje je potrebno preduzeti u tom slučaju.

U mnogim organizacijama koje su usvojile ovakav način razmišljanja, postalo je prihvatljivo da svaki radnik, čim uoči nastanak opasnog događaja, odmah zaustavi proces i obavesti odgovornu osobu. Zaustavljanje procesa sigurno predstavlja gubitak usled neostvarene proizvodnje/zarade, ali posledice dešavanja opasnog događaja uglavnom daleko prevazilaze taj gubitak i zato je razumljivo zašto je ovakav način razmišljanja poželjan.

11. KATEGORIJE SIGURNOSTI

Svaka glavna kategorija sigurnosti sadrži:

- ✓ Cilj kontrole kojim se navodi ono što treba ostvariti
- ✓ Jednu ili više kontrola koje se mogu primeniti kako bi se cilj kontrole ostvario

Opisi kontrola su klasifikovani na sledeći način:

- ✓ **Kontrola**
Definiše se specifičan izveštaj kontrole da bi se ispunio cilj kontrolisanja
- ✓ **Smernice za implementaciju**
Za podršku uspostavljanja određene kontrole i ispunjenja ciljeva te kontrole obezbeđuju se detaljnije informacije. Neke od ovih smernica možda neće biti pogodne u svim slučajevima, tako da će možda biti pogodniji neki drugi način implementacije te kontrole.
- ✓ **Ostale informacije**
Obezbeđuju se dalje informacije koje mogu biti uzete u obzir, kao što su na primer pravni aspekti i pozivanja na druge standarde.

12. POLITIKA SIGURNOSTI INFORMACIJE

Cilj politike sigurnosti informacija je da menadžment obezbedi podršku i usmerenje sigurnosti informacija koji su u skladu sa poslovnim zahtevima i odgovarajućim zakonima i propisima.

U skladu sa poslovnim ciljevima menadžment treba da uspostavi jasan pravac politike i da prikaže svoju podršku i privrženost sigurnosti informacija, kroz publikovanje i održavanje politike i sigurnosti informacija u celoj organizaciji.

Redni broj*: 12	Rizik:
Naziv kontrole: Politika sigurnosti informacija	Integritet informacija/zaštita od neovlašćenog pristupa i namernog ili slučajnog odavanja informacija
Aktivnosti u cilju snižavanja rizika: 1. Fizička zaštita informacija od neovlašćenog pristupa 2. Softverska zaštita pristupu informacijama/pravu pristupa 3. Evidencija zapisa o pristupu i manipulaciji informacijama	Aktivnosti u slučaju pojave incidenata: 1. U slučaju narušavanja fizičko tehničke zaštite, menjaju se brave/ključevi. 1. Promena pasvorda u slučaju ne namernog kompromitovanja informacija/ukidanja prava pristupa u ostalim slučajevima. 3. Pokretanje disciplinskog postupka u skladu sa statutom i Opštim aktima preduzeća.
Odgovoran za aktivnost: sistem administrator	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 7. - Primer kontrole za snižavanje rizika.

13. ORGANIZOVANJE SIGURNOSTI INFORMACIJA

Redni broj*: 13	Rizik:
Naziv kontrole: Politika sigurnosti informacija	Integritet informacija/zaštita od neovlašćenog pristupa i namernog ili slučajnog odavanja informacija
Aktivnosti u cilju snižavanja rizika: 1. Identifikuju se ciljevi sigurnosti informacija 2. Formuliše se, preispituje i odobrava politika sigurnosti informacija i preispituje se efektivnost implementirane politike sigurnosti informacija 3. Obezbeđuju se resursi koji su potrebni i dodeljuju specifične uloge i odgovornosti 4. Uključiti saradnju rukovodilaca korisnika, administratora, projekatara aplikacija, proveravača i osoblja obezbeđenja 5. Jasno se definišu oblasti za koje je svaki od pojedinaca odgovoran 6. Za nova sredstva dobiti odgovarajuću autorizaciju 7. Proveriti hardver i softver radi komatibilnosti sa ostalim komponentama 8. Uvesti neophodne kontrole kod korišćenja kućnih računara i laptopova 9. Napraviti sporazum o poverljivosti ili neotkrivanju 10. Definirati jasne uslove za zapošljavanje u kojima se odražava politika sigurnosti informacija 11. Uspostaviti procedure kada i ko kontaktira sa ovlašćenim telima 12. Pokrenuti nezavisno preispitivanje 13. Kada postoji potreba dozvoliti eksternoj strani pristup opremi za obradu informacija kako bi se identifikovali zahtevi za specifične kontrole 14. Pre davanja dozvole korisnicima za pristup bilo kojoj imovini organizacije uzeti u obzir ograničenja vezana za sigurnost. 14. Organizacija treba da obezbedi sebe u pogledu odštete od treće strane	Aktivnosti u slučaju pojave incidenata: 1. Preispitivanje odgovornosti i postupanje u skladu sa zakonskim i Opštim aktima preduzeća
Odgovoran za aktivnost: Menadzment	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 8. - Primer kontrole za snižavanje rizika.

13.1 Interno organizovanje

Cilj internog organizovanja je upravljanje sigurnošću informacija unutar oraganizacije. Treba uspostaviti okvire upravljanja kako bi se započela i kontrolisala implementacija sistema sigurnosti informacija unutar organizacije.

Menadžment treba da odobri politiku sigurnosti informacija, dodeli sigurnosne uloge i koordinira i preispituje implementaciju sigurnosti informacija unutar cele organizacije.

13.2 Eksterno organizovanje

Cilj je održati sigurnost informacija organizacije i opreme za obradu informacija kojima eksterne strane pristupaju, obrađuju ih, dostavljaju ili njima upravljaju.

Uvodjenje proizvoda ili usluga eksternih strana ne bi trebalo da umanja sigurnost informacija organizacije i opreme za obradu informacija. Svaki pristup eksternih strana opremi za obradu informacija, kao i obrada i razmena informacija sa eksternim stranama treba da budu kontrolisani.

Ocenjivanje rizika se sprovodi kako bi se odredile posledice po sigurnost i zahtevi za kontrolisanje kada postoji poslovna potreba za radom sa eksternim stranama koje mogu zahtevati pristupe informacijama i opremi za obradu informacija. Kada se neki proizvod ili usluga dobijaju od eksterne strane ili joj se obezbeđuju, takođe se sprovodi ocenjivanje rizika.

14. UPRAVLJANJE IMOVINOM

Redni broj*: 14	Rizik:
Naziv kontrole: Upravljanje imovinom	Otuđenje imovine
Aktivnosti u cilju snižavanja rizika: 1. Popisati imovinu i imenovati vlasnika 2. Dokumentovati vrednost imovine 3. Svi zaposleni, isporučioци i korisnici treće strane se pridržavaju pravila prihvatljivog korišćenja informacija i imovine	Aktivnosti u slučaju pojave incidenata: 1. Postupa se prema zakonskih odrednicama.
Odgovoran za aktivnost: Menadžment	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 9. - Primer kontrole za snižavanje rizika.

14.1 Odgovornost za imovinu

Cilj je ostvariti i održavati odgovarajuću zaštitu imovine organizacije. Sva imovina treba da bude popisana i da ima imenovanog vlasnika.

Za svu imovinu treba definisati vlasnike i dodeliti odgovornosti za održavanje odgovarajućih kontrola.

Implementaciju specifičnih kontrola vlasnik, po potrebi, može preneti na drugoga, ali ipak on ostaje odgovoran za odgovarajuću zaštitu imovine.

14.2 Klasifikovanje informacija

Cilj je osiguranje da će informacije dobiti odgovarajući nivo zaštite. Kako bi se ukazalo na potrebu, prioritete i očekivani stepen zaštite prilikom postupanja sa tim informacijama, informacije se moraju klasifikovati. Informacije imaju različite stepene osetljivosti i kritičnosti. Neki elementi mogu zahtevati dodatni stepen zaštite ili posebno postupanje. Šema za klasifikovanje informacija se primenjuje da bi se definisao odgovarajući skup nivoa zaštite i saopštila potreba za posebnim merama za postupanje.

15. SIGURNOST LJUDSKIH RESURSA

15.1 Radnje koje prethode zapošljavanju

Cilj je osiguranje da zaposleni, korisnici treće strane i isporučioци razumeju svoje odgovornosti, da su pogodni za svoje uloge i da se smanji rizik od prevare, krađe ili zloupotrebe opreme.

Odgovornosti u pogledu sigurnosti treba pre zapošljavanja naznačiti u adekvatnim opisima posla i u vidu uslova zapošljavanja. Posebno za osetljive poslove sve kandidate treba adekvatno proveriti. Zaposleni, isporučioци i korisnici opreme za obradu informacija treće strane treba da potpišu sporazum o njihovim ulogama i odgovornostima u pogledu sigurnosti.

15.2 Obaveze u toku zaposlenja

Cilj je osiguranje da svi zaposleni, isporučioци i korisnici treće strane budu upoznati sa pretnjama i brigom za sigurnost informacija, sa svojim odgovornostima, da budu opremljeni za podršku politici sigurnosti u organizaciji u toku svog normalnog rada, kao i da se smanji rizik od ljudske greške. Određene odgovornosti menadžmenta se definišu da bi se osiguralo da se sigurnost primenjuje u toku celog trajanja zaposlenja nekog pojedinca u organizaciji.

Svim zaposlenima, isporučioциma i korisnicima treće strane treba pružiti odgovarajući nivo upoznavanja i obuke o sigurnosnim procedurama i ispravnom korišćenju sredstava za obradu informacija kako bi se na minimum sveli mogući rizici po

sigurnost. Zvanični disciplinski postupak se uspostavlja onda kada dođe do narušavanja sigurnosti.

Redni broj*: 15.22	Rizik:
Naziv kontrole: Upoznavanje sa sigurnošću informacija, obrazovanje i obuka	Narušavanje sigurnosti
Aktivnosti u cilju snižavanja rizika:	Aktivnosti u slučaju pojave incidenata:
1. Svi zaposleni u organizaciji redovno dobijaju odgovarajuću obuku I redovno obnavljaju znanja o politici I procedrama u organizaciji koji odgovaraju njihovoj poslovnoj fuknkaciji., 2. U samom ugovoru o radu su takođe definisane osnovne obaveze zaposlenih po pitanju bezbednosti informacija. 3. Prilikom Ugovaranja poslova, druga Ugovorna strana mora biti upoznata sa svojim obavezama po pitanju bezbednosti informacija u toku trajanja i posle završetka projekta. Sa drugom ugovornom stranom se po pravilu potpisuje NDA sporazum ili se u samom ugovoru definišu pojedine klauzule koje se odnose na bezbednost. 4. Pre davanja pristupa informacijama ili uslugama započeti obuku upoznavanja sa zvaničnim postupkom podsticanja koji je projektovan radi uvođenja politika sigurnosti I očekivanja u samoj organizaciji.	1. Ukoliko zaposleni prekrši odredbe i pravila koja su propisana u Poslovniku i politici o bezbednosti informacija a tiču se bezbednosti informacija, direktor analizira težinu prekršaja, donosi mere radi ublažavanja nastanka eventualne štete po firmu, i po potrebi pokreće disciplinski postupak, koji osigurava ispravan I pošten postupan prema zaposlenima. Disciplinskim postupkom treba obezbediti stepenast pristup, čime se uzimaju u obzir činioici kao što su priroda I težina prekršaja I njegove posledice na poslovanje. 2. Ukoliko u toku rada na projektu druga ugovorna strana prekrši odredbe sporazuma (NDA ili ugovor) koje se tiču bezbednosti infromacija, direktor preduzima mere u cilju neutralisanja eventualno nastale štete i preduzima druge mere u cilju njene nadoknade (pregovori sa drugom ugovornom stranom, podnošenje tužbe...)
Odgovoran za aktivnost: Direktor	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 10. - Primer kontrole za snižavanje rizika

15.3 Prestanak ili promena zaposlenja

Cilj je osigurati da zaposleni, isporučioi ili korisnici treće strane odlaze iz organizacije ili menjaju radno mesto na propisan način.

Treba uspostaviti odgovornosti kako bi se osiguralo upravljanje odlaskom nekog zaposlenog, isporučioca ili korisnika treće strane iz organizacije, kao i da se vrate svi uređaji i ukinu sva prava na pristup. Promenom odgovornosti i zaposlenja unutar

organizacije treba upravljati kao da je to prestana zaposlenja i odgovarajućih odgovornosti u skladu sa ovim odeljkom, a svako novo zapošljavanje treba sprovoditi onako kako je to opisano u odeljku 8.1.

16. FIZIČKA SIGURNOST ILI SIGURNOST U OKRUŽENJU

Redni broj*: 16	Rizik:
Naziv kontrole: Fizička sigurnost ili sigurnost u okruženju	Otežan rad ili zastoj u poslovanju
Aktivnosti u cilju snižavanja rizika:	Aktivnosti u slučaju pojave incidenata:
1.Nabavka i montaža opreme za audio/video nadzor. 2.Kontrola pristupa poslovnoj zgradi 3.Oprema za obradu kritičnih podataka ili osetljivih informacija je smeštena u sigurnim oblastima,gde su sigurnosne zone razdvajanja jasno definisane 4.Postavlja se prijavnica sa osobljem,gde je pristup zgradi moguć samo ovlašćenim osobama 5.Sigurne oblasti zaštiti odgovarajućim kontrolama 6.Zapisivati datume ulaska/izlaska posetilaca i sve posetioce nadgledati 7.Projektovati i primeniti fizičku sigurnost za kancelarije,prostorije i sredstva gde se ključna oprema postavlja bez mogućnosti javnog pristupa 8.Projektovati i primeniti fizičku zaštitu od oštećenja usled požara, poplave, eksplozije,zemljotresa ili drugih oblika katastrofa 9.Tačke pristupa kao npr. utovar i isporuku ograničiti na identifikovano i ovlašćeno osoblje i izdvojeno od opreme za obradu informacija 10.Opremu zaštititi tako da se smanji rizik od opasnosti i pretnji iz okruženja. 11.Opremu održavati kako bi se osigurali neprekidna raspoloživost i integritet. 12.Popravke i servisiranje opreme treba da obavlja samo osoblje ovlašćeno za održavanje	1.Postupa se prema zakonskih odrednicama.
Odgovoran za aktivnost: Direktor	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 11. - Primer kontrole za snižavanje rizika

16.1 Sigurne oblasti

Cilj je sprečiti neovlašćeni fizički pristup, oštećenje i ometanje u prostorijama i na informacijama organizacije.

Oprema za obradu kritičnih ili osetljivih informacija treba da bude smeštena u sigurnim oblastima koje su zaštićene definisani sigurnosnim zonama razdvajanja, sa odgovarajućim sigurnosnim pregradama i kontrolama ulaska. Ona treba da bude fizički zaštićena od neovlašćenog pristupa, oštećenja i ometanja.

16.2 Sigurnost opreme

Cilj je sprečiti gubitak, oštećenje, krađu ili kompromitovanje imovine i prekid poslovanja organizacije.

Opremu treba zaštititi od fizičkih pretnji i pretnji iz okruženja. Zaštita opreme je neophodna kako bi se smanjio rizik od neovlašćenog pristupa informacijama i da bi se one zaštitile od gubitka i oštećenja. Mogu se zahtevati specijalne kontrole za zaštitu od fizičkih pretnji, kao i za odbranu sistema za podršku, kao što je električno napajanje i kablovska infrastruktura.

17. UPRAVLJANJE KOMUNIKACIJAMA I RADOM

17.1 Radne procedure i odgovornosti

Cilj je da se osigura ispravan i siguran rad sredstava za obradu informacija.

Treba uspostaviti odgovornosti i procedure za upravljanje i rad svih sredstava za obradu informacija. Ovo uključuje razvoj odgovarajućih radnih procedura. Treba implementirati razdvajanje dužnosti kada je to pogodno, kako bi se smanjio rizik od nemarnosti ili namerne zloupotrebe sistema.

17.2 Upravljanje pružanjem usluge preko treće strane

Cilj je implementacija i održavanje odgovarajućeg nivoa sigurnosti informacija i pružanja usluga u skladu sa sporazumima o pružanju usluge preko treće strane.

Organizacija treba da proverava implementaciju sporazuma, da nadgleda usklađenost sa sporazumima i da upravlja promenama kako bi osigurala da pružene usluge zadovoljavaju sve zahteve dogovorene sa trećom stranom.

17.3 Planiranje i prihvatanje sistema

Cilj je da rizik od otkaza sistema budem sveden na najmanju moguću meru.

Da bi se osigurala raspoloživost odgovarajućih kapaciteta i resursa za ostvarivanje zahtevanih performansi sistema, potrebni su prethodno planiranje i pripreme. Da bi se smanjio rizik od preopterećenja sistema, treba sagledati projekcije zahteva za kapacitete u budućnosti. Pre prihvatanja i korišćenja novih sistema treba uspostaviti zahteve za njihovu operativnost, treba ih dokumentovati i ispitati.

17.4 Zaštita od malicioznog i mobilnog koda

Cilj je zaštititi integritet softvera i informacija.

Potrebne su mere opreza kako bi se sprečilo i otkrilo uvođenje malicioznog koda i neautorizovanog mobilnog koda. Softver i sredstva za obradu informacija su ranjivi u odnosu na uvođenje malicioznog koda, kao što su računarski virusi, mrežni crvi, trojanski konji i logičke bombe. Korisnike treba upoznati sa opasnostima od malicioznog koda. Menadžment treba, onda kada to odgovara, da uvede kontrole za sprečavanje, otkrivanje i uklanjanje malicioznog koda, kao i da kontroliše mobilni kod.

Redni broj*: 17.4	Rizik:
Naziv kontrole: Zaštita od malicioznog koda	Narušavanje sigurnosti
Aktivnosti u cilju snižavanja rizika:	Aktivnosti u slučaju pojave incidenata:
1. Sistem administrator je zadužen da instalira i održava antivirus softver na svim klijentskim računarima i serverima. 2. Sistem administrator pokreće inicijativu za nabavku i/ili obnavljanje pretplate za antivirus softver i to slanjem e-maila direktoru u kome ga na vreme obaveštava o potrebnim merama 3. Sistem administrator je zadužen za administraciju anti vrus softvera i on proverava periodično update-ovanje baze antivirusnog softvera 4. Sistem administrator po potrebi instalira i administrira antispam softver na mail serveru	1. U slučaju nastanka štete upotrebom štetnog softvera, direktor preduzima mere da se nastala šteta umanjuje, daje nalog sistem administratoru da izvrši potrebne mere u cilju uklanjanja uzroka – virusa ili drugog štetnog virusa koji je izazvao štetu, skeniranje zaraženog računara ili svih računara. 2. Direktor zajedno sa sistem administratorom po potrebi preispituje i analizira sistem zaštite od virusa i ostalog štetnog softvera, i preduzima mere za njegovo unapređenje (dodatna administracija, zamena proizvođača antivirus softvera...)
Odgovoran za aktivnost: Sistem administrator	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 12. - Primer kontrole za snižavanje rizika

17.5 Rezervne kopije

Cilj je održanje integriteta i raspoloživosti informacija i sredstava za obradu informacija.

Treba uspostaviti rutinske procedure za implementiranje dogovorene politike i strategije čuvanja rezervnih kopija podataka i isprobavanja njihovog pravovremenog obnavljanja.

17.6 Upravljanje sigurnošću u mrežama

Cilj je osigurati zaštitu informacija u mrežama i zaštitu infrastrukture za podršku.

Sigurno upravljanje mrežama koje mogu da se protežu van granica organizacije zahteva pažljivo razmatranje tokova podataka, zakonskih posledica, nadgledanje i zaštitu. Da bi se zaštitili podaci koji prolaze kroz javne mreže, mogu biti potrebne dodatne kontrole.

17.7 Postupanje sa medijumima

Cilj je sprečiti neovlašćeno razotkrivanje, modifikovanje, ukljanjanje ili uništenje imovine i prekidanje poslovne aktivnosti.

Medijumi treba da se kontrolišu i da se fizički štite. Treba uspostaviti odgovarajuće radne procedure za zaštitu dokumenata, računarskih medijuma, ulazno izlaznih podataka i dokumentacije sistema od neovlašćenog razotkrivanja, modifikovanja, uklanjanja i uništenja.

17.8 Razmena informacija

Cilj je održati sigurnost informacija i softvera koji se razmenjuju unutar organizacije i sa bilo kojim eksternim entitetima.

Razmena informacija i softvera među organizacijama treba da se zasniva na zvaničnoj politici razmene koja se sprovodi u skladu sa sporazumima o razmeni i koja treba da bude u skladu sa odgovarajućim pravnim propisima. Treba uspostaviti procedure i standarde za zaštitu informacija i fizičkih medijuma koji su u tranzitu.

17.9 Usluge elektronske trgovine

Cilj je osigurati sigurnost u uslugama elektronske trgovine i njihovo sigurno korišćenje.

Treba uzeti u obzir posledice po sigurnost usluga u elektronskoj trgovini, uključujući direktne transakcije, kao i zahteve kontrole. Takođe treba uzeti u obzir integritet i raspoloživost informacija koje se elektronski objavljuju putem javno dostupnih sistema.

17.10 Nadgledanje

Cilj je otkriti neovlašćenje aktivnosti obrade informacija.

Sisteme treba nadgledati i treba zapisivati događaje u vezi sa sigurnošću. Da bi se osiguralo identifikovanje problema u informacionom sistemu, treba koristiti dnevnik operatera i zapisivanje neispravnosti. Nadgledanje sistema treba koristiti da bi se proverila efikasnost kontrola koje su usvojene i da bi se verifikovala usaglašenost sa modelom politike pristupa.

18. KONTROLA PRISTUPA

Redni broj*: 18. Kontrola pristupa	Rizik: Krađa intelektualne svojine uništenje intelektualne svojine
Aktivnosti u cilju snižavanja rizika: 1. Sistem administrator implementira i održava bazu korisnika i prava njihovih pristupa, na osnovu naloga koji mu izdaju rukovodstvo i/ili project manager-i pojedinih projekata 2. Za svakog zaposlenog kreira se jedinstveni korisnički nalog za pristup svom mail box-u, aplikaciji za project management, FTP serveru kao i repozitorijumu izvornog koda. Jedinstvena baza se održava kroz aplikaciju za project management. 3. Sistem administrator kreira, održava i ažurira listu prava pristupa za svakog zaposlenog u eDocumentus-u. Inicijalno, prilikom zapošljavanja novog radnika, lista prava pristupa popunjena samo sa pravom za pristupa e-mail, FTP serveru i testnom repozitorijumu izvornog koda 4. Prava pristupa u aplikaciji za project management se određuju prema sledećoj proceduri: kreiranje projekta je omogućeno rukovodstvu, kao i dodeljivanje project manager-a projektu. Project Manager kroz samu aplikaciju dodeljuje prava pristupa i nivoe prava za zaposlene koji rade na projektu. Project Manager daje nalog sistem administratoru da dodeli prava pristupa pojedinim zaposlenima repozitorijumu izvornog koda za taj	Aktivnosti u slučaju pojave incidenata: 1. U slučaju da se utvrdi da je došlo do neovlašćenog pristupa određenim resursima firme (mail box, repozitorijumu izvornog koda), sistem administrator obaveštava zamenika direktora o incidentu, momentalno preduzima mere da ukloni bezbednosni propust. Zamenik direktora, nakon razgovora sa sistem administratorom, nalaže neophodne mere za povećanje sigurnosti podataka (preispitivanje sistema prava pristupa, disciplinski postupak protiv odgovornih...)

projekat. PM je odgovoran za održavanje privilegija i prava pristupa za projekat kojim rukovodi.	
Odgovoran za aktivnost: Sistem administrator	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 13. - Primer kontrole za snižavanje rizika

18.1 Poslovni zahtevi za kontrolu pristupa

Cilj je kontrola pristupa informacijama.

Pristup informacijama, sredstvima za obradu informacija i poslovnim operacijama treba kontrolisati na osnovu poslovnih potreba i zahteva za sigurnost. Pravila za kontrolisanje pristupa treba da uzmu u obzir politike distribuiranja informacija i autorizovanja.

18.2 Upravljanje pristupom korisnika

Cilj je osiguranje pristupa ovlašćenim korisnicima i sprečavanje neovlašćenog pristupa informacionim sistemima.

Treba da postoje formalne procedure za kontrolu dodele prava za pristup informacionim sistemima i uslugama. Ove procedure treba da obuhvate sve faze životnog ciklusa pristupa korisnika.

18.3 Odgovornosti korisnika

Cilj je sprečiti pristup neovlašćenih korisnika i kompromitovanje ili krađu informacija i sredstava za obradu informacija.

Za efektivnu sigurnost osnovna je saradnja izmedju ovlašćenih korisnika. Korisnici trebaju da budu svesni svojih odgovornosti za održavanje efektivnosti kontola pristupa, posebno u pogledu korišćenja lozinki i sigurnosti korisnikovih uređaja. Treba implementirati politiku praznog stola ili praznog ekrana radi smanjenja rizika od neovlašćenog pristupa, gubljenja ili oštećenja papira, medijum i sredstava za obradu informacija.

18.4 Kontrola pristupa na mrežu

Cilj je da se spreči neovlašćeni pristup mrežnim uslugama.

Pristup uslugama treba kontrolisati i na internim i na eksternim mrežama. Da pristup korisnika na mrežu i mrežnim uslugama ne bi narušio sigurnost ovih usluga, neophodno je obezbediti sledeće:

- ✓ Odgovarajuće interfejsse izmedju sopstvene mreže u organizaciji i mreža čiji su vlasnici druge organizacije ili javnih mreža

- ✓ Odgovarajuće mehanizme za utvrđivanje verodostojnosti korisnika i uređaja
- ✓ Sprovođenje kontrole pristupa korisnika informacionim uslugama

Redni broj*: 18.4 Kontola pristupa na mrežu	Rizik: Krađa intelektualne svojine ,Uništenje intelektualne svojine
Aktivnosti u cilju snižavanja rizika: 1. Sistem administrator je odgovoran da održava, čuva, proverava i analizira logove pristupa e-mail serveru, FTP serveru, web serveru, pristupu fajlovima servera (SSH pristup) 2. Jedino sistem administrator može imati pristup logovima navedenim u tački 1 ovog mehanizma i može ih pokazati samo članovima rukovodstva na njihov zahtev 3. Sistem administrator je dužan da obezbedi da se loguju komande koje on izvršava na serveru. Pristup tim log informacijama je moguć i rukovodstvu firme 4. Log informacije se čuvaju za period od najmanje mesec dana 5. Greške sistema, kao i greške aplikacija se čuvaju u sistemskim i aplikativnim logovima. Sistem administrator povremeno prosleđuje log informacije iz aplikativnih logova Project Manager-ima koji su zaduženi za tu aplikaciju zbog analize poruka i grešaka. Project Manager obaveštava zamenika direktora o preduzetim akcijama u cilju sprečavanja pojavljivanja grešaka u logovima 6. Informacije koje su bitne za poslovanje firme (komercijalni uslovi ponuda, Ugovori, planovi poslovanja), čuvaju se na posebnim mestima kojima pristup imaju samo članovi rukovodstva	Aktivnosti u slučaju pojave incidenata: 1. Sistem administrator analizira logove, i u slučaju neovlašćenih pristupa ili akcija obaveštava zamenika direktora o tome 2. Zamenik direktora daje nalog sistem administratoru da otkloni bezbednosne propuste koje su doveli do neovlašćenog pristupa 3. Zamenik direktora po potrebi pokreće disciplinski postupak u skladu sa mehanizmom - Disciplinski postupak protiv zaposlenih ukoliko su neovlašćeno pristupali određenim informacijama
Odgovoran za aktivnost: Sistem administrator	Odgovoran za aktivnost: Zamenik direktora
Napomene:	Napomene:

Tabela 14. - Primer kontrole za snižavanje rizika

18.5 Kontrola pristupa operativnim sistemima

Cilj je da se spreči neovlašćeni pristup operativnim sistemima.

Za ograničavanje pristupa sistemu na ovlašćene korisnike treba da se koriste sredstva za sigurnost.

18.6 Kontrola pristupa aplikacijama i informacijama

Cilj je sprečiti neovlašćeni pristup informacijama koje su sadržane u aplikacijskim sistemima.

Sredstva za sigurnost treba koristiti za ograničavanje pristupa aplikacijskim sistemima, kao i unutar njih. Logički pristup aplikacijskom softveru i informacijama treba ograničiti na ovlašćene korisnike.

18.7 Mobilno računarstvo i rad sa udaljenosti

Cilj je da se osigura zaštita informacija prilikom korišćenja mobilnih računara i sredstava za rad sa udaljenosti.

Zaštita koja se zahteva treba da bude primerena rizicima do kojih dovodi ovakav način rada. Kada se koristi mobilni računar, u obzir treba uzeti rizike od rada u nezaštićenom okruženju i treba primeniti odgovarajuću zaštitu. U slučaju rada sa udaljenosti, organizacija treba da primeni zaštitu na udaljenom mestu i da osigura da se uspostave odgovarajući uslovi za ovakav način rada.

19. NABAVKA, RAZVOJ I ODRŽAVANJE INFORMACIONIH SISTEMA

Redni broj*: 19	Rizik:
Naziv kontrole: Nabavka, razvoj i održavanja informacionih sistema	Otežan rad ili zastoje u poslovanju, greške, gubitak, neovlašćene modifikacije i zloupotreba informacija.
Aktivnosti u cilju snižavanja rizika: 1. U specifikacijama zahteva za kontrole razmatraju se automatizovane kontrole koje se ugrađuju u informacioni sistem i potrebe za podršku ručnih kontrola 2. Zahteve sistema u pogledu sigurnosti informacija i procese za implementaciju sigurnosti integrisati u ranim fazama projektovanja informacionih sistema. 3. Kod kupovine proizvoda držati se formalnih	Aktivnosti u slučaju pojave incidenata

procesa ispitivanja i nabavke. 4.Sprovesti validaciju podataka koji se unose u aplikacije. 5.Sprovesti dvojnu proveru na ulazu ili druge ulazne provere, kao i proceduru za verodostojnost ulaznih podataka, kao i procedutre za odziv na greške. 6.Definisanje odgovornosti sveg osoblja 7.Oceniti rizik narušavanja sigurnosti radi utvrdjivanja da li se zahteva integritet poruka 8.Sprovoditi validaciju izlaznih podataka iz aplikacije 9.Izraditi politiku korišćena kriptografskih kontrola 10.Svi kriptografski ključevi treba da budu zaštićeni od modifikovanja,gubljenja i uništenja. Opremu za generisanje i arhiviranje ključeva treba fizički zaštititi. 11.Kontrolisati pristup sistemskim datotekama i izvornom programu. 12.Strogo kontrolisati okruženja projektovanja i podrške 13.Modifikacije na softverskim paketima ne podržavati, sve promene strogo kontrolisati. 14.Ograničiti rizik curenja informacija primenom i korišćenjem tajnih kanala 15.Postojanje kompletnog i ažurnog inventara imovine	
Odgovoran za aktivnost: Menadzment	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 15. - Primer kontrole za snižavanje rizika.

19.1 Zahtevi za sigurnost informacionih sistema

Cilj je da se obezbedi da sigurnost bude sastavni deo informacionih sistema.

Informacioni sistemi obuhvataju operativne sisteme, infrastrukturu, poslovne aplikacije, gotove proizvode, usluge i aplikacije koje razvija korisnik. Projektovanje i implementacija informacionog sistema za podršku poslovnog procesa mogu biti kritični po sigurnost. Pre projektovanja informacionih sistema treba da se identifikuju zahtevi za sigurnosti i o tome treba napraviti sporazum. Svi zahtevi za sigurnost treba da se identifikuju u fazi izrade projektnih zahteva i treba da se obrazlože, sporazumno prihvate i dokumentuju kao deo u okviru ukupnog poslovnog paketa za neki informacioni sistem.

19.2 Ispravna u obrada u aplikacijama

Cilj je da se spreče greške, gubitak, neovlašćene modifikacije ili zloupotreba informacija u aplikacijama.

Da bi se osigurala ispravna obrada, u aplikacijama treba da budu projektovane odgovarajuće kontrole, uključujući aplikacije koje razvija korisnik. Ove kontrole treba da obuhvate validaciju ulaznih podataka, unutrašnju obradu i izlazne podatke.

19.3 Kriptografske kontrole

Cilj je da se pomoću kriptografskih sredstava zaštiti poverljivost, verodostajnost ili integritet informacija.

Treba izraditi politiku korišćenja kriptografskih kontrola. Za podršku kriptografskih postupaka treba uspostaviti upravljanje ključevima.

19.4 Sigurnost sistemskih datoteka

Cilj je da se osigura sigurnost sistemskih datoteka.

Treba kontrolisati pristup sistemskim datotekama i izvornom programu, a IT projekte i aktivnost za podršku treba sprovoditi na siguran način. Treba obratiti pažnju na to da se izbegne izlaganje osetljivih podataka u ispitnom okruženju.

19.5 Sigurnost u procesima razvoja i podrške

Cilj je da se održi sigurnost softvera i informacija u aplikacijskim sistemima.

Treba strogo kontrolisati okruženja projektovanja i podrške. Rukovodioci zaduženi za aplikacijske sisteme treba takođe da budu odgovorni za sigurnost u okruženju projektovanja ili podrške. Oni treba da osiguraju da se sve predložene promene na sistemu preispituju kako bi se proverilo da ne narušavaju sigurnost ni sistema ni operativnog okruženja.

19.6 Upravljanje tehničkim ranjivostima

Cilj je smanjivanje rizika od iskorišćavanja javno objavljenih tehničkih ranjivosti.

Upravljanje tehničkim ranjivostima treba implementirati na efektivan, sistematičan i ponovljiv način sa merenjima koja se preduzimaju radi potvrđivanja njegove efektivnosti. Ova razmatranja treba da obuhvate operativne sisteme i bilo koje druge aplikacije koje se tekuće koriste.

**20. UPRAVLJANJE INCIDENTIMA NARUŠAVANJA
SIGURNOSTI INFORMACIJA**

Redni broj*: 20	Rizik:
Naziv kontrole: Upravljanje incidentima narušavanja sigurnosti informacija	Otežan rad ili zastoje u poslovanju, Krađa intelektualne svojine
Aktivnosti u cilju snižavanja rizika:	Aktivnosti u slučaju pojave incidenata:
1. Napraviti formalne procedure za izveštavanje i širenje činjenica o događajima vezanim sa sigurnošću. Sve zaposlene, isporučioce i korisnike treće strane upoznati sa procedurama za izveštavanje. 2. Zapisivati i izveštavati o svakom uočenom ili sumnjivom slabljenju sigurnosti u sistemima ili uslugama 3. Nadgledanje sistema i upozorenja o slabostima 4. Uspostaviti procedure za postupanje sa raznim tipovima incidenata narušavanja sigurnosti informacija.	1. Postupa se prema zakonskim odrednicama. 2. Prikupljanje dokaza o incidentu, čuvanje i predstavljanje u skladu sa pravilima dokazivanja koje postavlja odgovarajući zakon.
Odgovoran za aktivnost: Menadzment	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 16. - Primer kontrole za snižavanje rizika

20.1 Izveštavanje o događajima u vezi sa sigurnošću informacija i o slabostima

Cilj je osigurati da se o događajima u vezi sa sigurnošću informacija i slabostima vezanim za informacione sisteme obaveštava na takav način da bude omogućeno blagovremeno preduzimanje korektivnih mera.

Treba da postoje formalne procedure za izveštavanje i širenje činjenica o događajima u vezi sa sigurnošću. Sve zaposlene, isporučioce i korisnike treće strane treba upoznati sa procedurama za izveštavanje o raznim tipovima događanja i slabostima koji mogu imati posledice po sigurnost imovine organizacije.

20.2 Upravljanje incidentima narušavanja sigurnosti informacija i poboljšanja

Cilj je da se osigura dosledan i efektivan pristup upravljanju incidentima narušavanja sigurnosti informacija.

Treba uspostaviti odgovornosti i procedure za efektivno postupanje sa događajima u vezi sa sigurnošću informacija i slabostima kada se o njima podnese izveštaj. Treba

primeniti postupak stalnog poboljšavanja odgovora, nadgledanja, vrednovanja i ukupnog upravljanja incidentima narušavanja sigurnosti informacija.

21. UPRAVLJANJE KONTINUITETOM POSLOVANJA

Redni broj*: 21	Rizik:
Naziv kontrole: Upravljanje kontinuitetom poslovanja	Otežan rad ili zastoje u poslovanju, Zaštita od uticaja većih otkaza ili katastrofa
Aktivnosti u cilju snižavanja rizika: 1. Razviti i održavati proces za kontinuitet poslovanja koji je upravljiv koji se proteže kroz celu organizaciju. 2. Razumevanje rizika sa kojim se organizacija suočava u pogledu verovatnoće njihovog nastajanja i njihovih posledica 3. Identifikovanje svih dobara koji su uključeni u kritične poslovne procese 4. Razumevanje posledice koje će prekidi imati po poslovanje 5. Razmatranje uplate pogodnog osiguranja 6. Identifikovanje potrebnih resursa 7. Formulisanje i dokumentovanje planova za kontinuitet poslovanja 8. Identifikovanje događaja koji mogu da dovedu do prekida poslovnih procesa 9. Implementirati planove kako bi se u kritičnim poslovnim procesima posle prekida održale ili ponovo uspostavile poslovne operacije.	Aktivnosti u slučaju pojave incidenata:
Odgovoran za aktivnost: Menadžment	Odgovoran za aktivnost: Direktor
Napomene:	Napomene:

Tabela 17. - Primer kontrole za snižavanje rizika.

21.1 Aspekti sigurnosti informacija kod upravljanja kontinuitetom poslovanja

Cilj je da se uspostave protivmere za prekide u poslovnim aktivnostima, kako bi se kritični poslovni procesi zaštitili od uticaja većih otkaza ili katastrofa i da bi se osiguralo njihovo blagovremeno nastavljjanje.

Da bi se na minimum sveo uticaj na organizaciju treba implementirati proces upravljanja kontinuitetom poslovanja, kombinacijom kontrola za prevenciju i oporavak.

Treba analizirati posledice katastrofa, otkaza sigurnosti, gubitka usluge i raspoloživosti uluga u odnosu na poslovanje. Sigurnost treba da bude integralni deo ukupnog procesa kontinuiteta poslovanja, kao i ostalih procesa rukovođenja u organizaciji.

22. USKLAĐENOST

Redni broj*: 22	Rizik:
Naziv kontrole: Usklađenost	Neusklađenost sa zakonskim odredbama
Aktivnosti u cilju snižavanja rizika: 1.Savete o zakonskim zahtevima/regulativi definišu pravni savetnici u organizaciji. 2.Za svaki informacioni sistem i organizaciju treba eksplicitno definisati,dokumentovati i ažurno održavati sve odgovarajuće propise,statutarne i ugovorne zahteve,kao i pristup organizacije zadovoljenju ovih zahteva. 3.Implementirati odgovarajuće procedure kako bi se osigurala usklađenost u pogledu korišćenja materijala koji može biti predmet prava intelektualne svojine i korišćenja softverskih proizvoda koji predstavljaju vlasništvo. 4.Projektovati i implementirati politiku zaštite i tajnosti podataka organizacije 5.Korisnike odvratiti od korišćenja sredstava za obradu informacija za neautorizovane namene 6.Upoznavanje korisnika sa preciznim područjem njihovog dozvoljenog pristupa 7.Kriptografske kontrole primenjivati u skladu sa svim odgovarajućim sporazumima,zakonima i propisima. 8.Rukovodioci osiguravaju da sve procedure sigurnosti u području njihove odgovornosti ispravno sprovede. 9.Redovno proveravati usklađenost informacionih sistema sa standardima za implementaciju sigurnosti. 10.Pažljivo isplanirati zahteve za proveru na operativnim sistemima i dogovoriti sa odgovarajućim menadžmentom. 11.Zaštiti pristup alatima za proveru	Aktivnosti u slučaju pojave incidenata:
Odgovor za aktivnost: Menadžment	Odgovor za aktivnost: Direktor
Napomene:	Napomene:

Tabela 18. - Primer kontrole za snižavanje rizika.

22.1 Usklađenost za zakonskim odredbama

Cilj je izbeći kršenja bilo kojih zakonskih propisa, statutarne ili ugovorene obaveze, kao i bilo kojeg zahteva za sigurnost.

Projektovanje, rad, korišćenje i upravljanje informacionim sistemima može da podleže propisima, statutarne i ugovorne zahtevima za sigurnost. Savete o specifičnim zakonskim zahtevima treba potražiti od pravnih savetnika u organizaciji ili odgovarajuće kvalifikovanih pravnika.

12.2 Usklađenost sa politikama i standardima sigurnosti i tehnička usklađenost

Cilj je da se osigura usklađenost sistema sa politikama sigurnosti u organizaciji i sa standardima.

Sigurnost informacionih sistema treba redovno preispitivati. Takva preispitivanja treba obavljati prema odgovarajućim politikama sigurnosti i tehničkim platformama i treba proveravati usklađenost informacionih sistema sa standardima za implementaciju sigurnosti i dokumentovanim kontrolama sigurnosti.

22.3 Razmatranje provere informacionih sistema

Cilj je da se ostvari maksimalna efikasnost i da se na minimum svedu smetnje procesa provere sistema.

Prilikom provere sistema u radu treba da postoje kontrole za sigurno zaštitu operativnih sistema i alata za proveru. Zaštita je potrebna i radi odbrane integriteta i sprečavanja zloupotrebe alata za proveru.

16. ZAKLJUČAK

Sigurnost, kao jedan bitan segment današnjeg vremena ne treba zanemariti. Pretnje današnjeg vremena organizacije moraju spremno dočekati. ISO 27001 je takav standard u kome je zapisano sve ono što bi trebalo da bude dovoljno da odbrana od napada bude efikasna.

Standard ISO 27001 je atipičan u odnosu na sisteme menadžemnta. Osnovni deo sadrži relativno malo zahteva, ali ima Aneks A koji je obiman i zahtevan. Potrebno je bar godinu dana intenzivnog rada kako bi se pripremilo sve što je potrebno, u pogledu dokumentacije i primene u praksi. Primena ovog standarda je nemoguća bez uključenja IT sektora, koji je po prirodi specifičan. Aspekti primene su tehnički, organizacioni i kombinovani. Dokumentacija koja je potrebna je veoma obimna i postupak provere je veoma detaljan.

Veoma je važna obuka zaposlenih i razvijanje njihove svesti o zaštiti informacija, kako bi uspešnije sprovodili sistem i ukazivali na potencijalne probleme.

Aneks A standarda ISO 27001 sadrži 133 kontrole koje se ne tiču isključivo informatičkih tehnologija, već pokrivaju i fizičku sigurnost, pravnu zaštitu, upravljanje ljudskim resursima, organizaciona pitanja, itd. S toga se Aneks A može posmatrati kao katalog sigurnosnih mera koje se koriste u toku postupka obrade rizika – kad u postupku procene rizika odredite neprihvatljive rizike, Aneks A vam pomaže da odaberete meru/meru/kontrolu/kontrole kojima ćete smanjiti takve rizike. Takođe sprečava i da zaboravite neku važnu kontrolu.

Aneks A je na neki način veza između standarda ISO 27001 i ISO 27002. Kontrole u ISO 27002 imaju iste nazive kao i one u Aneksu A standarda ISO 27001, ali je razlika u količini detalja gde ISO 27001 daje kratku definiciju pojedinačnih kontrola, dok u ISO 27002 postoje jako detaljne smernice o tome kako treba primeniti kontrolu.

Ako sada mislite da je Aneks A savršen implementacijski alat za vaš projekt informacijske sigurnosti, nemojte biti previše sigurni jer ćete u njemu naći i neke stvari koje nemaju smisla. Ponekad različite kontrole definišu skoro ista pitanja i zbog toga mogu delovati zbunjujuće. Takav je slučaj s kontrolama A.9.2.6 (rashodovanje ili ponovna uporaba opreme) i A.10.7.2 (rashodovanje medija). To nisu jedine nejasnoće. U nekim kontrolama Aneks A govori o politikama i procedurama, ali ne propisuje da moraju biti dokumentovane.

Najbolje stvari u standardu ISO 27001 su upravo fokus i fleksibilnost u primeni sigurnosnih mera, samo treba paziti da budu iskorišteni na najbolji mogući način.

Literatura:

1. "Sigurnost informacija I IT Service menagement" – Stanislav Lisse
2. Standard SPRPS ISO IEC 27001
3. Standard SRPS ISO IEC 27002
4. [www. Energoprojekt Holding a.d. - ims consulting](http://www.Energoprojekt Holding a.d. - ims consulting)
5. www.energoprojekt-oprema.com
6. [www. Wikipedia.org](http://www.Wikipedia.org).