**SVEUČILIŠTE U ZAGREBU**

**FAKULTET ORGANIZACIJE I INFORMATIKE**

**VARAŽDIN**

**Marko Momčilović**

**ISO 27001**

SIS KNJIGA

Varaždin, siječanj 2014.

Sadržaj

[1.Uvod 1](#_Toc377039881)

[2.Povijest norme ISO/IEC 27001:2005 2](#_Toc377039882)

[3.Procesni pristup 3](#_Toc377039883)

[4.Terminologija 5](#_Toc377039884)

[5.ISMS 7](#_Toc377039885)

[5.1.Opći zahtjevi 7](#_Toc377039886)

[5.2.Uspostavljanje i upravljanje ISMS-om 7](#_Toc377039887)

[5.3.Zahtjevi za dokumentaciju 9](#_Toc377039888)

[6.Odgovornost uprave 11](#_Toc377039889)

[6.1.Opredjeljenje uprave 11](#_Toc377039890)

[6.2.Upravljanje sredstvima 11](#_Toc377039891)

[7.Interne prosudbe (auditi) ISMS-a 12](#_Toc377039892)

[8.Provjera ISMS-a od strane uprave 13](#_Toc377039893)

[9.Poboljšanje ISMS-a 14](#_Toc377039894)

[10.ISO 27001 certificiranje 15](#_Toc377039895)

[11.ISO 27000 zaključak 17](#_Toc377039896)

[Literatura 18](#_Toc377039897)

# 1.Uvod

U današnje doba kada su pojedini proizvodi veoma rašireni na tržištu, a konkurencija velika, nastaje potreba za neprestanim poboljšanjem tih istih proizvoda. Ovo dovodi do većih očekivanja i potreba za informacijama kao pokretačkim snagama svake organizacije. Dok se s jedne strane svaka organizacija bori za što većim brojem korisnika i zahtjeva neprestano poboljšanje svojih proizvoda ili usluga, s druge strane, kod korisnika se javlja potreba za osiguranjem raspoloživosti, povjerljivosti i cjelovitosti informacija.

Sve veća važnost počinje se pridodavati području informatike kao potpornom procesu svih zainteresiranih stranaka, ali i najvišeg vodstva. Ono što je bitno za **ISO/IEC 27001 normu** (eng. *International Organization for Standardization / International Electrotechnical Commission*) jest to da je ona međunarodna norma pripremljena kako bi pružila model za uspostavljanje, implementaciju, rad, nadziranje, provjeru, održavanje i unaprjeđivanje sustava upravljanja informacijskom sigurnošću – **ISMS** (eng. *Information Security Management Systems*). Usvajanje ISMS-a treba biti strateškom odlukom organizacije, odnosno da se očekuje da će implementacija ISMS-a pratiti potrebe organizacije.

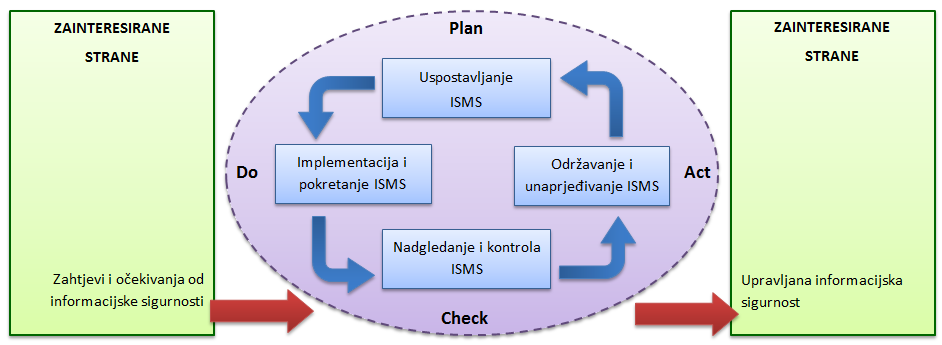
# 2.Povijest norme ISO/IEC 27001:2005

Prije nastajanja ISO normi, postojala je BS 7799 norma (nastala pod okriljem British Standard Institute). Prvi put je izišla kao kodeks dobre prakse 1995.g. Tijekom godina je nadopunjavana, te je 1999.g. podijeljena na dva dijela, BS 7799-1 i BS 7799-2. Nekoliko godina kasnije, normu BS 7799-1 preuzima ISO (Međunarodna organizacija za standardizaciju) i izdaje ju pod imenom ISO/IEC 17799. Kasnije je norma BS 7799-2 izdana kao ISO/IEC 27001:2005 [Knez J, 2006, str. 1] U istoj su opisani pojedini elementi sustava upravljanja sigurnošću informacija. Norma je napisana u obliku zahtjeva, koje sustav treba ispunjavati, te omogućava ocjenjivanje bilo interno ili vanjsko, od neovisne certifikacijske institucije.

# 3.Procesni pristup

ISO 27001 usvaja procesni pristup za uspostavljanje, implementaciju, rad, nadziranje, provjeru, održavanje i unaprjeđivanje organizacijskog ISMS-a [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 1] Organizacija treba identificirati i upravljati mnogim aktivnostima ukoliko želi učinkovito funkcionirati.

Bitno je naglasiti kako ova međunarodna norma usvaja **PDCA model**. Slika 1 prikazuje uzimanje zahtjeva za informacijsku sigurnost i očekivanja zainteresiranih strana, kao ulaznu komponentu, te kroz neophodne procese stvara rezultate informacijske sigurnosti koji odgovaraju tim zahtjevima i očekivanjima, kao izlaznu komponentu.



Slika 1 - PDCA model primijenjen na ISMS procese [Zavod za ispitivanje kvalitete d.o.o., 2007., str.2]

PDCA model je skraćeni naziv za „Plan-Do-Check-Act“ model i primjenjen je u oblikovanju svih ISMS procesa. Što se sve podrazumijeva pod PDCA, opisano je u sljedećoj tablici:

Tablica 1 - Opis PDCA modela [Zavod za ispitivanje kvalitete d.o.o, 2007., str. 2]

|  |  |
| --- | --- |
| **PDCA model** | **Opis** |
| **Plan**  (uspostaviti ISMS) | Uspostaviti ISMS politiku, ciljeve, procese i procedure važne za upravljanje rizikom i poboljšanje informacijske sigurnosti kako bi dali rezultate u skladu s ukupnom politikom i ciljevima organizacije |
| **Do**  (implementirati i izvršavati ISMS) | Implementirati i izvršavati ISMS politiku, kontrole, procese i procedure |
| **Check**  (nadgledati i provjeravati ISMS) | Procijeniti i gdje je primjenjivo, mjeriti izvršavanje procesa u odnosu na ISMS politiku, ciljeve i praktično iskustvo, te izvještavati upravu o rezultatima radi provjere |
| **Act**  (održavati i poboljšavati ISMS) | Poduzeti korektivne i preventivne akcije zasnivane na rezultatima interne ISMS prosudbe (audita) i provjere uprave ili ostalim bitnim informacijama kako bi se postiglo stalno poboljšanje ISMS-a |

# 

# 4.Terminologija

Za potrebe ISO 27001 definiramo i primjenjujemo sljedeće nazive i definicije, prikazane u tablici niže:

Tablica 2 - Nazivi i definicije koje se primjenjuju u ISO 27001 [Zavod za ispitivanje kvalitete d.o.o, 2007., str. 4]

|  |  |
| --- | --- |
| **Pojam** | **Definicija** |
| **Imovina** | Sve što predstavlja vrijednost za organizaciju |
| **Dostupnost** | Osobina dostupnosti i upotrebljivosti imovine na zahtjev ovlaštenog entiteta |
| **Povjerljivost** | Osobina da informacija nije učinjena dostupnom ili otkrivena neovlaštenim osobama, entitetima ili procesima |
| **Informacijska sigurnost** | Očuvanje povjerljivosti, integriteta i dostupnosti informacije uključiti se mogu i druge osobine kao što su vjerodostojnost, odgovornost, neporecivost i pouzdanost |
| **Sigurnosni događaj** | Prepoznatljiv slučaj stanja sustava, usluge ili mreže koji upućuje na moguću povredu politike informacijske sigurnosti ili neuspjeh zaštite ili do tada nepoznate okolnosti koje mogu biti važne za sigurnost |
| **Sigurnosni incident** | Jedan ili više neželjenih ili neočekivanih sigurnosnih događaja koji imaju značajnu vjerojatnost ugrožavanja poslovnih aktivnosti i informacijske sigurnosti |
| **Sustav upravljanja informacijskom sigurnošću (ISMS)** | Dio cjelokupnog sustava upravljanja, temeljen na pristupu sa stane poslovnih rizika, kako bi uspostavio, implementirao, nadzirao, provjeravao, održavao i unapređivao informacijsku sigurnost. |
| **Integritet** | Osobina očuvanja autentičnosti i cjelovitosti imovine |
| **Rezidualni rizik** | Preostali rizik nakon obrade rizika |
| **Prihvaćanje rizika** | Odlika da se rizik prihvati |
| **Analiza rizika** | Sustavna uporaba informacija za određivanje izvora i procjenu rizika |
| **Procjena rizika** | Cjelokupan proces analize i njegovo vrednovanje |
| **Vrednovanje rizika** | Proces usporedbe procijenjenog rizika sa danim kriterijima, kako bi se ustanovio značaj rizika |
| **Upravljanje rizikom** | Usklađene aktivnosti za usmjeravanje i kontrolu organizacije u smislu rizika |
| **Obrada rizika** | Proces odabira i primjene mjera za promjenu rizika |
| **Izjava o primjenjivosti** | Dokumentirana izjava koja opisuje ciljeve kontrola i kontrole koje su relevantne i primjenjive na ISMS organizacije |

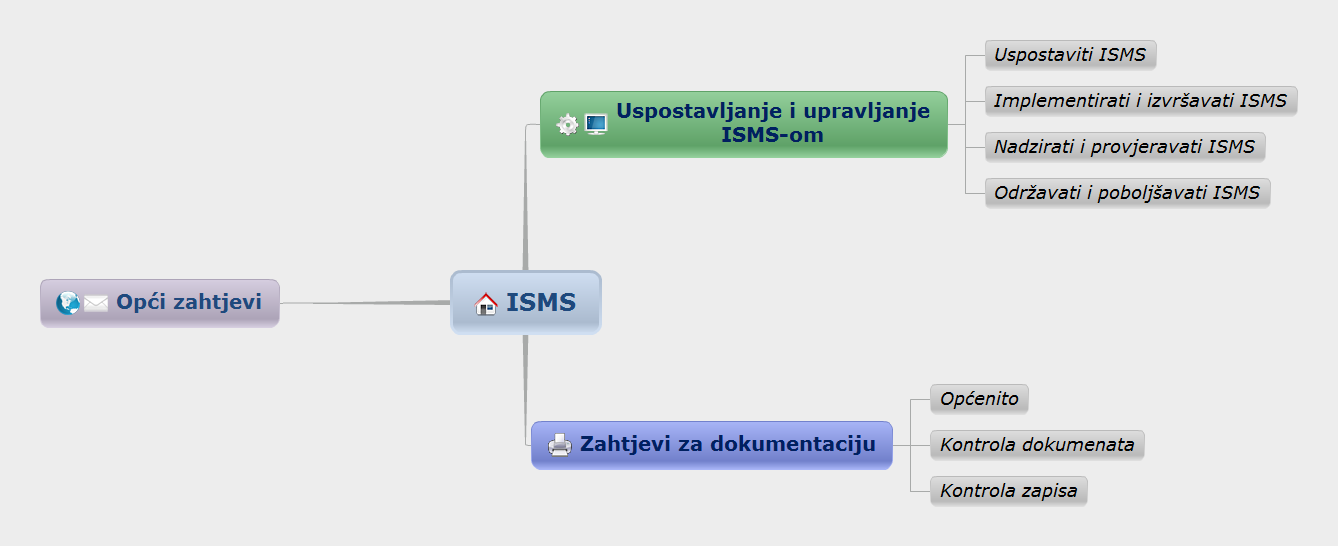
# 

# 5.ISMS

Kao što mu i sam naziv govori, ISMS (eng. *Information Security Management Systems*) je sustav upravljanja informacijskom sigurnošću. U tekstu prije je navedeno kako ISMS, prema ISO 27001 normi, pruža sustavan pristup upravljanju osjetljivim informacijama kako bi ih zaštitio i obuhvaća sve što je unutar organizacije, a tiče se procesa, informacijske imovine i zaposlenika. ISMS također možemo nazvati „sredstvo“ kojim uprava neke organizacije prati i nadzire sigurnost IS-a. Za izgradnju sustava upravljanja informacijskom sigurnošću potreban je PDCA model (spomenut u prethodnim poglavljima), koji se kontinuirano provodi. Izgradnja samog ISMS-a je iterativni proces koji se neprestano nadograđuje i poboljšava.

Ključni koraci koji vode do uspješne izgradnje ISMS-a i primjene ISO 27001 norme navedeni su u sljedećim potpoglavljima.

Ukratko, svi koraci prikazani su na mentalnoj mapi, a kasnije kroz tekst i opisani.



Slika 2 - Koraci u izgradnji ISMS-a

## 5.1.Opći zahtjevi

Što se tiče općih zahtjeva, za organizaciju je važno upostaviti, implementirati, izvršavati, nadzirati, održavati i poboljšavati dokumentirani ISMS unutar konteksta cjelokupnih poslovnih aktivnosti organizacije i rizika s kojima se ona suočava [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 6].

## 5.2.Uspostavljanje i upravljanje ISMS-om

Što se tiče uspostavljanja i upravljanja ISMS-om, ono se dijeli na četiri podgrupe: [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 6-9]

1. **Uspostaviti ISMS**

Da bi se uopće uspostavio ISMS, organizacija mora poduzeti nekoliko koraka, a to su:

* 1. Određivanje opsega i granica ISMS-a
  2. Definiranje politike ISMS-a
  3. Definiranje pristupa organizacije procjeni rizika
  4. Identifikacija rizika
  5. Analiza i vrednovanje rizika
  6. Identifikacija i vrednovanje opcija za obradu rizika
  7. Odabir ciljeva kontrola i kontrola za obradu rizika
  8. Dobivanje odobrenja uprave za predložene rezidualne rizike
  9. Dobivanje ovlaštenja uprave za implementaciju i izvršavanje ISMS-a
  10. Priprema Izjave o primjenjivosti

1. **Implementirati i izvršavati ISMS**

Nakon što su se ispunili svi uvjeti za uspostavu ISMS-a, sljedi korak implementacije i izvršavanja ISMS-a:

1. Formulacija plana za obradu rizika
2. Implementacija plana za obradu rizika
3. Implementacija odabranih kontrola kako bi se zadovoljili ciljevi kontrola
4. Određivanje načina mjerenja učinkovitosti odabranih kontrola ili grupa kontrola
5. Implementacija programa obuke i podizanja svijesti o informacijskoj sigurnosti
6. Upravljanje izvršavanjem ISMS-a
7. Upravljanje resursima za ISMS
8. Implementacija procedure i drugih kontrola sposobnih za omogućavanje pravovremene detekcije sigurnosnih događaja i odgovor na sigurnosne incidente
9. **Nadzirati i provjeravati ISMS**

Za provođenje implementacije i izvršavanja ISMS-a može se reći da je posljednji korak u uspostavi ISMS-a. Nakon što organizacija uspješno provede cjelokupnu uspostavu ISMS-a, na red dolazi kontrola, odnosno nadziranje i provjera ISMS-a, a koja obuhvaća sljedeće:

1. Izvršavanje procedure nadzora i provjere, te ostale kontrole
2. Izvođenje redovite provjere učinkovitosti ISMS-a
3. Mjerenje učinkovitosti kontrola (svrha: provjera da li su sigurnosni zahtjevi zadovoljeni)
4. Provjeravanje procjene rizika u planiranim intervalima
5. Provođenje interne prosudbe u planiranim intervalima
6. Provođenje provjere ISMS-a od strane uprave na redovnoj bazi
7. Nadopunjavanje sigurnosnih planova kako bi se u obzir uzeli rezultati aktivnosti za nadzor i provjeru
8. Bilježenje akcija i događaja koji bi mogli imati učinak na učinkovitosti ili izvođenju ISMS-a
9. **Održavati i poboljšavati ISMS**

Posljednji korak koji organizacija mora redovito provoditi, a tiče se dijela upravljanja ISMS-om je održavanje i poboljšavanje ISMS-a, koje se provodi kroz par koraka:

1. Implementacija uočenih poboljšanja ISMS-a
2. Poduzimanje odgovarajućih korektivnih i preventivnih akcija
3. Obavještavanje svih zainteresiranih strana o aktivnostima i poboljšanjima
4. Osiguranje da poboljšanja postignu njihove namjeravane ciljeve

Tek nakon ovih dugotrajnih procesa, može se reći da je ISMS, ne samo uspješno postavljen, već i održavan od strane organizacije.

## 5.3.Zahtjevi za dokumentaciju

Sa prethodne slike (slika 2) može se vidjeti što sve obuhvaćaju *Zahtjevi za dokumentaciju*. Osim ugrubo nabrojanih zahtjeva, oni će kroz daljnji dio teksta biti malo detaljnije opisani.

Zahtjevi za dokumentaciju dijele se u 3 podgrupe: [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 9-10]

1. **Općenito**

Općenito, dokumentacija mora sadržavati zapise o odlukama uprave, zatim osiguravati sljedivost postupaka do odluka uprave i politika, te na kraju osigurati da se zapisani rezultati mogu ponovno proizvesti. Ukratko, sada će biti nabrojano što sve ISMS dokumentacija mora sadržavati:

* 1. Dokumentirane izjave ISMS politike i ciljeva
  2. Opseg ISMS-a
  3. Procedure i kontrole koje podupiru ISMS
  4. Opis metodologije procjene rizika
  5. Izvještaj procjene rizika
  6. Plan obrade rizika
  7. Organizaciji potrebne dokumentirane procedure za učinkovito planiranje, rad i kontrolu njenih procesa informacijske sigurnosti
  8. Zapise zahtijevane ovom međunarodnom normom
  9. Izjavu o primjenjivosti

1. **Kontrola dokumenata**

Dokumenti moraju biti zaštićeni i kontrolirani. Također, mora biti uspostavljena procedura koja će odrediti akcije uprave potrebne kako bi se:

* 1. Odobrila adekvatnost dokumenata prije izdavanja
  2. Pregledali i dopunili dokumenti i ponovo odobrili
  3. Osiguralo da se identificirane izmjene i status trenutne revizije dokumenata
  4. Osiguralo da su relevantne verzije primjenjivih dokumenata dostupne na mjestu upotrebe
  5. Osiguralo da dokumenti ostanu čitki i lako prepoznatljivi
  6. Osiguralo da su dokumenti dostupni onima koji ih trebaju
  7. Osiguralo da su identificirani dokumenti vanjskog porijekla
  8. Osiguralo da je distribucija dokumenata kontrolirana
  9. Spriječilo nenamjernu upotrebu zastarjelih dokumenata
  10. Ukoliko su iz bilo kod razloga sačuvanima, dokumentima dodijelilo odgovarajuću identifikaciju

1. **Kontrola zapisa**

Moraju se uspostaviti i održavati zapisi koji pružaju dokaze o usklađenosti sa zahtjevima i učinkovitom radu ISMS-a. Oni moraju biti zaštićeni i kontrolirani. Zapisi moraju ostati čitki, lako prepoznatljivi i dostupni. Kontrole moraju biti dokumentirane i implementirane.

# 6.Odgovornost uprave

Što se tiče odgovornosti uprave, dvije su stvari na koje se odgovornost uprave dijeli, a prikazane su na slici niže (slika 3): [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 10]



Slika 3 - Odgovornost uprave

## 6.1.Opredjeljenje uprave

Uprava mora pružiti dokaz svoje opredjeljenosti uspostavi, implementaciji, izvršavanju, nadziranju, provjeri, održavanju i poboljšanju ISMS-a. To može učiniti kroz veći broj uvjeta, a neki od njih su:

* Uspostavljanje ISMS politike
* Osiguravanje da su ciljevi i planovi ISMS-a uspostavljeni
* Odlučivanje o kriteriju za prihvaćanje rizika i prihvatljivim razinama rizika
* Osiguranje provođenja internih prosudbi (audita) ISMS-a
* Provođenjem provjera ISMS-a od strane uprave

...

## 6.2.Upravljanje sredstvima

Upravljanje sredstvima dijeli se na:

* Dodjeljivanje sredstava
* Obučavanje, razina svijesti i sposobnosti

# 7.Interne prosudbe (auditi) ISMS-a

Interne prosudbe, odnosno auditi moraju se provoditi u planiranim intervalima, kako bi se ustanovilo da ciljevi kontrola, kontrole, te procesi i procedure njenog ISMS-a udovoljavaju zahtjevima ove međunarodne norme i identificiranim zahtjevima informacijske sigurnosti, te učinkovito implementirani i održavani i izvršavaju se kako se od njih očekuje [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 11].

Dokumentiranom procedurom moraju također biti definirani odgovornosti i zahtjevi za planiranje i provođenje prosudbi.

# 8.Provjera ISMS-a od strane uprave

Kao što se provode interne prosudbe u planiranim intervalima od strane organizacije, također se i provjera organizacijskog ISMS-a mora održavati i to minimalno jednom godišnje. Provjeravanje ISMS-a osigurava njegovu stalnu podobnost, primjerenost i učinkovitost. Za provjeru ISMS-a bitni su ulazni podaci, te na kraju i sami rezultati provjere. U daljnjem tekstu ukratko su nabrojani ulazni podaci i rezultati provjere: [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 11, 12]

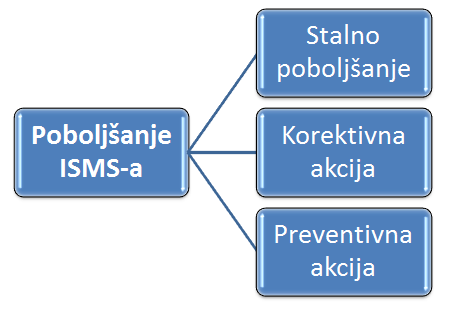
* **Ulazni podaci za provjeru** – podaci koje je potrebno dostaviti upravi za potrebe provjere sadržavaju:
  + Rezultate prosudbi i provjera ISMS-a
  + Povratne informacije zainteresiranih strana
  + Status preventivnih i korektivnih akcija
  + Rezultate mjerenja učinkovitosti
  + Naknadne akcije iz prethodnih provjera uprave
  + Preporuke za poboljšanje

...

* **Rezultati provjere** uprave moraju sadržavati sve odluke i akcije vezane uz sljedeće:
  + Poboljšanje učinkovitosti ISMS-a
  + Ažuriranje procjene rizika i plana obrade rizika
  + Izmjene procedura i kontrola
  + Potrebe za sredstvima
  + Poboljšanja načina mjerenja učinkovitosti kontrola

# 9.Poboljšanje ISMS-a

Poboljšanje ISMS-a dijeli se na 3 skupine (slika 4):



Slika 4 - Poboljšanje ISMS-a

Kada se govori o **stalnom poboljšanju**, onda se misli na to da organizacija mora konstantno poboljšavati učinkovitost ISMS-a. Poboljšavanje učinkovitosti ISMS-a odvija se kroz uporabu politike informacijske sigurnosti, ciljeva informacijske sigurnosti, rezultata prosudbi i slično.

Osim stalnog poboljšavanja, moraju se poduzimati i **korektivne akcije** kako bi se uklonili uzroci nesukladnosti sa ISMS zahtjevima, te se mora provoditi dokumentirana procedura za korektivnu akciju, koja pak mora definirati zahtjeve za: [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 12]

* Identificiranje nesukladnosti
* Ustanovljavanje uzroka nesukladnosti
* Ustanovljavanje i implementiranje potrebne korektivne akcije
* Provjeravanje poduzete korektivne akcije

...

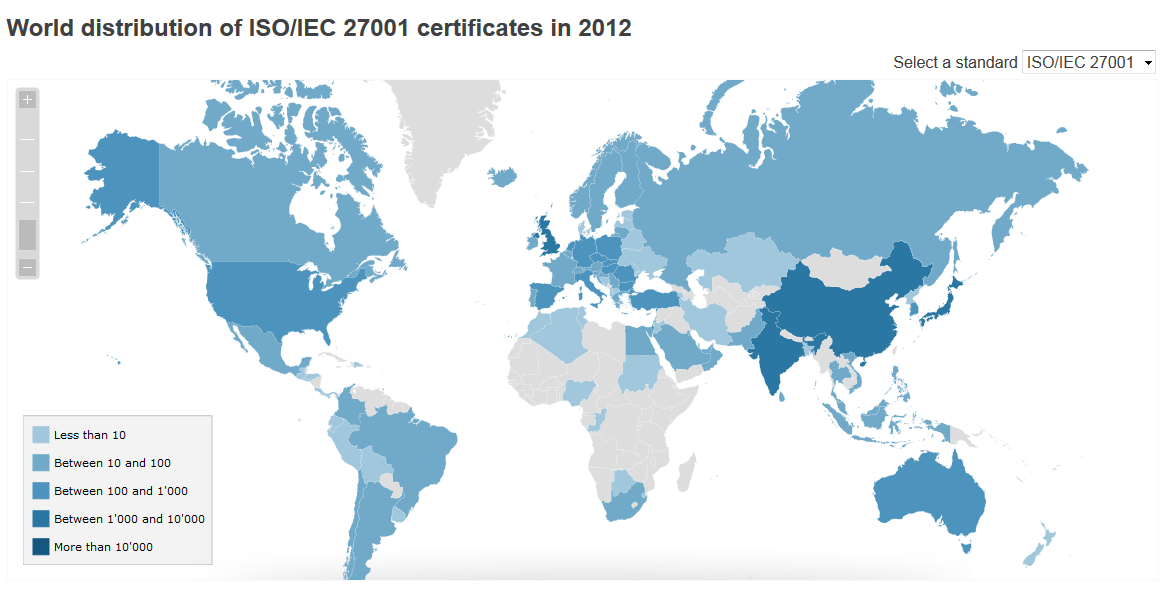
Na kraju, pored stalnog poboljšanja i korektivnih akcija, postoje i **preventivne akcije**, što podrazumijeva da organizacija mora odrediti akciju za uklanjanje uzroka koji može uzrokovati potencijalne nesukladnosti sa ISMS zahtjevima. Organizacija mora identificirati promijenjene rizike i identificirati zahtjeve za preventivnom akcijom s pažnjom usmjerenom na znatno promijenjene rizike [Zavod za ispitivanje kvalitete d.o.o., 2007, str. 12].

# 10.ISO 27001 certificiranje

Kažu da je dobro da organizacija ima ISO 27001 certifikat, ali zašto? CRN (Computer Reseller News) 2009.godine najbolje je to predočio sa 10 razloga: [CRN.com.au, 2013]

1. ISO 27001 je internacionalno prepoznat, pa će i iskustvo organizacije biti
2. Najbolja praksa; odvajanje onih sa stvarnim iskustvom od onih koji samo razmišljaju o tome na način da se profitira od iskustva drugih
3. Baziran na riziku; gleda što organizacija treba, te ne nameće određene standarde; pravovremeni, pravedni i isplativ savjet
4. Standard za upravljanje, a ne tehnički standard; daje model upravi koja tada mora pokazati svoje vještine donošenja odluka
5. Holistički; razmatra sve aspekte informacijske sigurnosti, ne samo tehničke mjere, demonstrira dubinu i širinu
6. Organizacije mogu biti nezavisno certificirane; daje vanjski nezavisni pogled na poslove o sigurnosti u organizaciji
7. Daje način kako držati rizike pod kontrolom, dopuštajući redovit pregled i objektivnu analizu rizika
8. Daje proces za praćenje sigurnosti i napretka; mogućnost dokazivanja koristi od sigurnosti i ulaganja u sigurnost
9. Komplementaran je sa drugim standardima, poput ISO 9001, ISO 14001 i ISO 20001
10. Svaka organizacija sa ISO 27001 certifikatom je izjavila da je popravila upravljanje sigurnošću u organizaciji

Zanimljiv podatak su države koje imaju najveći broj certifikata. Za početak, slika niže (slika 5) prikazuje države i dodijeljene im certifikate u 2012. Godini [ISO, 2012].



Slika 5 - ISO 27001 certificiranje u 2012. godini [ISO27001, 2012]

U sljedećoj tablici (tablica 3) prikazano je 10 država s najviše dodijeljenih ISO 27001 certifikata u 2012. godini:

Tablica 3 - TOP 10 država s najviše dodijeljenih ISO 27001 certifikata [ISO27001, 2012]

|  |  |  |
| --- | --- | --- |
| **RB** | **Država** | **Broj certifikata** |
| 1. | Japan | 7199 |
| 2. | Velika Britanija | 1701 |
| 3. | Indija | 1600 |
| 4. | Kina | 1490 |
| 5. | Rumunjska | 866 |
| 6. | Tajvan | 855 |
| 7. | Španjolska | 805 |
| 8. | Italija | 495 |
| 9. | Njemačka | 488 |
| 10. | SAD | 415 |

Hrvatskoj je dodijeljeno 58 certifikata.

# 11.ISO 27000 zaključak

Ukratko, za kraj, norme iz serije ISO 27000 izrađene su tako da svaka od normi daje naglasak na nešto. U daljnjem tekstu nabrojane su norme od ISO 27001 do ISO 27006 i u jednoj rečenici objašnjen je naglasak pojedine norme:

* **ISO 27001** služi za postavljanje temelja informacijske sigurnosti i određivanje njezinih okvira.
* **ISO 27002** služi za implementaciju sigurnosnih mjera.
* **ISO 27003** pruža upute za implementaciju kao pomoć osobama koje implementiraju ISO 27000 standarde. U osnovi se bazira na smjernicama iz ISO 27001 standarda, te pruža vodstvo sve do pokretanja ISMS projekta.
* **ISO 27004** služi da pomogne organizacijama mjeriti, izvještavati i na temelju istoga sistematski poboljšavati kvalitetu ISMS.
* **ISO 27005** služi za provedbu procjene rizika.
* **ISO 27006** je akreditacijski standard koji vodi certificiranje kroz formalni proces certifikacije ISMS organizacija prema ISO 27001 standardu. U istome su navedene sve potrebe i upute kako izvesti certifikaciju i koje uvjete organizacija mora zadovoljiti.

# Literatura

1. Zavod za ispitivanje kvalitete d.o.o. (2007). *BS ISO/IEC 27001:2005*. Zagreb, Denona d.o.o.
2. Knez J. (2006). Sigurnost informacija po normi ISO/IEC 27001 u postojećim sustavima upravljanja. Dostupno 30.12.2013. na <http://www.kvaliteta.net/informacije/radovi/Knez_J_rad.pdf>
3. CRN.com.au (2013). *Koraci zašto je dobar ISO 27001*. Dostupno 30.12.2013. na <http://www.crn.com.au/News/152262,10-reasons-why-iso-27001-makes-a-better-is-security-professional.aspx>
4. ISO (2012). *Svjetska distribucija ISO / IEC 27001 certifikata u 2012*. Dostupno 30.12.2013. na <http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=AF#standardpick>