UPRAVLJANJE SUSTAVIMA INFORMACIJSKE SIGURNOSTI (ISO 27001)

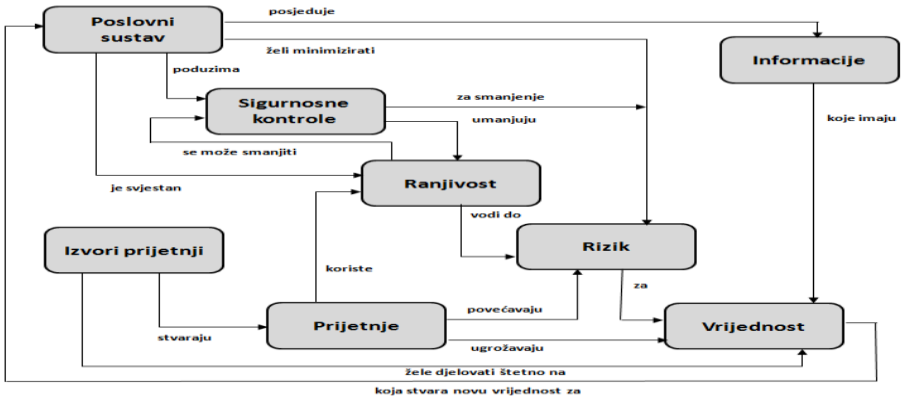
Značaj

Informacije su danas najvažniji resurs svakog poslovnog sustava, njegova krucijalna imovina. Bez obzira na veličinu i oblik poslovnih sustava (pripadnost javnom ili privatnom sektoru, profitnoj ili neprofitnoj orijentaciji), svi oni prikupljaju, obrađuju, pohranjuju i prenose informacije na više načina, elektronički, fizički i verbalno. Pri tome informacije se pojavljuju u mnogim oblicima: pisanim dokumentima, klasičnim i informatiziranim bazama podataka, slikama, dijagramima, poslovnim pravilima i nalaze se na mnogobrojnim nositeljima.

Svaki poslovni sustav ima informacije o svojoj viziji, misiji, strategiji, dugoročnijoj poslovnoj orijentaciji i strateškim ciljevima, poslovnim politikama, financijama, poslovnim procesima, tržištima, kupcima, dobavljačima, osoblju i njihovim kompetencijama, postupcima kojima se ostvaruju zakonske, regulatorne ili ugovorne obveze, informacije o načinu njegovog organizacijskog funkcioniranja i pripadajućim odgovornostima, instaliranoj računalnoj opremi, elektroničkim medijima, perifernoj opremi, sistemskoj programskoj opremi, korisničkim aplikacijama, telekomunikacijskim mrežama, IT zaposlenicima, kao i niz drugih vrijednih informacija.

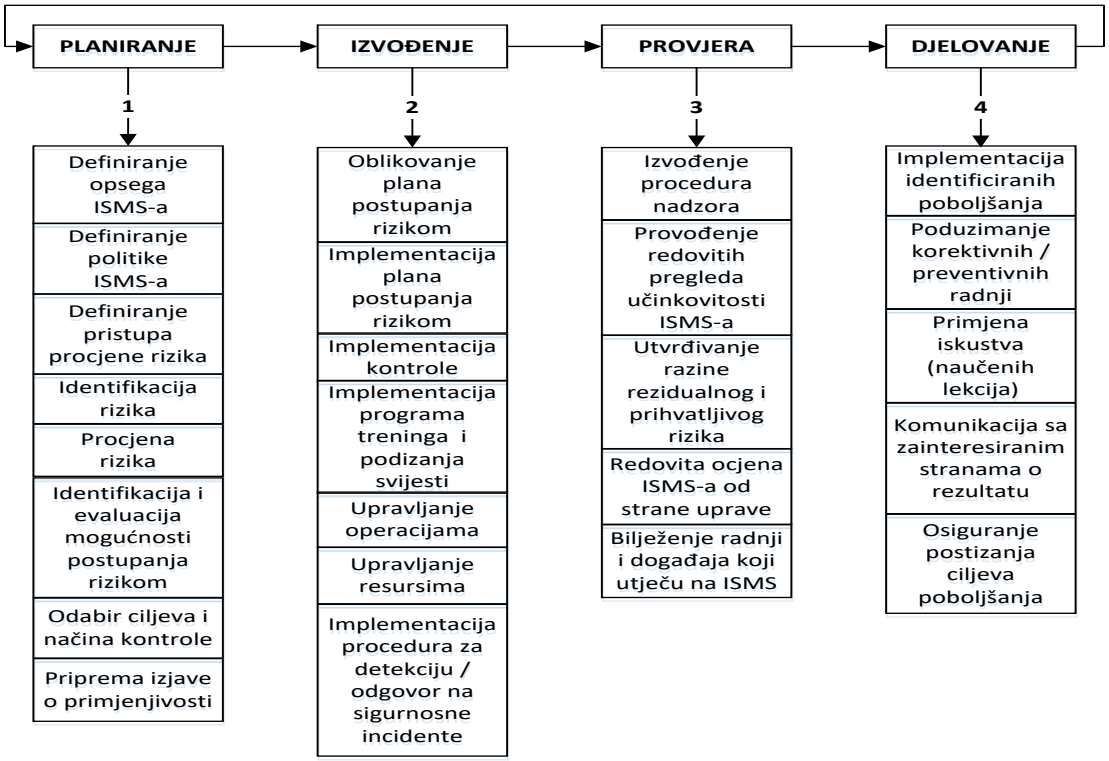
Kao i kod drugih oblika poslovne imovine, postoje mnogobrojni izvori prijetnji od napada na ovu informacijsku imovinu, koji, ukoliko se dese, a ne postoji uspostavljena dovoljno dobra informacijska sigurnost, mogu izazvati velike neželjene posljedice. Skupine takvih prijetnji su: tehničke pogreške, neautorizirani pristupi IT opremi ili podacima, prekidi u pružanju IT potpore poslovnim procesima, prirodne nepogode, fizička oštećenja, kompromitiranje podataka i informacija i sl. Međutim, danas najveće prijetnje dolaze od ljudi – hakera, računarskih kriminalaca, terorista, industrijske špijunaže, vlastitih zaposlenika.

Da li će se desiti negativne posljedice napada na informacijsku imovinu, ovisi od toga da li postoje adekvatne sigurnosne mjere i da li su one pravilo inkorporirane u cjelokupni sustav sigurnosti. Ukoliko je njihova razina nedovoljna, poslovni sustav je ranjiv i postoji rizik da će doći do ugrožavanja ove imovine. Mnogobrojna relevantna istraživanja, studije i izvješća, od kojih je većina dostupna putem interneta, upozoravaju na rastući broj napada na informacijsku imovinu i sve veće posljedice. Da bi se ova negativna pojava dovela u uvjete prihvatljivih rizika, ISO je razvio niz normi, od kojih je za uspostavu konzistentnog sustava informacijske sigurnosti vodeća norma ISO 9001 - *Information technology — Security techniques — Information security management systems — Requirements*, skraćeno ISMS. Ova norma skrbi o odnosu informacijske imovine, njene vrijednosti, izvora prijetnji, prijetnji, sigurnosnih kontrola, ranjivosti i rizika, na način koji je pojednostavljeno prikazan na slici:



Norma propisuje 114 sigurnosnih zahtjeva kojima se uspostavlja sustav informacijske sigurnosti, razvrstanih u 14 skupina: politike ISMS-a, organizacija informacijske sigurnosti, sigurnost ljudskih resursa, upravljanje informacijskom imovinom, kontrole pristupa, kriptografija, fizička sigurnost i sigurnost okruženja, sigurnost operacija, sigurnost komunikacija, nabava-razvoj-i-održavanje sustava, odnosi s dobavljačima, upravljanje incidentima, kontinuitet poslovanja i sukladnosti.

Upravljanje ovim sustavom provodi se putem poznatog PDCA (PIPD) ciklusa prikazanog na slici u nastavku:



Upravljanje ISMS-om provodi se na razini poslovodstva, kao i na operativnoj razini. Iz navedenih dijelova PDCA ciklusa nije teško prepoznati odgovornosti ovih razina.

Problematika sustava upravljanja informacijskom sigurnošću naročito je interesantna:

- Članovima vodstva poslovnih sustava zaduženim za sigurnost
- Voditeljima korporativne sigurnosti
- Voditeljima funkcije informatike
- Voditeljima informacijske sigurnosti
- Stručnjacima koji se bave informacijskom sigurnošću
- Auditorima / procjeniteljima informacijske sigurnosti
- Svima koje zanima područje sigurnosti i informacijske sigurnosti

Usluge ZIH-a

Konzultantske

ZIH može pružiti sve konzultantske usluge kojima se pokriva PDCA ciklus sustava informacijske sigurnosti. Obično se takav projekt čine slijede aktivnosti:

- Procjena trenutačnog stanja informacijske sigurnosti
- Priprema ISMS projekta
- Izrada politika informacijske sigurnosti
- Izrada sigurnosnih procedura (obvezne dokumentacije)
- Upravljanje imovinom
- Procjene i obrade sigurnosnih rizika
- Oblikovanje organizacije informacijske sigurnosti
- Sigurnost ljudskih resursa
- Kontrole pristupa
- Kriptografija
- Fizička sigurnost i sigurnost okoline
- Sigurnost operacija
- Sigurnost komunikacija
- Nabava, razvoj i održavanje informacijskih sustava
- Odnosi s dobavljačima
- Upravljanje sigurnosnim incidentima
- Upravljanje kontinuitetom rada
- Sukladnosti sa zakonodavstvom i drugim propisima

*Seminar*i

Razvoj, implementacija i audit sustava informacijske sigurnosti

- Uvod u informacijsku sigurnost
- Projektiranje ISO 27001 sustava upravljanja informacijskom sigurnošću
- Osposobljavanje za interne procjenitelje u skladu s normom ISO 27001
- Certified ISO 27001 Foundation (PECB)
- Certified ISO 27001 Lead Implementer (PECB)
- Certified ISO 27001 Lead Auditor (PECB)

Kontrole informacijske sigurnosti (ISO 27002)

- Kontrole informacijske sigurnosti u skladu s ISO 27002
- Certified ISO 27002 Foundation (PECB)

- Certified ISO 27002 Manager (PECB)
- Certified ISO 27002 Lead Manager (PECB)

Način rada

Poduhvat razvoja, implementacije i izobrazbi iz područja sustava informacijske sigurnosti ZIH realizira zajedničkim radom svojih stručnjaka i stručnog tima korisnika, uz usku suradnju s predstavnikom vodstva poslovnog sustava nadležnim za ovo područje.