

# Studija slučaja: Uvođenje sustava upravljanja informacijskom sigurnošću prema standardu ISO 27001

pišu **SINIŠA PINTEK** i  
**GABRIJELA VARGA**

## Motiv ulaganja

U Omega software smo, na tragu želje da razumijemo sadašnje i buduće potrebe svojih kupaca i nastavno na uvedeni sustav upravljanja kvalitetom prema standardu ISO 9001, prepoznali važnost sigurnosti informacija kao jedan od ključnih faktora koji unapređuju poziciju tvrtke na tržištu.

## Zašto sigurnost?

Sustav upravljanja informacijskom sigurnošću (Information Security Management System - ISMS) prema normi ISO/IEC 27001:2005 pruža sustavan pristup upravljanju osjetljivim informacijama kako bi ih zaštitio, a obuhvaća procese, informacijske imovinu i zaposlenike. On je isto tako sredstvo uz pomoć kojeg poslovanje organizacije prati i nadzire sigurnost informacijskih sustava organizacije svodeći poslovni rizik na minimum i osiguravajući da sigurnosni

zahtjevi poslovanja ispunjavaju organizacijske, kupčeve i pravne obveze. Ta međunarodna norma prihvaća model 'Plan-Do-Check-Act' primijenjen u oblikovanju svih ISMS-ovih procesa, a predviđa ciklus od četiri faze koje se kontinuirano trebaju provoditi kako bi se uveo sustav upravljanja informacijskom sigurnošću (ISMS). One su:

- 1) uspostava ISMS-a
- 2) uvođenje i izvršavanje ISMS-a
- 3) nadzor i provjera ISMS-a
- 4) održavanje i poboljšavanje ISMS-a.

## Preduvjeti uspjeha

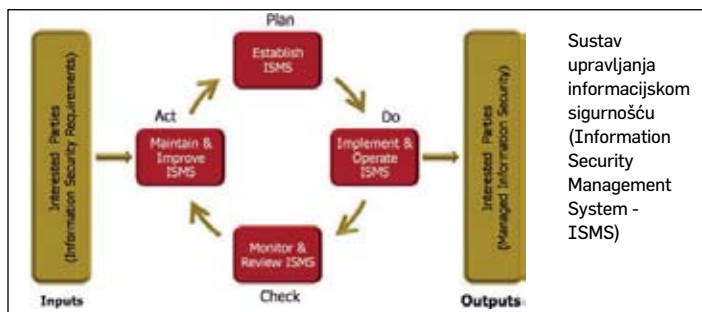
Kao i za svaki projekt, predanost uprave najvažniji je čimbenik uspjeha projekta. Nakon Uprave odluke da će se u tvrtku uvesti sustav bili su osigurani potrebni resursi. Stručni tim sastojao se od zaposlenika tvrtke specijaliziranih za pojedina područja i vanjskih konzultanata čija je uloga bila analiza postojećeg sustava i usklađivanje sa zahtjevima norme.

## Opseg sustava

S obzirom na motive ulaganja i na najviše kriterije kvalitete koje smo si postavili odlučili smo obuhvatiti sve poslovne procese u tvrtki. Tako sustav pokriva projektiranje, izgradnju i integraciju složenih informacijskih sustava, uvođenje aplikativnih i programskih rješenja, informatičko savjetovanje, podršku, pomoć i održavanje informacijskih sustava.

## Tijek uvođenja

Na početku posebnu pozornost posvetili smo pomnom odabiru konzultanata koji su nas pratili tijekom cijelog projekta. Projektni tim sastojao se od voditelja projekta, sistem-administratora i voditeljice informacijske sigurnosti potpomognutih vanjskim konzultantima, a uključeni su bili i svi



zaposlenici jer sustav obuhvaća cijelu tvrtku.

Projekt je imao nekoliko faza:

- **Uspostava** sustava sastojala se od analize stanja, klasifikacije informacija i izrade kataloga imovine te upravljanja rizicima.
- **Implementacija** je uključila izradu plana tretiranja rizika, izvedbu potrebnih postupaka za uspostavu i mjerenje učinkovitosti sustava te program izobrazbe svih zaposlenika tvrtke čiji je rezultat bilo podizanje razine svijesti o informacijskoj sigurnosti.
- Postavljanje **nadzora** omogućilo je žurno otkrivanje pogrešaka, sigurnosnih incidenata te redovite provjere i mjerenja učinkovitosti, što uključuje i unutarnje prosudbe kvalitete sustava.
- **Postupkom certifikacije** projekt je uspješno dovršen; ona je uključivala neovisnu prosudbu sustava koju je provela vanjska certifikacijska kuća.

## Rizici

Od rizika prepoznatih na početku projekta (nedostatak resursa, nedovoljne poslovne i tehničke kompetencije, nedovoljna kvaliteta vanjskih konzultanata) tijekom projekta aktivirao se rizik nedostatka resursa koji je bio uzrokom pomicanja roka završetka projekta za tri mjeseca. Tako je

ukupno trajanje projekta pomaknuto sa šest na devet mjeseci, a proračun projekta ostao je isti.

## Dobrobiti

**Najvažnije su dobrobiti uspostave takvog sistematičnog pristupa upravljanju sigurnošću informacija:**

- **sigurnost i pouzdanost uvedenih rješenja**
- **povjerenje poslovnih partnera u sigurnost informacijske imovine**
- **usklađenje s hrvatskom i zakonskom regulativom EU**
- **konkurentna prednost na tržištu**
- **osiguranje kontinuirane raspoloživosti usluge**
- **povećanje svijesti zaposlenika o informacijskoj sigurnosti**
- **posjedovanje međunarodno priznatog certifikata prema normi ISO 27001**

Uvođenje sustava upravljanja informacijskom sigurnošću i certifikacija prema normi ISO 27001 dodali su našem poslovanju znatnu vrijednost jer tako svim svojim poslovnim partnerima pokazujemo da Omega software u svoje poslovanje ugrađuje svjetski dokazanu najbolju praksu i potpisuje vrhunsku kvalitetu i integritet svojih poslovnih rješenja i usluga. ■

## VAŽNI RAZLOZI

### Dva su glavna motiva ulaganja:

- S obzirom na to da pristupamo visoko povjerljivim informacijama svojih klijenata, uvođenje takvog sustava dodatno je jamstvo postupanja takvim informacijama na najvišoj razini sigurnosti.
- Ujedno smo zadovoljili Uredbu o mjerama informacijske sigurnosti koja tijelima državne uprave, od kojih su mnoga naši klijenti, propisuje mjere informacijske sigurnosti za postupanje s klasificiranim i neklasificiranim podacima.