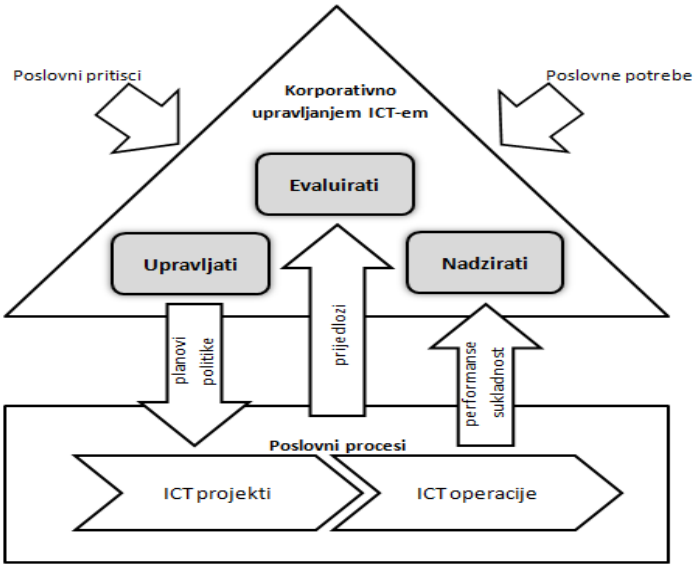
Zavod za informatičku djelatnost Hrvatske d.o.o.

ISO 38500 pristup IT Governance-u

1. Prikaz ISO/IEC 38500 modela

Ciljevi, principi i smjernice za primjenu

Poslovni sustavi, bez obzira da li pripadaju privatnom ili javnom sektoru, danas ne mogu funkcionirati bez IT-a. Međutim, kako to postići na učinkovit i djelotvoran način, krupno je pitanje. Odgovor na njega rezultanta je više čimbenika, osobito visine ulaganja u ovo područje, odgovornosti za IT i poslovnih učinaka koji se time dobiju. Investicije u IT nisu male i stalno se povećavaju. IT zahtijeva i značajne ljudske resurse. Tijekom vremena uvidjelo se da povrat ulaganja od ovih investicija nije zadovoljavajući, a brojna istraživanja ovog fenomena ukazala su da je temeljni uzrok tome nedostatni poslovni kontekst korištenja IT-a. Drugi aspekt ovog problema jest način odlučivanja o IT-u – da li ga provode informatičari ili menadžment, a treći aspekt su nedostatni napori za uspostavu čvršće veze poslovni ambijent - IT. Već je rečeno da se ova problematika istražuje relativno dugo, i put njenom rješenju vidi se u primjeni Governance načina upravljanja poslovnim sustavima, a time i IT-a. Kao rezultat takvih nastojanja, razvijena je i norma ISO/IEC 38500. Namijenjena je upravama i najvišem menadžmentu za evaluaciju, usmjeravanje i nadzor korištenja IT-a u poslovnim sustavima. Njena svrha je uputiti kako razumjeti i ispuniti poslovne, zakonske, regulatorne, etičke i dr. obveze u vezi s IT-em, na način da se ostvare maksimalni poslovni učinci. Sastoji se od definicija, načela i modela IT Governance-a te smjernica kako ih ostvariti. Ima tri temeljna cilja: 1. pružiti jamstvo dionicima poslovnog sustava da imaju povjerenje u IT, 2. omogućiti da uprava i menadžment usmjere primjenu IT-a prema poslovnim potrebama, ali i da nadzire njegov rad i uspješnost, te 3. dati osnovu za objektivnu procjenu kvalitete IT-a. Korisnici ove norme, osim već spomenutih uprava i menadžmenta, mogu biti i CIO-i, osobe koje se bave nadzorom korištenja resursa, kao što su pravni i financijski stručnjaci, procjenitelji / auditori, vlasnici poslovnih procesa, dobavljači IT opreme i usluga. Naravno da je norma namijenjena i IT populaciji, osobito njegovom menadžmentu. Model korporativnog upravljanja informatikom prema ovoj normi prikazan je na slici 1. Polazište su potrebe da IT bude infrastruktura ostvarenju poslovne strategije, te potrebe poslovnih procesa za IT potporom. Na toj osnovi ciklusom EDC (eng. Evaluate-Direct-Control), ovi zahtjevi se prenose na IT i to i na razvoj novih IT projekata i na IT operativu.



Slika 1. Model IT Governance-a prema normi ISO 38500

Zadaću *Evaluirati (eng. Evaluate)* vodstvo *(*uprava i izvršni menadžment) treba ostvariti na način da se istražuje i čini prosudba sadašnjeg i budućeg korištenja IT-a, polazeći od poslovne strategije, zahtjeva poslovnih procesa, tehnoloških promjena te ekonomskih i socijalnih trendova. Ova prosudba mora uključiti sadašnje i buduće poslovne potrebe i ciljeve s ocjenom da li je uz potporu IT-a moguće zadržati i povećati konkurentsku prednost, ili postići druge poslovne učinke. Zadaća *Usmjeriti (eng. Direct*) traži od uprave i izvršnog menadžmenta da definira odgovornosti za pripremu i implementaciju IT planova i politika. Planovi moraju uključivati i investicije u IT razvojne projekte i IT operativu. Vodstvo treba stvoriti uvjete da se novi projekti razviju i uspješno primijene u praksi. Očekuje se i da uprava od izvršnog menadžmenta traži povremeno izvješćivanje o statusu ovih projekata, ali i ostvarenju principa IT Govrnance-a. Zadaća *Nadzirati (eng. Monitor)* zahtijeva od uprave da nadzire performanse uspješnosti IT-a, npr. ostvarenje planova, doprinos IT-a unapređenju poslovanja, poštivanje pravne regulative, ostvarenje IT politika, poštivanje internih radnih procedura itd.

Norma polazi od šest principa IT Governance-a. Princip 1 je *Odgovornost, a* nalaže da pojedinci i grupe unutar poslovnog sustava trebaju razumjeti i prihvatiti svoje obveze u vezi IT-a. Princip 2 je *Strategija* i nalaže da poslovna strategija mora uzeti u obzir sadašnje i buduće mogućnosti IT-a, dok princip 3 *Akvizicija*, nalaže da se nabava IT resursa temelji na opravdanim poslovnim razlozima, odgovarajućim i kontinuiranim analizama s jasnim i transparentnim odlučivanjem te da postoji ravnoteža između koristi, mogućnosti, troškova i rizika. Princip 4 jesu *Pokazatelji* i zahtijeva da je IT sposoban pružiti mjerljivu potporu poslovnom sustavu u vidu IT usluga te potrebnu razinu njene kvalitete, kako bi se zadovoljili trenutni i budući zahtjevi poslovanja. Princip 5 jest *Usklađenost* i traži da IT djeluje u skladu sa svim obveznim zakonima i propisima te s jasno definiranim, implementiranim i provođenim vlastitim politikama i praksama. Naposljetku, princip 6 *Ljudsko ponašanje* polazi od toga da IT politike, odluke i praksa uvažavaju potrebu da zaposlenici razumiju značaj IT-a za poslovanje i ostvarenje postavljenih ciljeva, te da se ponašaju na očekivani način.

Za svaki od ovih principa norma usmjerava kako ostvariti EDC ciklus. Tako npr. za princip *Odgovornosti,*

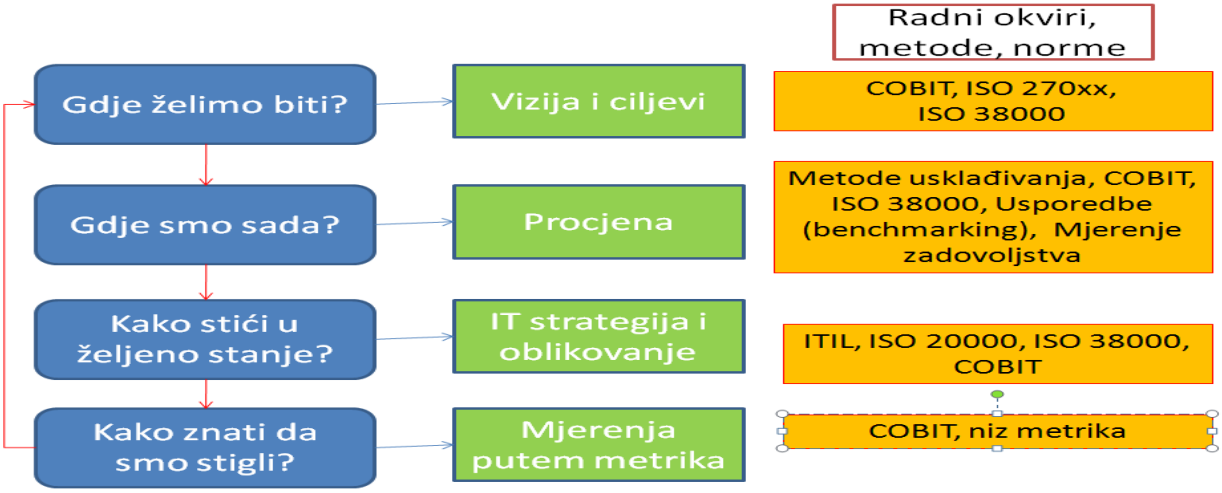
- Za zadaću *Evaluirati* vodstvo - uprava i izvršni menadžment, trebaju procjenjivati da li se dodijeljene odgovornosti ostvaruju, da li je IT funkcija učinkovita i djelotvorna te koliko uspješno doprinosi ostvarenju poslovnih ciljeva. U provedbi ove obveze vodstvo treba usko surađivati s menadžerima zaduženim za određena poslovna područja i odgovornim za ostvarenje konkretnih poslovnih ciljeva.
- Za zadaću *Usmjeriti*, vodstvo treba skrbiti da poslovni sustav funkcionira i da se ostvaruju njegovi planovi u skladu s dodijeljenim IT odgovornostima, a
- Za zadaću *Nadzirati*, vodstvo treba voditi računa da funkcioniraju svi dijelovi korporativnog upravljanja informatikom, a njegovi sudionici razumiju i ostvaruju svoje uloge te da se postižu planirane performanse.

Na sličan način ostvaruje se EDM ciklus i za druga načela. Više informacija o tome može se naći u ovoj normi.

2. Usluge ZIH-a

2.1. Konzultantski poslovi primjene norme ISO 38500

ZIH može pružiti cjelokupnu potporu u primjeni norme ISO 38500. Ova norma traži da se jasno identificiraju uloge i odgovornosti uprave i izvršnog menadžmenta u nekom poslovnom sustavu u definiranju njihovog očekivanja od IT-a i obvezuje ih da stvore uvjete za njeno djelotvorno i učinkovito korištenje. To na vrlo pojednostavljeni način prikazuje i slijedeći primjer - konkretni poslovni sustav želi podići razinu sadašnjeg načina korištenja svoje informatike na razinu korporativnog upravljanja. Da bi to učinio, nužno je odrediti novu viziju primjene IT-a s mjerljivim ciljevima, procijeniti sadašnje stanje korištenja IT-a, oblikovati strategiju prelaska u željeno, novo stanje i činiti nadzor njenog ostvarenja. Ova četiri koraka s najčešće korištenim metodama za njihovu realizaciju, prikazana su na slici 2.



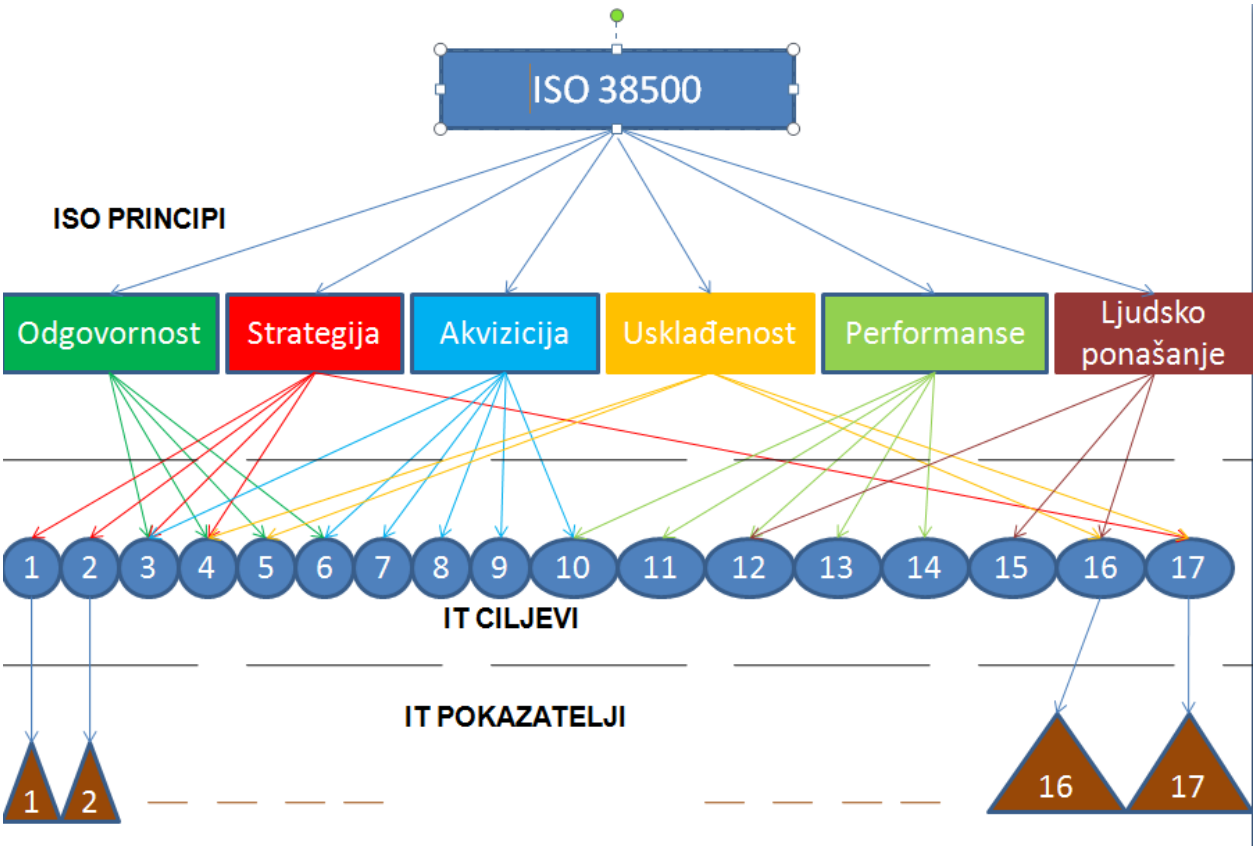
Slika 2. Mogući način korištenja norme ISO/IEC 38500

Polazište primjene jesu principi ove norme. Za svakog od njih određuju se IT ciljevi i IT indikatori, kako bi se mogao činiti nadzor ostvarenja postavljenih ciljeva. Obično se za svaki od 6 principa definira 3 do 6 IT ciljeva, koji se dalje kaskadiraju na primjerene IT indikatore. Npr., za princip *Odgovornost,* IT ciljevi mogu biti*:* 1.) učinci koji se očekuju od IT-a koji se žele postići primjenom ovog koncepta, 2.) način odlučivanja koji usklađuje poslovnu i IT strategiju, 3.) donošenje politike i izrada procedura koje su u skladu s propisima i međunarodnim normama, te 4.) odlučivanje o IT-u temeljiti na argumentiranim poslovnim razlozima. Također, na sličan način za druge principe ove norme, nužno je odrediti njihove IT ciljeve i IT pokazatelje. Time se dobije skup od 17 IT ciljeva visoke razine, prikazanih na slici 3.

Cilj	Opis cilja
1	Odrediti viziju i strategiju IT-a za cijeli poslovni sustav
2	Uskladiti strategiju poslovnog sustava i strategiju IT-a
3	Ostvariti IT ciljeve primjenom koncepta korporativnog upravljanja
4	Odlučivanje o IT-u provoditi u funkciji ostvarenja IT ciljeva
5	Donijeti IT politike u skladu s propisima
6	Imati poslovne argumente za svaku IT odluku
7	Provoditi ROI
8	IT projekti ostvaruju postavljene ciljeve
9	IT arhitekturu oblikovati u skladu s potrebama poslovnih procesa
10	Nabavu IT-a činiti tako da ona zadovoljava postavljene ciljeve
11	Ostvarivati novu primjenu IT-a u skladu s planovima
12	Nove IT usluge su na razini koju očekuju korisnici
13	Upravljati IT rizicima
14	Osigurati da su IT sustavi fleksibilni i prilagodljivi budućim promjenama
15	Provesti odgovarajuća osposobljavanja za nove metode i tehnologije
16	Skrbiti da IT strategija uvažava vrijednosti okoline
17	Razmjenjivati iskustva s drugim poslovnim sustavima

Slika 3. Skup postavljenih IT ciljeva visoke razine

Nakon što je određen skup IT ciljeva visoke razine kojima se realiziraju principi norme ISO/IEC 38500, treba načiniti njihovo međusobno povezivanje, npr. princip *Odgovornos*t, povezan je s IT ciljevima 3, 4, 5 i 6. Slika 4. prikazuje povezivanje svih 6 principa primijenjene norme i postavljenih 17 IT ciljeva.



Slika 4. Povezivanje principa norme ISO/IEC 38500, IT ciljeva i IT pokazatelja

Do sada prikazane radnje osnova su za procjenu sadašnjeg stanja načina korištenja i upravljanja informatikom. Da bi se načinila takva procjena, nužno je koristiti i druge pristupe, okvire i norme, kao što su COBIT, ISO/IEC 27001, ITIL i dr. Ovaj opis prešao bi domete ovog prikaza, zbog čega se u nastavku vrlo pojednostavljeno prikazuje rezultat procjene dobiven i iskazan u obliku CMM modela zrelosti, te način planiranja daljnjeg razvoja. Može se vidjeti da je trenutačna zrelost upravljanja informatikom u promatranoj tvrtki na razini 1, a kao strategija unapređenja i ciljana vrijednost, postavlja se razina zrelosti 2, dok je ova zrelost za industriju u kojoj tvrtka pripada, već na razini 2,5. Dakle, tvrtka neučinkovito koristi mogućnosti današnjih IT potencijala i odnos prema njima mora značajno promijeniti. Da bi se ova strategija ostvarila, tvrtka treba primijeniti strateško planiranje daljnjeg razvoja IT-a, pri čemu je i ovdje korisno kombinirati i već spomenute druge pristupe, okvire i norme (ISO/IEC 27001, ITIL, BSC, ISO 20000 i dr.) Slika 5. prikazuje to vizualno.

Slika 5. CMM rezultat sadašnjeg i ciljanog stanja upravljanja informatikom prema normi ISO/IEC 38500 u promatranoj tvrtki

Naša je procjena da su glavne prednosti norme ISO/IEC 38500 to što jasno identificira ulogu i odgovornost uprave i menadžmenta u definiranju njihovog očekivanja od IT-a i obvezuje ih da stvore uvjete za njeno djelotvorno i učinkovito korištenje prema EDC ciklusu. Iako ova norma predstavlja smjernicu, dobar je okvir za uspostavu i primjenu IT Governance-a, ali ju je nužno kombinirati i s drugim okvirima, metodologijama i standardima (COBIT, ISO/IEC 27001, ISO/IEC 31000, ITIL, ISO/IEC 20000-1 itd.) kojima se navedeni ciklus realizira.

2.2. Seminari, treninzi, radionice

ZIH pruža slijedeće vidove izobrazbi iz primjene norme ISO 38500**:**

- Motivacijska prezentacija poslovodstvu – prethodi odluci za pokretanje ovog poduhvata
- Radionica *ISO 38500*
    - ISO 38500 Foundation
    - ISO 38500 IT Corporate Governance Manager
    - ISO 38500 Lead IT Corporate Governance Manager

Priredio: Prof.dr.sc. Zdravko Krakar