DRAGUTIN VUKOVIĆ
KING ICT d.o.o., Zagreb
drago.vukovic@king-ict.hr

DALIBOR UREMOVIĆ
ALTER-INFO d.o.o., Zagreb
dalibor.uremovic@alterinfo.hr

SVE SE SVODI NA RIZIKE
UPRAVLJANJE RIZICIMA U INTEGRIRANIM SUSTAVIMA UPRAVLJANJA

Stručni rad/Professional paper

Sažetak

Upravljanje rizicima informacijske sigurnosti središnji je dio sustava upravljanja informacijskom sigurnošću prema normi ISO 27001. Upravljanje aspektima okoliša, koje zahtijeva norma ISO 14001, također je upravljanje rizicima, no onima koji se odnose na okoliš. Nacrt nove revizije norme ISO 9001, planiran za objavljivanje u 2015. godini, predlaže značajne promjene sustava upravljanja kvalitetom tako da će osnova biti upravljanje rizicima. Ovaj rad razmatra mogućnosti jedinstvenog upravljanja rizicima u integriranim sustavima upravljanja koji povezuju sve tri spomenute norme. Također se pokazuje primjer alata prikladnog za ovu namjenu.

Ključne riječi: *rizik, upravljanje rizicima, kvaliteta, integrirani sustavi upravljanja*

1. UVOD

Mnogo je već rečeno i raspravljano o tome kako je upravljanje rizikom budućnost upravljanja kvalitetom. Ali što to zapravo znači i kako to može funkcionirati? Ovo pitanje si sve više postavljaju savjetnici, menadžeri i ostali koji se bave upravljanjem kvalitetom u svojim organizacijama, posebno otkako je Međunarodna organizacija za standardizaciju ISO najavila za rujan 2015. godine objavljivanje nove revizije norme ISO 9001:2015 [1]. Uvidom u nacrt revizije ove norme, objavljen u lipnju 2013. godine [2], vidljivo je da se očekuju brojne promjene u strukturi i sadržaju dokumenta, kako to i najavljuje Nigel H. Croft, predsjednik tehničkog odbora ISO TC 176/SC 2, zaduženog za normu ISO 9001 [4]. Iako je revizija norme još u tijeku, prilično je jasno da su dvije najznačajnije promjene sasvim izvjesne: format norme u skladu s 'High Level Structure (HLS), prema Annex SL Appendix 2 ISO/IEC Smjernica [3] i uvođenje upravljanja rizicima kao osnove za upravljanje kvalitetom. U ovom radu razmatramo ovu drugu promjenu, upravljanje rizicima i njen mogući utjecaj na integrirane sustave upravljanja (ISU) u organizaciji.
Integrirani sustavi upravljanja najčešće u isti radni okvir povezuju sustav upravljanja kvalitetom prema normi ISO 9001, sustav upravljanja okolišem prema normi ISO 14001 i sustav upravljanja informacijskom sigurnošću prema normi ISO 27001. Norma ISO 27001 [5] od početka je uključivala zahtjev upravljanja rizicima informacijske sigurnosti, a u svojoj najnovijoj reviziji iz listopada 2013. godine usklađena je s HCL. Upravljanje okolišem prema normi ISO 14001 [6] također se temelji na upravljanju rizicima, a revizija norme najavljena za iduću godinu bit će usklađena s HCL. U slijedećem poglavlju razmotrit ćemo kako se upravljanje kvalitetom može povezati s rizicima.

2. POVEZIVANJE UPRAVLJANJA KVALITETOM I RIZICIMA

Razmotrimo neke uobičajene primijenjene definicije kvalitete: nula grešaka, zadovoljstvo kupca, kontrolirana varijanca procesa, pouzdanost, sigurnost, prikladnost za upotrebu. Sve to možemo promatrati kao ciljeve kojima težimo kroz upravljanje kvalitetom. Norma ISO 9000:2005, članak 3.1.1, definira kvalitetu kao „stupanj u kojem skup svojstvenih značajki ispunjava zahtjeve“. *BusinessDictionary.com* nudi ovu definiciju kvalitete: „U proizvodnji, mjera izvrsnosti ili stanje odsutnosti grešaka, nedostataka ili značajnih varijacija“. U razvoju softvera razlikuju se dvije mjere: funkcijska kvaliteta i strukturalna kvaliteta. Consortium for IT Software Quality (CISQ) i Object Management Group (OMG) definirali su pet glavnih poželjnih značajki potrebnih da bi neki softver ostvario poslovnu vrijednost: pouzdanost, učinkovitost, sigurnost, održivost i prikladnu veličinu. Promijenimo li gledište na kvalitetu u perspektivu rizika, ove uobičajene definicije postaju: rizik greške, rizik nezadovoljstva kupca, rizik nekontrolirane varijance procesa, rizik nepouzdanosti proizvoda, rizik sigurnosnog incidenta i rizik neprikladnosti za upotrebu. Drugim riječima – rizik neostvarivanja ciljeva kvalitete. U domeni rizika fokus nije na ciljevima kvalitete već na rizicima njihovog neostvarivanja. Upravljanje rizicima primjenjuje se kako bi rizici bili pod kontrolom, umanjila se vjerojatnost njihova događanja i njihov utjecaj na ciljeve kvalitete ako se dogode. Time se raste vjerojatnost ostvarenja ciljeva kvalitete.
Upravljanje kvalitetom se može promatrati kao proces oblikovanja i realizacije proizvoda i usluga koji u konačnici mora biti efektivan, efikasan i ekonomičan. Efektivnost je sposobnost proizvoda ili usluga da zadovolje ili premaše očekivanja kupca. Efikasnost podrazumijeva sposobnost stvaranja proizvoda i usluga bez nepotrebnog trošenja resursa. Ekonomičnost je sposobnost stvaranja prihoda neophodnog da bi organizacija bila održiva.
Upravljanje rizicima je proces kojim identificiramo, razmatramo, prioritiziramo i uklanjamo potencijalne uzroke neuspješnosti u postizanju ciljeva. Upravljanje rizicima postavlja pitanje „Što ako?“ te promatra vjerojatnosti i posljedice mogućih ishoda da bi odredilo koji 'što-ako' je značajan rizik koji moramo na prikladan način uvažiti i tretirati. Većina definicija upravljanja rizicima pokriva čitavu organizaciju. Tako Committee of Sponsoring Organizations (COSO) definira upravljanje rizicima kao: „*Proces kojeg provode uprava, menadžment i ostali zaposlenici, primijenjen na strateške odrednice u cijeloj organizaciji, oblikovan da identificira potencijalne događaje koji mogu imati utjecaj na organizaciju i upravlja rizicima da ih svede na prihvatljivu razinu kako bi se ostvarilo razumno osiguranje postizanja ciljeva organizacije*“.

2.2 Upravljanje rizicima i normizacija

Kako bi se osigurao dosljedan pristup upravljanju rizicima razvijeni su, i dalje se razvijaju, modeli i norme. Norme upravljanja rizicima pružaju slijedeće pogodnosti: referencu za proces upravljanja rizicima; suglasnost o najboljim praksama; definiciju radnog okvira za podršku odlučivanju u vezi s rizicima; zajednički rječnik za raspravu i usporedbu procesa upravljanja rizicima.
Neke od normi koje se temelje na upravljanju rizicima su: ISO 27000, za informacijsku sigurnost; ISO 28000, za sigurnost dobavnog lanca; ISO 22000, za zdravstvenu ispravnost hrane; FAA Safety Management System i AS 9100 za zrakoplovstvo.
Trenutno aktualna norma za upravljanje općenitim rizicima je ISO 31000:2009 [7]. U toj normi rizik je definiran kao „*učinak neizvjesnosti na ciljeve*“ a upravljanje rizicima je nešto što „*pomaže donošenju odluka uzimajući u obzir neizvjesnost i njene učinke na ostvarivanje ciljeva, te procjenjujući potrebe za poduzimanje akcija*“.

Norma ISO 31000 identificira kritične elemente upravljanja rizicima:

- Identifikacija rizika: identificira izvore rizika, rizične događaje i njihove potencijalne posljedice;
- Analiza rizika: analizira uzroke i izvore rizika i vjerojatnost njihovog događanja;
- Vrednovanje rizika: utvrđuje treba li rizike tretirati;
- Tretiranje rizika: utvrđuje strategije i mjere za ublažavanje i kontrolu rizika.

Nadalje, ISO 31000 tvrdi da upravljanje rizicima treba „*osigurati da organizacije trebaju imati primjeren odziv na rizike koji na njih utječu*“. Upravljanje rizicima stoga mora „*pomoći u izbjegavanju neefektivnih i neefikasnih odziva na rizike koji bi mogli, ali ne nužno, spriječiti legitimne aktivnosti ili izobličiti dodjelu resursa*“. Kako bi bilo efektivno unutar organizacije, upravljanje rizicima mora biti „*integralni dio općeg vladanja, upravljanja, izvještavanja, politika, filozofije i kulture*“.

Prema ISO 31000 upravljanje rizicima uključuje „primjenu logičkih i sustavnih metoda“ za:

- Komunikaciju i savjetovanje kroz cijeli proces;
- Uspostavljanje konteksta;
- Identificiranje, analizu, vrednovanje i tretiranje rizika pridruženih aktivnostima, procesima, funkcijama, projektima, proizvodima, uslugama i imovini;
- Nadzor i ocjenjivanje rizika;
- Primjereno bilježenje i izvještavanje o rezultatima.

2.3 Upravljanje rizicima: proaktivno - prediktivno - preventivno - preemptivno

Još jedan paralela između kvalitete i rizika je njihov respektivni fokus. Kvaliteta ima svog Deminga i njegov 'plan-do-check-act' (PDCA) ciklus. Danas sve priznatiji autoritet u domeni upravljanja rizicima, Greg Hutchins, identificira četiri P upravljanja rizikom: proaktivno-preventivno-prediktivno-preemprivno [8]. (Vrlo prikladno, u hrvatskom jeziku Demingov ciklus također možemo prikazati sa četiri P: planiraj-provedi-provjeri-poboljšaj.)

Analiza rizika je proaktivna po poduzimanju formalne analize za identificiranje, procjenu i brigu o rizicima. To uključuje prepoznavanje (predviđanje i navođenje potencijalnih rizika) te zatim analizu (ocjenjivanje u odnosu na ozbiljnost rizika). Ozbiljnost se određuje gledanjem na vjerojatnost rizika i rezultirajuće posljedice. Postoje različite metode za analizu rizika ali sve se mogu razvrstati u dvije kategorije: kvalitativne i kvantitativne. Kvalitativne analize oslanjaju se na stručnjake u specifičnom području koji na temelju svog znanja i iskustva ocjenjuju oboje, vjerojatnost i posljedice, koristeći neku stupnjevanu skalu (1-5, nisko/ srednje/visoko, i slično) ili koristeći toplinske mape (heatmaps). Kvantitativne analize oslanjaju se na upotrebu numeričkih vrijednosti za vjerojatnost i posljedice jer se to smatra objektivnijom procjenom. Za određivanje vrijednosti koriste se povijesni ili znanstveni podaci o procesu ili aktivnosti. Ove metode zahtijevaju razumijevanje teorije vjerojatnosti. Bez obzira koja metoda analize se koristi, očigledno je da se rizicima s velikom vjerojatnošću i jakim posljedicama mora posvetiti veća pažnja.

Kad su značajni rizici utvrđeni, njima se možemo svjesno baviti. U slučajevima kad postoje kvalitetni podaci moguće je ukloniti dio neizvjesnosti. Uklanjanje neizvjesnosti povećava našu sposobnost prediktivnog djelovanja, tj. predviđanja pojave rizičnog događaja. Primjenom mjera za tretiranje rizika rizici se mogu spriječiti ili umanjiti, na primjer tako da obustavimo aktivnosti koje su izvor rizika, smanjimo vjerojatnost pojave rizika ili smanjimo njegove posljedice po organizaciju. Time smo ostvarili preventivno djelovanje. Ukoliko nismo u mogućnosti djelovati na samu pojavu rizičnog događaja, možemo podijeliti njegove posljedice s drugima, na primjer osiguranjem od štetnog događaja, prijenosom dijela aktivnosti na partnere i slično. Time smo preduhitrili rizični događaj, tj. ostvarili preemptivno djelovanje.

Ključno je ovdje primijetiti da čitav ovaj proces predstavlja svjesni trud koji mora po svojoj prirodi biti vidljiv menadžmentu organizacije. Promjenom perspektive stvorili smo pogled na kvalitetu kao funkciju rizika i pomakli se iz pretežno reaktivnog pristupa mjerenjem i kontrolom varijanci ka proaktivnom pristupu identificiranja, analizirana i tretiranja potencijalnih izvora nekvalitete.

3. IMPLEMENTACIJA ISO 9001 POMOĆU UPRAVLJANJA RIZICIMA

Organizacije najčešće identificiraju i razvrstavaju procese u tipične kategorije kao što su operativni procesi, pomoćni procesi i vanjski procesi. Skup kontrola prakticiranih nad ovim procesima čini njihov sustav upravljanja kvalitetom. Mnoge organizacije i njihovi savjetnici za ISO 9001 implementiraju procese upravljanja kvalitetom na vrlo površan način što rezultira sustavom koji ne stvara vrijednost za organizaciju pa tako niti ne ostvaruje povrat investicije u implementiranje i održavanje sustava. Glavni razlog zašto se takve organizacije certificiraju prema normi ISO 9001 je zadovoljavanje ugovornih obveza prema kupcima. Međutim, ISO 9001 može pružiti mnogo više organizacijama koje ga implementiraju na pravi način. Učinkovito upravljanje rizicima u svakom procesu i njihovom međudjelovanju može rezultirati velikim poboljšanjima produktivnosti pa posljedično i konačne bilance poduzeća.

3.1 Kako kontrolirati procese upravljajući rizicima

Procesi tipično imaju ulaze, izlaze i aktivnosti koje dodaju vrijednost. Svaka od tih odrednica procesa koristi različite resurse koje možemo razvrstati u sedam grupa, poznatih kao 7M: materijale (Materials), strojeve i opremu (Machinery), ljude (Manpower), okoliš (Milieu), postupke (Methods), mjerenja (Measurements) i upravljanje (Management). Pri korištenju tih resursa organizacija će iskusiti različite stupnjeve rizika i morat će primijeniti prikladne mjere (kontrole) za umanjivanje svoje izloženosti tim rizicima.
U analizi rizika vezanih uz navedene resurse možemo koristiti neke poznate alate kao što su analiza uzroka i posljedica (Fishbone/Ishikawa dijagram) ili FMEA (Failure Mode and Effects Analysis). Kako koristiti ove alate za analizu rizika ostavljamo za neku drugu raspravu. Ovdje ćemo pregledno navesti neke od resursa povezanih s rizicima kvalitete i njima pridružene mjere (kontrole) namijenjene upotrebi u sustavu upravljanja kvalitetom.

Tabela 1: Resursi povezani s rizicima kvalitete

Materijali (Materials) - Upravljanje inventarom - Inspekcija/testiranje - Normizacija - Specifikacije - Upravljanje dobavljačima - Identifikacija - Sljedivost - Praćenje obrta materijala - Čuvanje materijala	**Postupci (Methods)** - Sustavi upravljanja - Standardni postupci - Inspekcija/testiranje - Planovi kvalitete / kontrolne liste - Radne upute - Sastavnice - Tehnologija/automatika/robotika - Operacijski i administracijski softver - Dijagrami tijeka procesa - FMEA / nadzor procesa - Nacrti/planovi
Strojevi i oprema (Machinery) - Sposobnosti/kapaciteti/tehnologija - Inženjering/podrška	**Mjerenja (Measurement)** - Ciljevi/praćenje/ocjenjivanje/poboljšavanje - Norme/pravila/regulativa

- Inspekcija/mjerenje - Ispitna oprema - Alati/pribor - Održavanje/potrošni materijal - Razmještaj opreme	- Specifikacije/tolerancije/kriteriji - Operativni podaci/statistike - Statistička kontrola procesa - Efikasnost/efektivnost - Zadovoljstvo kupca - Uspoređivanje (benchmarking)
Ljudi (Manpower) - Vještine/znanje/iskustvo - Trening/osposobljavanje - Odgovornosti/ovlaštenja - Motivacija/moral - Primjerenost osoblja - Zdravlje/sigurnost	**Upravljanje (Management)** - Vodstvo/planiranje - Politike/ciljevi - Posvećenost/uključenost - Organizacija/resursi - Ocjenjivanje/poboljšavanje - Komunikacija
Okoliš (Mileu) - Upravljanje zgradama/prostorima - Kontrola okoliša - Klimatizacija/ventilacija/kvaliteta zraka - Održavanje/zdravlje/sigurnost - Osvjetljenje / kontrola buke - Mjere u slučaju opasnosti	

Svaki od ovih resursa predstavlja mogući izvor rizika u procesima koje želimo kontrolirati našim sustavom upravljanja kvalitetom. Svaka od njima pridruženih mjera primjenom može umanjiti izloženost specifičnim rizicima koji se mogu pojaviti u procesima. U tom kontekstu primjena upravljanja rizicima, sukladno normi ISO 31000, okvirno će izgledati ovako:

Identifikacija rizika:
- utvrditi koji od ovih resursa se odnose na svaki od identificiranih procesa u našem sustavu upravljanja kvalitetom;
- izraditi popis/registar svih instanci resursa;
- utvrditi ranjivosti pojedinih resursa i prijetnje kojima resursi mogu biti izloženi.

Analiza rizika:
- istražiti uzroke i izvore rizika;
- utvrditi vjerojatnost njihovog događanja;
- procijeniti posljedice nakon nastanka rizičnog događaja.

Vrednovanje rizika:
- uzimajući u obzir vjerojatnost nastanka i posljedicu rizika, utvrditi izloženost organizacije riziku; izloženost se najčešće određuje kao umnožak vjerojatnosti i posljedice rizika, ali moguće su i neke druge formule, ovisno u usvojenoj metodi procjene rizika;
- rangirati rizike prema izloženosti;
- odrediti koji rizici su prihvatljivi, a koje treba tretirati.

Tretiranje rizika:
- utvrditi kombinaciju mjera primjenjivu na pojedine resurse ili procesne varijable – ulaze, izlaze, aktivnosti; popis ovih mjera obično se naziva 'Izjava o primjenjivosti' (Statement of Applicability);
- Izraditi plan implementacije mjera;
- Implementirati primjenjive mjere u skladu s planom;
- Nadzirati i verificirati efektivnost mjera.

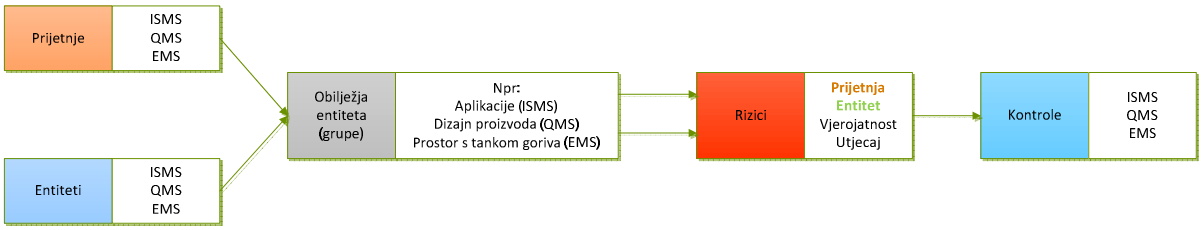
4. RIZICI U INTEGRIRANIM SUSTAVIMA UPRAVLJANJA

Već je rečeno da je ISO 31000 trenutno aktualna norma koja se koristi za upravljanje općenitim rizicima, usvojena i kao temelj sve nove i buduće revizije normi koje propisuju razne sustave upravljanja. Tako se i nova revizija norme ISO 27001 koja se bavi sustavima upravljanja informacijskom sigurnošću sada referencira na nju, a isto se odnosi i na sustave upravljanja kvalitetom sa sljedećom revizijom ISO 9001 norme.
Ovo predstavlja realizaciju strategije ISO odbora prema kojoj je moguće sve rizike voditi putem iste metodologije pa nije učinkovito raditi na nekoliko raznih metodologija, specifičnih za svaki sustav upravljanja. Slijedeće sheme i tabele pokazuju kako je moguće primijeniti iste korake koje propisuje ISO 31000 na rizike sustava upravljanja kvalitetom, ali i primjerice na rizike sustava upravljanja informacijskom sigurnošću i sustave upravljanja okolišem. Za potrebe daljnje razrade, koristit će se angloameričke skraćenice za sustave upravljanja kako se navode u svakoj normi i to:

- ISMS (engl. Information Security Management System) – sustav upravljanja informacijskom sigurnošću;
- QMS (engl. Quality Management System) – sustav upravljanja kvalitetom;
- EMS (engl. Environmental Management System) – sustav upravljanja okolišem.

Alat u kojem ćemo provesti slijedeće korake je web aplikacija AlterRisk™ [9] koja se koristi za automatiziranje postupaka upravljanja resursima (entitetima), analize utjecaja na poslovanje, procjene i obrade rizika, kao i za izvješćivanje o statusu sukladnosti organizacije sa poznatim svjetskim normama i standardima za sustave upravljanja (npr. ISO 27001, ITIL, CobIT i sl.).
Kako bi se isti koraci procesa upravljanja rizikom mogli primijeniti unutar različitih sustava upravljanja, potrebno je naći one korake kod kojih postoje specifični elementi u odnosu na svaki sustav. Slijedeća shema logički pojednostavljeno prikazuje proces upravljanja rizikom s temeljnim elementima koji se moraju definirati.

Slika 1: Proces upravljanja rizikom



U prethodnom poglavlju utvrđeno je da je potrebno identificirati resurse (entitete) za koje će se identificirati rizici. Ukoliko radimo s istom metodologijom, ali unutar različitih sustava upravljanja, tako će i resursi (entiteti) biti specifični za svaki od sustava. Tako, primjerice, unutar ISMS-a možemo naći entitete tipa Aplikacije, Hardver ili Podaci, unutar QMS-a entitete tipa Postupci, Materijali, Ljudi i sl., a unutar EMS-a entitete tipa Prostora za odlaganje otpada, Kemijske supstance, Strojeve za rad s opasnim tvarima i sl.
Na svaki od takvih entiteta djeluju neke prijetnje specifične za grupu odnosno obilježje kojem pripada pojedini entitet. Slijedeća tabela prikazuje neke od mogućih prijetnji za entitete tipa Aplikacije (za ISMS), postupak Inspekcije/testiranja (za QMS) te Prostora sa tankom goriva (za EMS).

Tabela 2: Primjeri prijetnji u različitim sustavima upravljanja

ISMS	
Aplikacije	Neovlašteni pristup informacijama
	Maskiranje/krivo predstavljanje djelatnika
	Nemogućnost rekonstrukcije događaja
	Spor odziv sustava
	Greške u aplikacijama
	Gubitak administratorskih zaporki/kriptografskih ključeva
	Zlouporaba privilegiranih/administratorskih računa
QMS	
Inspekcija/testiranje	Neprovođenje inspekcije
	Nevjerodostojni rezultati zbog malog uzorka
	Nestručnost osoblja za testiranje
	Nebaždareni/neadekvatni alati za testiranje
	Zastoj u radu zbog neplaniranih inspekcija
EMS	
Prostor sa tankom goriva	Prolijevanje tijekom pražnjenja ili punjenja tanka
	Zagađenje vode i tla tijekom čišćenja tanka
	VOC emisija tijekom punjenja vozila s gorivom
	Eksplozija tanka
	Curenje goriva kroz pukotine tanka

Ukoliko analiziramo ove identificirane prijetnje nad svakim entitetom navedenih tipova, dobit ćemo popis rizika koje je potrebno procijeniti odnosno vrednovati. Takav popis rizika sadržavat će sve parove entiteta i prijetnji kao na primjeru slijedećih rizika: spor odziv sustava u aplikaciji SoftwareTool; zlouporaba privilegiranih/administratorskih računa u aplikaciji SoftwareTool; nevjerodostojni rezultati zbog malog uzorka u procesu testiranja proizvoda X; zagađenje vode tijekom čišćenja tanka br. 6; eksplozija tanka br. 6; i slično.
Većina normi koje se bave upravljanjem rizicima navode sličnu metodu za vrednovanje rizika uzimajući u obzir vjerojatnost nastanka i posljedicu rizika. Rezultat operacije uparivanja vjerojatnosti i posljedice odnosno utjecaja je matrica vrijednosti rizika, kao u slijedećem primjeru.

Tabela 3: Matrica vrijednosti rizika

	Utjecaj			
Vjerojatnost ostvarivanja prijetnje	Vrlo veliki (100)	Umjereno veliki (60)	Srednji do mali (30)	Vrlo mali (10)
Vrlo velika (1)	Vrlo visok (100)	Vrlo visok (60)	Visok (30)	Srednji (10)
Umjereno velika (0,6)	Vrlo visok (60)	Visok (36)	Srednji (18)	Nizak (6)
Srednja do mala (0,3)	Visok (30)	Srednji (18)	Nizak (9)	Nizak (3)
Vrlo mala (0,1)	Srednji (10)	Nizak (6)	Nizak (3)	Nizak (1)

I dok se za vjerojatnost ostvarivanja prijetnje može koristiti ista definicija za svaku od kategorija u skali vjerojatnosti, definicije posljedica odnosno utjecaja mogu biti ponešto različite za svaki od sustava upravljanja. Slijedeća tabela daje jedan mogući set definicija utjecaja za svaku kategoriju iz odabrane skale za vrednovanje za svaki od promatranih sustava upravljanja.

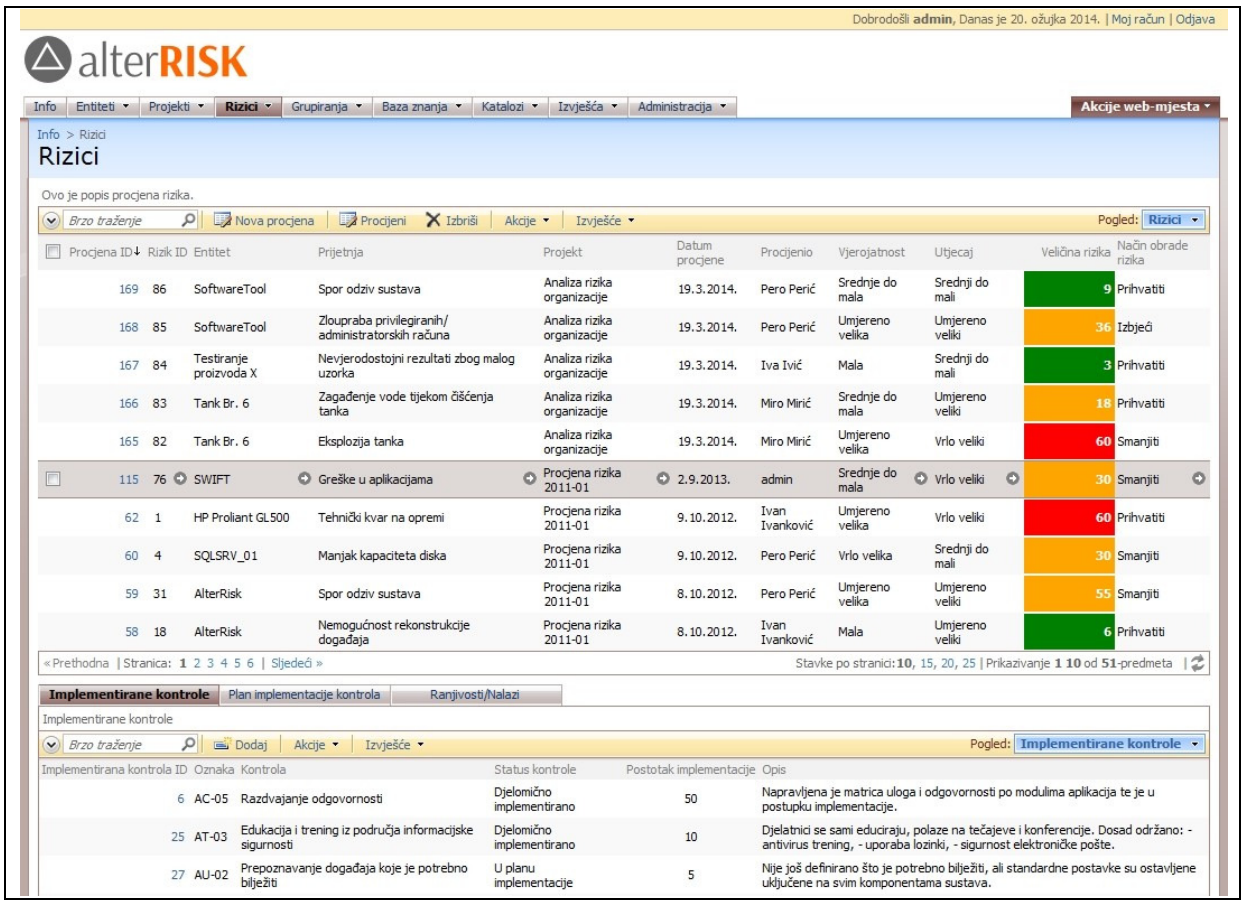
Tabela 4: Primjeri definicija utjecaja

Utjecaj	ISMS	EMS	QMS
Vrlo veliki	Vrlo veliki procijenjeni gubici organizacije. Zbog prirode prijetnje odnosno manjka sigurnosnih mjera u potpunosti se realizira njeno štetno djelovanje po obilježje informacijske imovine.	Potpuno iscrpljenje specifičnih prirodnih resursa u lokalnom okolišu; jako onečišćenje okoliša s trajnim ili dugotrajnim posljedicama; moguć gubitak života i značajnih šteta po zdravlje stanovništva; zakonske sankcije; značajni financijski gubitci zbog kazni, troškova sanacije i naknada oštećenima; snažan negativni publicitet i mogući prestanak poslovanja organizacije.	Značajno ugrožavanje života i zdravlja kupaca uslijed neispravnosti ili štetnog djelovanja proizvoda, neetičnosti ili nekvalitete pružanja usluga; zakonske sankcije; značajni financijski gubitci zbog povlačenja i popravaka proizvoda, kazni i naknada oštećenima; nekontrolirana učinkovitost procesa; snažan negativni publicitet i mogući prestanak poslovanja organizacije.
Umjereno veliki	Umjereno veliki procijenjeni gubici organizacije. Zbog prirode prijetnje odnosno manjka sigurnosnih mjera u znatnoj mjeri se realizira njeno štetno djelovanje po obilježje informacijske imovine.	Djelomično iscrpljenje specifičnih prirodnih resursa; značajno onečišćenja okoliša s nužnom hitnom sanacijom; nepovoljan utjecaj na zdravlje lokalnog stanovništva; zakonske sankcije; financijski gubitci zbog kazni, troškova sanacije i naknada oštećenima; značajan negativni publicitet i smanjenje tržišnog udjela.	Utjecaj na zdravlje uz značajno nezadovoljstvo kupaca kvalitetom proizvoda i usluga; zakonske sankcije; značajni financijski gubitci zbog zamjene i popravaka proizvoda, kazni i naknada oštećenima; slaba kontrola učinkovitosti procesa; negativni publicitet i smanjenje tržišnog udjela.
Srednji do mali	Srednje veliki procijenjeni gubici organizacije. Zbog prirode prijetnje odnosno manjka sigurnosnih mjera u djelomičnoj mjeri se realizira njeno štetno djelovanje po obilježje informacijske imovine.	Utjecaj na raspoloživost prirodnih resursa; umjerena onečišćenja i negativan utjecaj na kvalitetu okoliša bez trajnog djelovanja na zdravlje ljudi; manje zakonske sankcije; troškovi zbog kazni i sanacija; negativan publicitet s blažim utjecajem na poslovanje.	Bez utjecaja na zdravlje uz nezadovoljstvo kupaca pojedinim svojstvima proizvoda; zamjetni troškovi zamjene i popravaka proizvoda; učinkovitost procesa kontrolirana; manji negativan publicitet s blažim utjecajem na poslovanje.
Mali	Vrlo mali procijenjeni gubici organizacije. Zbog prirode prijetnje odnosno postojanja sigurnosnih mjera, realizacija štetnog djelovanje po obilježje informacijske imovine je nisko do zanemarivo.	Bez većeg utjecaja na prirodne resurse; onečišćenja okoliša mala do zanemariva, lokalizirana i kratkotrajna; bez utjecaja na zdravlje stanovništva; troškovi kazni i sanacija zanemarivi; bez negativnog publiciteta i utjecaja na poslovanje.	Sporadični slučajevi nezadovoljstva kupaca kvalitetom proizvoda i usluga; predvidivi troškovi zamjene i popravaka; učinkovitost procesa optimirana; bez negativnog publiciteta i utjecaja na poslovanje.

Procjena vjerojatnosti ostvarivanja prijetnje i utjecaja na organizaciju često nije jednostavna bez obzira koliko detaljno definirali svaku od kategorija vjerojatnosti ili utjecaja. Za lakšu i

objektivniju procjenu bi zato trebali koristiti podatke o trenutnom statusu implementiranih kontrola koje smanjuju rizik odnosno postojanju ranjivosti koje rizik povećavaju. Za identifikaciju kontrola možemo se poslužiti nekim od poznatih normi, standarda odnosno dobrih praksi za pojedini sustav upravljanja, kao što je to primjerice ISO 27002 za sustave upravljanja informacijskom sigurnošću. Kako može izgledati jedna takva procjena rizika prikazano je slijedećom snimkom ekrana iz alata AlterRisk™.

Slika 2: Primjer procjene rizika u alatu AlterRisk™



Kontrole koje će primijeniti organizacija za smanjivanje neprihvatljivih rizika biti će specifične za svaki od rizika kojeg obrađujemo unutar nekog od sustava upravljanja, ali postupak je isti. Kao što je vidljivo iz snimke, moguće je koristiti softverski alat koji podržava ISO 31000 metodologiju za rizike bilo kojeg sustava upravljanja. Ovim se organizacija približava integriranom sustavu upravljanja za koji vrijede ista načela i postupci uz uvažavanje specifičnosti svakog od pojedinih sustava upravljanja.

5. ZAKLJUČAK

Ovaj rad daje kratki pregled upotrebe pristupa implementaciji ISO 9001 primjenom upravljanja rizicima. Namjera nam je potaknuti razmišljanje i istraživanje u smjeru prepoznavanja i vrednovanja rizika koji se mogu povezati s procesima koji utječu na kvalitetu. Upravljanje rizicima je moćan način za implementiranje ISO 9001 kako bi se učinkovito kontrolirali poslovni procesi i ostvarilo značajna poboljšanja u smislu zadovoljstva korisnika i profitabilnosti. Svakom slijedećom revizijom neke od danas poznatih

normi kao što su ISO 9001, ISO 27001 ili ISO 14001, ISO odbor jasno daje do znanja da je ključ učinkovitosti organiziranja sustava upravljanja u ideji integriranog sustava upravljanja. Osim referenciranja na zajedničku metodologiju upravljanja rizicima koji trebaju poslužiti kao osnova za odabir kontrola, ovu ideju moguće je prepoznati i u novoj organizaciji poglavlja svake od normi koja također slijedi isti format definiran Aneksom SL ISO direktive. Ovakvim pristupom, organizacije će svaki slijedeći sustav upravljanja moći implementirati sve brže jer će koristiti iste metodologije, alate i postupke što bi u konačnici rezultiralo učinkovitim procesima integriranog sustava upravljanja.
Jedan od bitnih motiva za reviziju ISO 9001 u smislu uvođenja pristupa putem upravljanja rizicima u sustave upravljanja kvalitetom jest olakšavanje integriranja ovih sustava s drugim sustavima upravljanja. U tom smislu je metodologija i postupak upravljanja rizicima jaki integrativni element na razini cijele organizacije. Valja ipak imati na umu da su norme samo alati za poslovno upravljanje, stoga dobrobiti koje od njih može imati organizacija ovise o tome koliko se one učinkovito primjenjuju.

LITERATURA

[1] ISO, http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1751 , 2013.

[2] *ISO/CD 9001 - Committee Draft of ISO 9001*, Secretariat of ISO/TC 176/SC 2, 2013.

[3] *ISO/IEC Directives, Part 1, Consolidated ISO Supplement — Procedures specific to ISO*, *Fourth edition*, International Organization for Standardization & International Electrotechnical Commission, 2013.

[4] Nigel H. Croft, *ISO 9001:2015 and beyond - Preparing for the next 25 years of quality management standards*, http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1633, 2012.

[5] ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements

[6] ISO 14001:2004 Environmental Management Systems

[7] ISO 31000:2009 Risk management — Principles and guidelines

[8] Greg Hutchins, Proactive – Preventive – Predictive – Preemptive, u ISO9001:2015@Risk™, http://insights.cermacademy.com/2013/03/proactive-preventive-predictive-preemptive/, 2014

[9] Alter info d.o.o. – AlterRisk™ v3.2 – korisnička dokumentacija, 2014.

EVERYTHING'S COMING UP RISKS
RISK MANAGEMENT IN INTEGRATED MANAGEMENT SYSTEMS

Summary

Information security risk management is the central part of an ISO 27001-compliant information security management system. Environmental aspects management, required by the ISO 14001 standard, is nothing else but management of environment-related risks. The draft of the new revision of the ISO 9001 standard, scheduled for release in 2015, proposes significant changes in quality-management systems, so that risk management will serve as a foundation for quality-management. This paper discusses the possibilities of unified risk management in integrated management systems, connecting all three standards mentioned here. A software tool, suitable for this purpose, is also presented.

Keywords: *risk, risk management, quality, integrated management systems*