ASOCIJACIJA ZA KVALITET I STANDARDIZACIJU SRBIJE

FESTIVAL KVALITETA 2007.
34. Nacionalna konferencija o kvalitetu
Kragujevac, 08. - 11. maj 2007.

KVALITET INTERAKCIJA U ZAJEDNICAMA PRAKSI I SISTEMI MENADŽMENTA ZNANJA

QUALITY OF INTERACTION AT COMMUNITIES OF PRACTICE AND KNOWLEDGE MANAGEMENT SYSTEMS

Prof. dr Milorad K. Banjanin, Aleksandar Sredojević, dipl.inž.

Sadržaj: *Mnoge organizacije u okviru inicijativa menadžmenta znanja razvijaju zajednice prakse (Communities of Practice-CoPs) sa idejom umrežavanja ljudi koji imaju zajednička interesovanja i s ciljem unapređenja učenja tokom zajedničkog rada. Mnoge CoPs su interne za kompanije ali u novije vreme dolazi do uključivanja članova drugih kompanija (savezi i partnerstva). Taj trend za sobom povlači brojne rizike vezane za raspoloživost informacija, zaštitu pristupa, integritet znanja unutar skladišta znanja i ostale rizike vezane za bezbednost i kontrolu sistema menadžmenta znanja. S tim ciljem, dat je okvir za obezbeđivanje sistema menadžmenta znanja- reviziju znanja i kontrolu tokova znanja.*
Ključne reči*: menadžment znanja, deljenje znanja, CoPs, sistem menadžmenta znanja, menadžment rizika, bezbednost, kontrole.*

Abstract: *CoPs are expected to play a significance role in future organizations learning. Theirs difference from project teams is presented by theirs main goal, knowledge sharing. Knowledge management systems are proliferating through organizations as management seeks to gain competitive advantage by enhancing and sharing knowledge across the organizations. Unfortunately there are risks and consequences associated with knowledge management systems that may not be adequately controlled and audited, and may breach privacy concerns and legislation. This paper addresses these issues and provide framework and guidelines for management to provide assurance over their KM systems.*

1. UVOD

Zajednice možemo definisati kao mreže ljudi sa sličnim problemima, pitanjima i potrebama [3]. Zajednice prakse ili CoPs se mogu definisati kao*" neformalna mreža ljudi koji rade zajedno, koji dele zajednička interesovanja u specifičnim oblastima znanja ili kompetencija, koji imaju opredeljenje da rade i uče zajedno tokom vremenskog perioda razvijajući i deleći znanje ".*

Koncept "zajednice prakse" prvi su uveli Lave i Wenger 1991. godine nakon stečenog uverenja da je sticanje znanja *socijalni proces* gde ljudi učestvuju u komunalnom učenju na različitim nivoima i zavisno od nivoa autoriteta ili pozicije u grupi u kojoj su novi ili su članovi duže vreme.

Kao primeri zajednica prakse mogu se uzeti: *grupa umetnika* koja traži nove oblike izražavanja, *grupa inženjera* koji se sreću jednom nedeljno za vreme pauze za kafu da bi podelili ideje ili istražili slične probleme, *grupa hirurga* koja istražuje nove operativne tehnike itd. CoPs postoje u mnogim različitim oblicima, veličinama, i različito se nazivaju u mnogim kompanijama jer još uvek dosta eksperimentišu sa njima.

Zajednice prakse imaju potencijal da dramatično promene način na koji preduzeća funkcionišu i stiču konkurentnost jer su one mehanizam kroz koji se znanje i kreira i primenjuje u praksi. Znanje je ekstremno vredan resurs kako za pojedinca tako i za organizaciju i jedini je resurs koji se ne troši. Mnogi pojam ''znanje'' vezuju za organizaciju i čoveka ali, ima i onih koji su okrenuti tehničkim rešenjima kao npr. kreiranju baza znanja koje sadrže eksplicitne forme znanja predstavljene preko seta podataka.

U osnovi, postoje podela znanja na *eksplicitno* i *implicitno*. Eksplicitno znanje je kodifikovano, tj. može se potpuno predstaviti preko pisanih sredstava (štampa, formule) i relativno i lako artikulisati i saopštiti. Implicitno znanje nema te karakteristike i daleko je komplikovanije obezbediti kontekst za njegov transfer i deljenje. Implicitno znanje je sadržano u glavama ljudi,

1) Fakultet tehničkih nauka Univerziteta u Novom Sadu

neizrečeno je (tacit znanje), i vrlo ga je teško opisati i izraziti. Obično se saopštava određenim oblicima prezentovanja ili pokazivanja (demonstracijom) i iskazuje mentalne, materijalne i biheviоralne performanse ili njihovu integraciju u kategoriji individualnih vestina [3]. Pokazalo se da je najbolji način za transfer implicitnog znanja zajednički rad tj. saradničko učenje (tim, zajednica itd.).

Upravljanje znanjem *(Knowledge Managemant- KM)* se može definisati kao ''multidisciplinarni prilaz za postizanje organizacionih ciljeva najboljim korišćenjem raspoloživog znanja'' [2]. To se postiže identifikacijom, najboljim prilagođavanjem i aktivnim upravljanjem intelektualnim dobrima, bilo da se radi o eksplicitnom, ili implicitnom znanju.

Bezbednost i kontrole u skladištima znanja predstavljaju neophodnost kako bi se banka znanja jedne organizacije sačuvala od brojnih rizika i time omogućio razvoj i deljenje znanja- sticanje konkurentskih prednosti.

2. ZAJEDNICE PRAKSE- COPS

CoPs se kreiraju s namerom olakšavanja transfera implicitnog znanja jer je znanje u suštini društveno bazirano i poseduju ga grupe i pojedinci. CoPs imaju potencijal za deljenje i eksplicitnog i implicitnog znanja i u svrhu podrške tom procesu neophodna je **tehnička infrastruktura** sa čitavim kolekcijama kolaborativnih alata. Najveći preblem sa CoPs je da ih njihova organska i neformalna priroda čini veoma odbojnim za kontrolu i monitoring, odnosno nepotrebno mešanje u njihove aktivnosti od strane menadžmenta. Međutim, ako kvalitet menadžmenta nije adekvatan, zajednica se često raspada [2].

Unutar CoPs-a ljudi direktno sarađuju, uče jedni od drugih, dele iskustva i znanja na načine koji gaje inovativnost i najviši nivo poverenja. Rezultat toga je da su CoPs snaga koja je i *socijalna i profesionalna* i koja operiše izvan tradicionalnih organizacijskih granica i hijerarhije.

Stvarnu zajednicu prakse, određuju međusobno zavisna tri bitna entiteta: *Domen* (ono šta znaju)- članovi se okupljaju oko zajedničkog domena identifikujući se sa zajedničkim poduhvatom; *Identitet zajednice* (ono što jesu)- ljudi funkcionišu u zajednici kroz veze u zajedničkom angažovanju koje spajaju članove zajedno u društvenu jedinku; *Praksa* (ono šta rade)- zajednica gradi mogućnosti u svojoj praksi stvarajući zajedničku bazu resursa: alate, dokumente, rutine, vokabular, simbole. Akumulirano znanje služi za buduće učenje [3]. One su kanali za znanje koje preseca granice kreirane od strane toka rada, funkcija, prostora i vremena.

Kriterijum	Zajednice prakse	Timovi
Cilj	Širenje znanja i unapređivanje učenja u pojedinim oblastima	Kompletiranje specifičnih projekata
Članstvo	Slobodno izabrano-dobrovoljno; uključujući vanredne i marginalne članove	Selektovano na osnovu sposobnosti doprinosa timskim ciljevima; puno vreme
Organizac-ija	Neformalna; samoorganizacija, rukovođenje varira prema predmetima	Hijererhijska, sa vođom projekta-menadžerom
Trajanje	Razvija se u hodu vremena a; raspušta samo kada ne postoji interes za dalje postojanje	Traje sve dok jse deo ili celi projekat ne kompletira (U nekim slučajevima, tim može evoluirati u zajednicu)
Vrednosti	Generativne vrednosti u razmeni znanja i informacija	Materijalne i druge vrednosti koje grupa-tim isporučuje u rezultatima koje proizvodi
Menadž-ment	Stvaranje veza između članova; obezbeđivanje svežih i vrednih tema	Koordinacija mnogo nezavisnih zadataka.

Tabela 1. RAZLIKE IZMEĐU CoPs-a i TIMOVA

Kod oblikovanja elemenata uspešne zajednice posebnu pažnju treba obratiti na izgradnju *poverenja* i stvaranje *socijalnog kapitala*.

CoPs se razlikuju od ostalih organizacionih grupa kao što su timovi, interesne zajednice, mreže u sledećem:

1. **Vreme** je bitan resurs koji je potreban da bi se razvile CoPs, što znači da postoji istorija učenja;
2. **Inicijativa** ili ideja oko koje će se formirati dodatna vrednost za pojedince je takođe potrebna, ali ne postoji program rada ili akcioni predmeti kao što to imaju projektni timovi;
3. **Učenje** je ključni element ove inicijative. CoP razvija sopstvene načine postupanja sa ''svojim svetom'' a posledica toga je:
   - ❖ CoPs su odgovorne samo sebi i svojoj politici tj. ne postoji formalni šef a lideri teže da se pojavljuju samo pri pojavi novog predmeta debate.
   - ❖ Odnosi unutar CoPs-a se stvaraju u toku rada, neodređeni su i teže da budu okarakterisani međusobnim poverenjem.

- CoPs se brinu više za sadržaj nego za formu. Kao rezultat toga, one nisu podložne identifikovanju i imenovanju jedinica.

Tabela 1. pokazuje kriterijume (*cilj, članstvo, organizacija, trajanje, vrednosti, menadžment*) po kojima se razlikuju CoPs od timova. Moguće je da pojedini tipovi grupa eventualno evoluiraju u CoPs iako ne poseduju prave oznake CoPs-a. Slobodnije spojene grupe mogu više koristiti svrhama CoPs-a i one predstavljaju razvojno okruženje za nove zajednice [2]. Takođe, unutar CoPs-a postoje različiti, legitimni tipovi učešća tj. ne treba svi članovi CoPs-a da budu jednako aktivni.

CoPs se najčešće poistovećuju sa timovima, ali za razliku od timova, CoPs su tipično *dobrovoljne* i *nestruktuirane* grupe sa članstvom koje po svojoj pripadnosti preseca unutrašnje i spoljašnje organizacione granice.

Jedinstven put ka razvoju CoPs-a se kreće najpre od njihovog identifikovanja, zatim pokretanja funkcionalnosti i na kraju održavanja. Uobičajen pristup za *identifikovanje* CoPs-a je pronalaženje neformalnih grupa koje već operativno deluju i podrške da se međusobno povežu kao zajednica. *Pokretanje* funkcionisanja CoPs-a može predstavljati problem. Zato je potrebno pre svega shvatiti prepreke, učiniti znanje lakim za upotrebu, meriti vrednosti, razviti poverenje, uspostaviti koordinacione uloge, motivisati ljude, i nadgledati evoluciju. CoPs u procesu *održavanja* zahteva posebne oblike "kultivizacije" i neophodnu podršku menadžmenta, prihvatanje od strane organizacione kulture i svakako, tehnička infrastruktura.

3. TEHNIČKA INFRASTRUKTURA TRANSFERA ZNANJA U COPS-U

Kada se govori o tehničkoj infrastrukturi transfera znanja u CoPs-u potrebno je pomenuti sledeće elemente sistema informaciono-komunikacione podrške:

- *Lokalna podrška* vršiocima prakse, uključujući dobru komunikaciju kao što je, pristup telefonu, faksu, e-mail-u;
- *Obimna biblioteka* i *Web pristup* kao i mogućnost pristupa ekspertizama i dokumentima;
- *Govorna tehnologija* koja olakšava pristup i deljenje znanja kako lokalno tako i globalno;
- *Kolaborativne tehnologije* koje omogućavaju ljudima da rade zajedno. Tu spadaju alati za razvijanje i deljenje znanja; alati za koordinaciju, odnose i građenje poverenja; alati koji olakšavaju funkcionisanje i upravljanje CoPs-om,
- Alati za *konekciju, doprinos i pristup zajednici*- npr. softver koji će smanjiti teškoće i "trenje" u pokušaju da se radi zajedno. Postoje alati koji automatski pronalaze, evidentiraju i kodifikuju znanja za kasniju ponovnu upotrebu [2].

Da bi znanje moglo da bude deljeno, prvo mora biti ”uhvaćeno”, kodifikovano i razvijeno u formatu prihvatljivom za korisnike. Samo stvaranje znanja pristupačnim se ne smatra i transferom znanja. Transfer znanja je proces koji se sastoji od transmisije i apsorbcije znanja i odvija se direktno, radom zajedno, komunikacijom, učenjem iz rada, istraživanjem, konverzacijom kroz lične diskusije, ili kroz procedure, mentorstva i razmenu dokumenata. Argote i Ingram (1999) definišu transfer znanja kao "proces kroz koji je jedna jedinica (grupa, odeljenje, ili divizija) pod uticajem iskustva druge". Znanje može biti preneseno iz skladišta na ljude, od timova na individualce, i između individualaca. Cilj je unaprediti i olakšati deljenje znanja, kolaboraciju i umrežavanje.

4. SISTEMI MENADŽMENTA ZNANJA I MENADŽMENT RIZIKA

Sistemi menadžmenta znanja su nastali u organizacijama kao odraz menadžmentskih napora za sticanjem konkurentskih prednosti, razvijanjem i deljenjem znanja. *KMS (Knowledge Management System)* je distribuirani hipermedijski sistem koji pomaže u upravljanju znanjem u organizacijama, podržavajući kreiranje, skladištenje i širenje ekspertize i znanja. To je softversko- hardverska platforma koje olakšava čuvanje, izvlačenje, pretraživanje, integrisanje, transformaciju, vizuelizaciju, analiziranje, širenje, i korišćenje znanja. [5] Ideja KMS-a je da se službenicima omogući pristup kompanijskim faktima znanja, izvorima informacija, i rešenjima problema. Cilj KMS-a je pružiti prave informacije pravim ljudima u pravo vreme. To povećava efikasnost, vodeći ka povećanju konkurentskih prednosti. Sistemi menadžmenta znanja obično startuju kao kompjuterska baza podataka koja sadrži znanja koja su važna za organizaciju, omogućujući službenicima da dele svoja znanja sa drugima izbegavajući preopterećenje informacijama.

KMS se sastoji od četiri oblasti: Oblast 1: Kreiranje znanja; Oblast 2: Otkrivanje gde su informacije čuvane i gde se mogu dobiti; Oblast 3: Alokacija informacija; Oblast 4: Gde se primenjuju informacije. Neke od prednosti KMS su:

1. Laka upotreba,
2. Informacija je raspoloživa onda kada je potrebna,

3. Povećanje kvaliteta korisničkih odnosa,
4. Smanjena cena,
5. Smanjenje redundantnog rada,
6. Kreiranje organizacije

Najvažnija komponenta KMS su *skladišta znanja*. Organizaciona memorija ili skladište znanja je kompjuterski sistem koji kontinualno snima i analizira znanja jedne organizacije. To je kolaborativni sistem pomoću koga ljudi mogu ispitivati i pretraživati (struktuirane i nestruktuirane) informacije da bi retrivirali i sačuvali organizaciona znanja i olakšali kolaborativni rad. Cilj je vratiti podatke na *kontekstualno senzitivan* način a ne samo kroz upotrebu jednostavnog i na ključnim rečima baziranog retrivinga.

Postoje tri vrste skladišta znanja: *self-memory*- koja uključuju sve fajlove koje čuvaju korisnici kao što su npr. notesi. To omogućuje korisnicima da prilažu svoja znanja drugima u kompaniji. *Papirni dokumenti* su dokumenti koji su vidljivi ili koji se mogu tretirati kao slike. *Kompjuterski bazirani dokumenti*- dokumenti znanja koja se mogu pronaći u u kompjuteru.

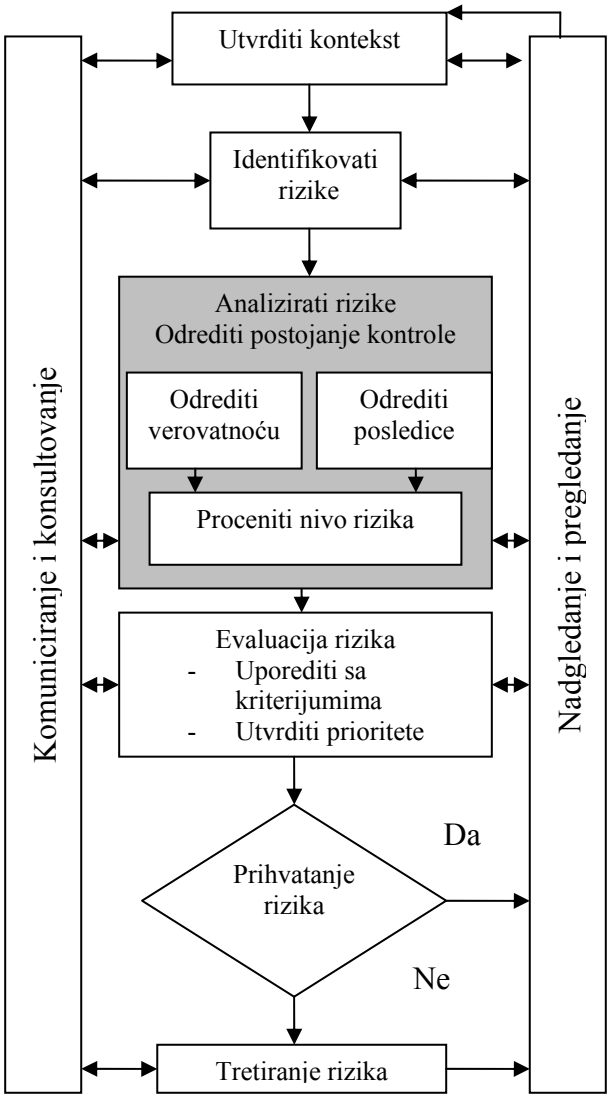
Jedna od osnovnih komponenti skladišta znanja je *dokument*, koji je i osnovni kontejner u koji se skladišti i pomoću kog se deli znanje. Dokument bi se mogao definisati nezavisno od tipa medija na kome se nalazi: "Dokument znači bilo koju belešku informacije, i uključuje:

- Bilo šta na čemu je pisano tj. bilo šta na čemu su oznake, brojke, simboli, koji imaju zanačenje za osobu kvalifikovanu da ih interpretira,
- Bilo šta iz čijih, zvukova, slika ili pisnja se može reprodukavati sa ili bez pomoći nečega drugog,
- Mapa, plan, crtež ili fotografija.

U vezi sa skladištenjem dokumenata unutar skladišta znanja postoje brojni rizici i posledice koje ne mogu biti adekvatno kontrolisane i revidirane i koje mogu prekršiti privatne interese i zakonodavstvo. Jedan od menadžment procesa koji se bavi razmatranjem rizika i podesnih mera zaštite je *manadžment rizika*. Menadžment rizika je širok proces koji identifikuje rizike, bezbednosti i kontrole za KM infrastrukturu i sisteme. Rizik mora uvek da postoji ali adekvatna kontrola i upravljanje rizikom mogu značajno doprineti podizanju kompanijskih performansi.

Prilikom implementacije KMS potrebno je uzeti u razmatranje tehnologije koje će biti upotrebljene. Primeri KM tehnologija uključuju:

- Motore za pretraživanje
- *Content management system*
- *Document i records management*
- Sistemi automatske klasifikacije kakvi su neugonske mreže, lingvistički ili semantički procesni sistemi.
- Inteligentne tehnologije uključujući AI *(Artifical Intelligent),* inteligentne agente, ekspertne sisteme, na slučajevima zasnovano rasuđivanje.
- Komunikacione sisteme uključujući e-mail, diskusione forume, groupware,
- Arhiviranje



Slika 1. Proces menadžmenta rizika

Svaka od ovih tehnologija ima svoje rizike, pomoćno obezbeđenje i mehanizme kontrole.

Iskladištenje znanja zahteva jaku i efektivnu administraciju podataka. Administracija podataka je vitalna u organizaciji i pojavljuje se kao funkcija za menadžment i kontrolu resursa podataka. Ciljevi administracije podataka važe za KMS i prilagođeni su da :

- Podrže poslovne ciljeve organizacije,

- Unaprede upotrebu znanja kao deljivog organizacionog resursa,
- Pomognu efikasnoj upotrebi rasursa znanja,
- Obezbede integritet znanja,
- Obezbede pogodno upravljanje resursom znanja,
- Obezbede koordinaciju i integraciju u organizaciji obezbeđivanjem veće deljivosti znanja;
- Povećaju dostupnost znanja na svim nivoima i
- Kontrolišu umnožavanje i redundantnost informacija

Od rizika koji se sreću u okruženju KM može se izvršiti klasifikacija rizika na:

Strategijske/ planirajuće gde spadaju: loša KM strategija i IT strategije, neidentifikovano ili prekomerno koštanje naročito održavanja i podrške, previđena suštinska KM funkcionalnost.

Slučajne ili namerne: štete, gubici, modifikacije, uništavanje i korišćenje:

- Hardvera koji služi za pokretanje KM sistema,
- KM softvera,
- Skladišta znanja,
- Softvera napajanja,
- Pomoćne baze podataka.

U ovaj tip rizika takođe spadaju gubitak ili onesposobljavanje ključnih KM eksperata, inženjera znanja, programera ili osoblja za održavanje znanja.

Prevara i zloupotreba gde spadaju**:** zamenjivanje ili brisanje skladišta znanja, neovlašćen pristup KM sistemima ili zapisima KM upravljanja ili revidiranja. Takođe tu spadaju još i modifikacija, brisanje ili umetanje KM informacija u mrežu uključujući i druge aplikativne softvere koji su povezani ili integrisani sa KM sistemom.

Druge izloženosti ricima su: nemogućnost ugrađenog KM softvera za ponovo pokretanje/restart, neuspeh KM hardvera ili softvera prilikom *real time* monitoringa. Oskudnost istorije upotrebljenog znanja (*revizionih zapisa*) na štampanim primercima, magnetskoj ili optičkoj formi takođe predstavlja rizik. KMS koji nisu bazirani na najboljem ekspertskom znanju, rezonovanju, i objašnjavanju povećavaju rizik za pogrešno donošenje odluka. Osim nabrojanih rizika još su značajni: neadekvatna kontrola i pristup KM skladištima, oskudan kvantitet ili kvalitet KM personala, oskudan menadžment, nadzor i kontrola KM aplikacija i skladišta koja su smeštena drugde u IT odeljenju, neadekvatno obučavanje i nadzor KM personala. U slučaju oslanjanja na zaključivanje KMS-a kada to mišljenje prouzrokuje gubitak života, štete, ili novčane gubitke može doći do pravne odgovornost.

5. BEZBEDNOST I KONTROLA U KM OKRUŽENJU

Da bi se obezbedio adekvatan odgovor na sve identifikovane rizike neophodno je svaki deo KMS infrastrukture pripremiti s tom pažnjom.

KM Hardver: Senzitivan pristup znanju:

- Oprema za zaključavanje,
- Ograničene/ kontrolisane startujuće procedure,
- Biometrijska kontrola pristupa,
- Mere enkripcije,
- Savremena dokumentacija,
- Regularna revizija KM opreme,
- Pronalaženje i praćenje svih saopštenih grešaka.

U KM okruženju potrebno je obezbediti:

- Neprekidno snabdevanje snagom kao i regulatore napona,
- Klima uređaje
- Fizičke zaštitne prepreke za sprečavanje fizičkih pristupa- bezbednosnu infrastrukturu.

KM softver je jedna od najvažnijih komponenti KMS-a. Stoga, potrebno je implementirati sledeće bezbednosne karakteristike softvera: automatske procedure za KM kontrolu pristupa sa punovažnim ugovorima softverskih licenci, aktuelnu dokumentaciju, proveravati integritet KM softvera i obezbediti podesnu KM strategiju održavanja. Tu još spadaju: poboljšanje KM softverskih kontrola, pronalaženje i praćenje svih saopštenih softverskih grešaka, enkripcija KM skladišta, proveravenje integriteta KM skladišta. Veoma su veliki zahtevi u pogledu grafičkog layout-a KM skladišta, rečnika znanja ili leksikona održavanja kontrole i pristupa, tragajućih objekata upotrebe znanja i pronalaženja revizionih zapisa svih aktivnosti. Takođe, neophodno je da softver bude potvrđen od strane glavnih konsalting/ računovodstvenih firmi.

Kontrole i bezbednosti prilikom *razvoja KM sistema* podrazumevaju prateću metodologiju razvoja KM sistema, podesan dizajn dokumentacije, validaciju i testiranje KMS-a, učešće kontrolora u pregledu razvoja KM sistema.

Kod *KM aplikacija* neophodna je sistemska bezbednost pristupa (šifra kao minimum) i jaka autentikacija. To se postiže sa Smart Card, Secure Clients (IPSec), enkripcijom skladišta znanja. Umerene provere podrazumevaju pregled izlaza od strane kompetentnog personala kao i menadžment/revizione preglede revizionih zapisa i zaštitu neovlašćenog kopiranja.

KM mrežne kontrole uključuju*:* Internet, Extranet, ili Intranet kontrole pristupa, virtuelne privatne mreže (VPN), transmisionu enkripciju znanja u tranzitu, Public Key Infractructure (PKI) i Firewalls

. Za *ljudske resurse* takođe postoje rizici koji se mogu eliminisati ili smanjiti određivanjem odgovornosti za:

- ⇨ KM sistemski razvoj
- ⇨ KM proizvodne operacije
- ⇨ KM planiranje katastrofa

Bezbednosti vezane za ljudske resurse podrazumevaju adekvatan trening KM personala, nadzor i menadžment KM personala, obavezne odmore, provere bezbednosti personala.

Autputi sistema baziranih na znanju, kao što su npr. ekspertni sistemi su obično u formi dokumenta ili izveštaja konsultovanja ili preporučivanja. Neophodno je obezbediti neke forme razumnog proveravanja i dobro obaveštenog korisničkog pregledanja ranijeg donošenja odluka jer postoji potencijalni veliki rizik nepažljivog oslanjanja na KM/KBS *(Knowledge Based System)*. Iz upotrebe KM/KBS može nastati *zakonska odgovornost*. Odluke donesene od strane KM sistema mogu prouzrokovati gubitak preimućstva ili života tako da konačna odgovornost mora pasti na osobu u organizaciji a ne na sistem.

Takođe je od velike važnosti neprekidna validacija i pregled znanja naročito u visoko rizičnim aplikacijama, ako du baze znanja i skladišta znanja od strateške važnosti za organizaciju. U tom slučaju potrebno je razmatrati i enkripciju KM skladišta.

U slučaju da se vrše dopune originalnih programa za neku aplikaciju na neki način je potrebno kontrolisati dopune, ažuriranje znanja, ili promene pravila funkcionisanja KM sistema. To podrazumeva provere da li je softver korektno apdejtovan, primenjen kao i provere da li je KM skladište u formi da neovlašćene dopune budu sprečene.

Radnici znanja ili vodiči za korisnike su korisni kao uvod u KM sistem koji takođe može biti on-line. Kada se operativna verzija KBS-a koristi za konsultovanje, potrebna je adekvatna dokumentacija konsultacija, obično u štampanom formatu kako bi poslužila na primer kao dokaz korisnicima ili se čuvala u svrhe pravne zabeleške kao dokaz poslovnih transakcija ili događaja. Za dokumentovanje istorije slučajeva za kasnije upravljanje ili revizione preglede mogu biti korisni optički ili magnetni snimci. Takođe se zahteva adekvatna dokumentacija operatorske odgovornosti na kraju dana što može obuhvatiti procedure za odgovarajuće čuvanje magnetskih, optičkih ili štampanih fajlova.

Planiranje nepredviđenih situacija za KMS je isto tako važno kao i za tradicionalne IT sisteme. Ako su KM sistemi kritični za organizaciju, moraju se pronaći alternativne lokacije skladišta i opreme naročito za specijalizovan KM/AI (*Artifical Intelligence*) hardver. Važni zahtevi kakav je KM skladište istorije slučajeva konsultacija i dokumentacije treba takođe da budu skladišteni izvan regularne baze. Ovo su tipovi sigurnosti i kontrola koje se razmatraju od strane organizacionog uspostavljanja KM sistema.

6. BEZBEDNOST I KONTROLA U SKLADIŠTIMA ZNANJA

Skladišta znanja sadrže baze podataka velike vrednosti koje sadrže najbolje prakse, naučene lekcije, odgovore na najčešće postavljena pitanja, linkove ka istraživanju, inženjerske materijale, i *help desk*-ove ekspertnih sadržaja. Postoje brojni problemi povezani sa skladištima znanja kao npr. gde su locirana i ko je odgovoran za njih i njihovu kontrolu. Ako se skladišta znanja kontrolišu na neki način kao korporativna baza podataka, onda ona mogu dobiti bezbednost koja je data za sve druge IT sisteme. Međutim, ako su skladišta znanja locirana unutar *end user* okruženja na serveru znanja onda ovi sistemi vrlo lako mogu biti neadekvatno kontrolisani. Posledica toga mogu biti:

- ❖ Nesistemska bezbednost pristupa,
- ❖ Neadekvatan monitoring,
- ❖ Nedostatak adekvatne podrške i procedura za povratak i olakšica.

Ako je ovo slučaj tada menadžment može zahtevati razmatranje bezbednosti ovih sistema menadžmenta znanja i primeniti iste procedure kao one kod IT sistema. Kada se razmatra bezbednost skladišta znanja potrebno je odgovoriti na pitanja: ko je odgovoran za smeštanje dokumenata unutar skladišta, kako je kontrolisan pristup do ovih dokumenata, i ko je odgovoran za raspolaganje dokumentima? Upravo kao odgovor na ova pitanja neke organizacije su kreirale otvorene *centre znanja* unutar različitih odeljenja njihove organizacije. Centri znanja su odgovorni za dodavanje, održavanje i razmatranje dokumenata smeštenih unutar skladišta znanja. Osoblje u centrima znanja je odgovorno za postavljanje i održavanje rečnika znanja ili leksikona. *Rečnik znanja* je veoma važan zato što sadrži ključ za pristupanje mnogim dokumentima sadržanim unutar skladišta znanja. Znanje sadržano u dokumentima unutar skladišta znanja je indeksovano i može mu se pristupiti preko reči postavljenih u skladištu znanja. Stoga, protekcija preko rečnika znanja je vitalna kao i bezbednost skladišta znanja. Osoba imajući pristup rečniku

znanja na prikriven ili nekompetentan način može namerno ili slučajno uništiti ili modifikovati ključne termine unutar rečnika znanja ili može u čak uništiti ceo rečnik znanja ili zameniti drugi na njegovo mesto. Ponovno građenje rečnika znanja zahteva mnogo napora osoblja ili može biti čak nemoguće za rekonstrukciju, time uzrokujući značajne organizacijske gubitke usled nesposobnosti za pristup dokumentima unutar skladišta znanja.

Još jedna zabrinutost je sa znanjem sadržanim unutar skladišta znanja. Vrlo je bitno kako su dokumenti čuvani unutar skladišta znanja, da li su oni enkriptovani ili držani u čistoj tekstualnoj formi, da li su u formi da ne mogu biti izmenjeni, ili su u otvorenoj formi tako da mnogi unutar organizacije mogu imati pristup i sposobnost da ih zamenjuju, modifikuju ili brišu? Ako su dokumenti čuvani u formi Acrobat PDF tada odlike bezbednosti dokumentacije moraju biti takve da obezbede zadovoljavajuću pristupačnost, štampanje, promene, izvod ili kopije, komentare autora.

Tri važna interesa povezana sa sigurnošću skladišta znanja obuhvataju: *poverljivost, integritet, i raspoloživost* [2].

Poverljivost podrazumeva osiguranje da skladišteno znanje ostane poverljivo i da se koristi samo u svrhe zbog kojih je to znanje sakupljeno. Poverljivost takođe implicira da mogu postojati različiti stepeni poverljivosti vezani za dokumente. Na primer, mogu postojati tri nivoa poverljivosti: otvoren pristup, komercijalno u poverenju, ili samo za viši menadžment. Razmatranjem nivoa poverljivost u organizaciji formuliše se sopstveni metod razvrstavanja informacija, i kontrole pristupa korišćenju informacija, tako da će na primer samo ovlašćeno osoblje unutar organizacije sa odgovarajućim sigurnosnim odobrenjem imati pristup znanju sadržanom na odgovarajućem bezbednosnom nivou.

Integritet je pitanje koje može biti previđeno od strane odgovornih za KM sisteme. Integritet implicira da znanje u skladištima znanja bude *aktuelno i tačno* tokom vremenskog perioda. U sistemu menadžmenta znanja nedostatak tačnosti ili aktuelnosti znanja može upetljati organizaciju u ozbiljne gubitke, narušavanje reputacije, ili jakom finansijskom izlaganju kao rezultat odluka načinjenih na osnovu znanja koje nije tačno ili aktuelno. Stoga, važno je da se proverava (revidira) znanje sadržano unutar skladišta znanja da bi se obezbedilo da je znanje aktuelno i ispravno sve vreme. Integritet se takođe dovodi u vezu sa bezbednošću držanog znanja jer ako neka neovlašćena osoba ima pristup znanju sadržanom unutar dokumenta tada ona može zameniti, modifikovati ili izbrisati znanje i stoga ugroziti tačnost tj. integritet znanja inkorporisanog unutar dokumenta.

Monitoring korišćenja znanja je takođe važan i organizacija bi trebalo da bude sposobna da prati ko je pristupio znanju iz dokumenata u skladištu, da identifikuje kada je dokumentu bilo pristupljeno, kao i šta je rađeno na dokumentu za vreme pristupa i ako je evidentirano, koja je korist bila od tog znanja.

Raspoloživost skladišta znanja je vezana za mogućnost korišćenja skladišta znanja od strane radnika znanja širom sveta. Do nemogućnosti korišćenja skladišta znanja može doći prilikom nekih nesrećnih slučajeva koji mogu uništiti skladište znanja ili sprečiti pristup do njih. Primeri uključuju aktove syber-terorizma ili aktuelnog terorizma, nesrećne slučajeve koji vode do brisanja ključnih skladišta znanja ili onesposobljavanja kominikacije. Raspoloživost zahteva da organizacijska infrastruktura znanja uključujući komunikacione linije, servere znanja i sisteme znanja, budu operativni i obezbeđeni od proboja. Neophodnost je da se sistemi ključnog znanja i njima udružena skladišta znanja podrže i potpomognu bezbednošću sa strane.

KM *revizioni* podsistem ima zadatak da obezbedi sredstva za neprekidan monitoring i reviziju osoblju u centrima znanja koji su odgovorni za pregledanje izveštaja ravidiranja znanja. Kada radnik znanja pristupi dokumentu u skladištu znanja, sistem revizije znanja snima datum i vreme pristupa, kao i to koji radnik znanja je pristupio dokumentu, koji dokument je bio posećen, i za šta je upotrebljeno to znanje (ako je ova karakteristika inkorporisana u sistem revizije znanja). Zapisi o pristupu dokumentima znanja tada postaju deo revizionog zapisa (*audit trail*) koji menadžment centra znanja može pregledati i pratiti.

Deo monitoring KM revizionih sistema može obuhvatati unpozoravajuću komponentu koja može biti neka vrsta kontrole pristupa specifikovana na izvesnim dokumentima. Na primer, svaki pristup pojedinačnom dokumentu ili neka promena pojedinačnog dokumenta. Ako se takav jedan pristup ili promena desi na dokumentu , tako primetno, tada ne samo da će snimak upozorenja biti upisan u bazu podataka revizije znanja, nego će i jedan trenutačan znak upozorenja biti poslat u konzolu upozorenja u centru znanja za neposredno praćenje od strane osoblja centra znanja. Izveštaji revizije znanja mogu biti zahtevani od strane menadžmenta, policije i drugih vladinih agencija, u slučaju ozbiljnog kriminala, zloupotrebe ili drugih kriminalnih akata. Ovi izveštaji znanja treba da budu osigurani i čuvani u sigurnosnom delu tako da se mogu retrivirati radi evidencije.

Preporuka je da izveštaji revizije znanja treba da budu čuvani minimum sedam godina.

7. KVALITET PRIVATNOSTI U KMS-U

Privatnost je važno pitanje i koje je potrebno razmotriti kada se diskutuje o skladištima znanja. U mnogim zamljama postoji zakonodavstvo tajnosti za javne i privatne sektore. Zakonodavstvo tajnosti nalaže da organizacija prijavi sve osobe od kojih koristi znanje ili informacije koja se smeštaju u skladište znanja. Sakupljajući znanja preko Interneta, organizacija bi trebalo da osigura privatnost za osobe koje daju svoju ekspertizu. Organizacijska odgovornost je da nadgleda ko ima pristup tom znanju, ko održava znanje, i kako se to znanje koristi unutar organizacije. Narušavanje privatnosti u KM sistemu može prouzrokovati nedostatak *poverenja* od strane korisnika/saradnika koji mogu čak napustiti organizaciju otvorenu za legalnu odgovornost. Održanje nivoa poverenja je jako važno za saradnju i saradničko učenje jer su ljudi emotivno vezani za ono što znaju i deljenjem znanja sa drugima oni daju deo sebe. Takođe, potrebno je ljudima koji dele svoja znanja obezbediti na neki način garancije da će znanje biti korišćeno u određene svrhe.

Jedan slučaj implementacije bezbednosnih i kontrolnih mehanizama predstavljenih gore, je KM bezbednosna infrastruktura Schlumberger, kompanije za informacione tehnologije. Schlumberger upotrebljava niz bezbednosnih tehnologija uključujući VPN (*Virtual Private Network*) i PKI (*Public Key Infractructure*) i *smart-card* bazirane enkripcione servise koji garantuju pristup informacijama od strane samo relevantnih osoba, nakon odgovarajućih dozvola i autentikacije i obezbeđivanja poverljivosti, integriteta, raspoloživosti resursa. Rešenje koje je Schlumberger obezbedio je *DeXa.Net Secure Connectivity Centers (SCCs)* koji olakšava višestranačko, višeoganizacijsko deljenje znanja u skladištu. Predefinasani nivoi pristupa i sofisticirano IP rutiranje omogućava strankama da pristupaju skladištima bez narušavanja poverljivosti znanja. SCC je osnovni menadžment sistem za sigurnosnost saobraćaja koji ostavlja revizioni zapis.

LITERATURA

[1] Banjanin M, ***"Komunikacioni inženjering"***, Saobraćajno-tehnićki fakultet Doboj, 2007

[2] Elias M. Awad & Hassan M. Ghaziri, ***"Knowledge Management",*** Chapter 9, 2003.

[3] Clyde W. Holsapple, ***"Handbook on Knowledge Management",*** Chapter 20, 25 2005.

[4] Sredojević, A. **Informaciono-komunikaciona infrastruktura u zajednicama prakse (CoPs),** diplomski rad, Fakultet tehničkih nauka Novi Sad, 2007.

[5] www.community-intelligence.com, 10.09.2006.

[6] www.wikipedia.org 25.11.2006.