

Факултет инжењерских наука Универзитета у Крагујевцу



Назив студијског програма: Инжењерски менаџмент

Ниво студија: Мастер академске студије

Предмет: Интегрисани системи менаџмента

Број индекса: 601/2015

Оливера Р. Гавриловић

**Интегрисани систем менаџмента (ISO 9001:2015,
ISO/IEC 27001:2013 и ISO 26000:2010) у предузећу
„Интранеа решења“**

мастер рад

Комисија за преглед и одбрану:

1. Проф. др Славко Арсовски - ментор

2. _____

3. _____

Датум одбране: _____

Оцена: _____

У оквиру овог мастер рада кандидат треба да уопштено анализира питање интеграције система менаџмента на основу прегледа литературе, објасни значај интеграције и могућност примене. Након прегледа општих тачака стандарда ISO 9001:2015, ISO/IEC 27001:2013 и ISO 26000:2010 и анализе њиховог значаја, кандидат ове стандарде треба да интегрише у оквиру одабраног предузећа. Кандидат треба да анализира процесе *Маркетинг и продаја* и *Пројектовање и развој* у датом предузећу. На крају, кандидат треба да изнесе своје закључке и препоруке за будуће побољшање по овом питању.

Препоручена литература:

1. Arsovski S., i drugi (2013), *Integrisani sistemi menadžmenta*, Univerzitet u Kragujevcu, Fakultet inženjerskih nauka, Centar za kvalitet
2. ISO 9001:2015 Quality management systems – Requirements
3. ISO 26000:2010 Guidance on social responsibility
4. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
5. Karapetrovic, S. (2003). "Musings on integrated management systems." *Measuring Business Excellence* 7(1): 4-13.

Крагујевац, 2016.

ментор:

Проф. др Славко Арсовски

Резиме:

Интеграција система менаџмента данас постаје један од предуслова за успешно пословање једне организације. Како би се повећала ефикасност али и признање на међународном нивоу, све више организација одлучује да се сертифициује према стандардима Међународне организације за стандардизацију. У основи успешног пословања се свакако налази систем менаџмента квалитетом. Међутим, у време све већег развоја информационих технологија, један од битних захтева постаје и заштита података, чиме се намеће потреба за системом менаџмента сигурношћу информација. Такође, као последица глобализације и шире доступности података услед интернета, организације су под лупом различитих заинтересованих страна, па се све чешће говори о проблему друштвене одговорности. Овај рад се бави овим питањима на конкретном примеру предузећа из области компјутерских делатности, при чему је дат приказ интеграције стандарда ISO 9001:2015, ISO/IEC 27001:2013 и ISO 26000:2010.

Кључне речи: интегрисани системи менаџмента, систем менаџмента квалитетом, систем менаџмента сигурношћу информација, друштвена одговорност ISO 9001:2015, ISO/IEC 27001:2013, ISO 26000:2010

Abstract:

Integrated management systems have become a prerequisite if an organization wants to do business effectively. In order to increase their efficiency as well as international recognition, an increasing number of organizations decide to become ISO-certified. Quality management system is found at the base of successful business. However, considering the growing development of information technologies, information security management has become an important requirement in terms of data protection. Additionally, because of globalization and easier availability of information via the Internet, organizations have found themselves under close scrutiny of various stakeholders, which is why the issue of social responsibility has become discussed so often. This paper deals with these issues and the issue of integrating ISO 9001:2015, ISO/IEC 27001:2013 and ISO 26000:2010 in a computer-related company.

Key words: integrated management systes, quality management system, information security management system, social responsibility, ISO 9001:2015, ISO/IEC 27001:2013, ISO 26000:2010

Садржај

1. Увод	4
2. Преглед литературе	8
3. Преглед стандарда ISO 9001:2015	13
4. Преглед стандарда ISO/IEC 27001:2013	18
5. Преглед стандарда ISO 26000:2010	26
6. Интеграција захтева стејхолдера у предузећу „Интрanea решења“	35
6.1 Основни подаци о предузећу „Интрanea решења“	35
6.2 Преглед стандарда	40
6.3 Приказ мапе и метрике свих процеса и приказ интеракција између процеса	43
6.4 Преглед одабраних процеса и захтева стандарда који се на њих односе	47
6.5 Маркетинг и продаја	49
6.5.1 Мерење и праћење процеса	52
6.6 Пројектовање и развој	53
6.6.1 Мерење и праћење процеса	56
6.7 Процедура за процес Маркетинг и продаја	57
6.8 Процедура за процес Пројектовање и развој	65
7. Закључци	72
Литература	73

1. Увод

Конкурентност организација приморала је компаније да све више улажу у ресурсе за побољшавање својих пракси менаџмента. Економска и тржишна глобализација, која је довела до нових интеракција на тржишту, дала је доста значаја улози стандарда у пословању. Такође, настојећи да се створе квалитетнији производи и услуге, јавила се потреба за универзалним међународним стандардима. Стандарди нуде могућност организацијама да искористе екстерне мреже контаката, повећају производну и иновативну ефикасност, умање количину нетачних и редундантних информација, шире иновације, смањују трошкове, промовишу конкуренцију, увећају компатибилност, побољшају менаџмент процесима и промовишу и помажу добробит друштва.

Крајем двадесетог века, примећено је да организације са успостављеним TQM системом (*engl. Total Quality Management*) нису толико успешне у поређењу са компанијама које су тражиле тотални квалитет а да се притом нису ограничавале на технике које су повезане само са TQM-ом, већ су настојале да интегришу и друге технике. Примена само TQM стратегије неће довести до одрживих промена. Најуспешнији менаџери били су они који су системе менаџмента засновали на TQM техникама интегрисаним са другим техникама. Ово је тако управо због тога што квалитет не може да се достигне ако се занемаре други аспекти као што су интерно и екстерно окружење, управљање ресурсима, друштвена одговорност, и други. Такође, стејкхолдери померају своју идеју о квалитету производа или услуге ка једној свеобухватнијој квалитативној процени при којој обраћају пажњу на то како организације поступају према свом окружењу или запосленима (Salomone 2007), а не само према стандарду квалитета. Све ово повећава конкурентност компанија, због чега компаније успостављају неколико система менаџмента, при чему најчешће почињу од система менаџмента квалитетом. Све то се ради са циљем да се побољша профит и да пословање компаније буде одрживо.

Најпростије речено, интеграција представља комбинацију, односно, склапање свих интерних система менаџмента у један систем на такав начин да компоненте тог система не буду одвојене већ повезане и да чине један интегрални део система менаџмента једне компаније. Другим речима, интегрисани систем менаџмента (IMS) јесте систем менаџмента који комбинује све компоненте пословања у један кохерентан систем како би се омогућило постизање циљева и мисије предузећа. Главни циљ интеграције јесте да

се упросте процеси и да се избегне дуплирање посла, као и да се смање трошкови пројектовања и успостављања појединих система менаџмента. Поврх тога, ефективан интегрисан систем менаџмента омогућава компанијама да се лакше прилагођавају различитим условима и да лакше доносе одлуке у условима несигурности.

Интегрисани систем менаџмента генерално има следеће карактеристике (Dalling 2007):

1. IMS ће обухватити целокупне процесе и системе организације и размотриће квалитет, безбедност информација, средину, људске ресурсе, финансије, маркетинг, односе са јавношћу, друштвену одговорност и остале аспекте као битне факторе који утичу на вредности, циљеве и пословање организације.
2. Формално се дефинише у униформном стилу који варира у зависности од циља тог одељка – на пример, опис општих принципа ће се разликовати од дефинисаних корака које треба пратити у неком процесу.
3. Ако се IMS успостави на ефективан начин, умањује се дуплирање документације.
4. Структура IMS-а не прати структуру одређеног стандарда већ је осмишљена тако да контролише и води процесе једне организације на најефективнији и најефикаснији начин.
5. Свака компонента система менаџмента посвећује пажњу на одговарајући начин осталим компонентама система.
6. Омогућава транспарентност у смислу испуњавања свих кључних захтева стејкхолдера преко релевантних стандарда.

Постоје разлози за и против интеграције система менаџмента.

Главни разлози за интеграцију система менаџмента јесу следећи:

- *Растући захтеви система менаџмента* – све је већи притисак на компанијама да се квалификују за добијање једног или више међународних стандарда. Поред тога, неке смернице или стандарди постоје за различите системе менаџмента који се примењују у одређеним делатностима. Такође, компаније морају да испуне захтеве својих стејкхолдера и очекивања корисника. Компанија онда може наићи на изазов да остане конкурентна на тржишту а да истовремено испуни све захтеве система. Једини начин да се то постигне јесте да компанија има јединствени

интегрисани систем менаџмента. Самим тим, лакше је интегрисати нове захтеве у већ постојећи систем. IMS поједностављује систем, пружа му више функционалности и свеобухватности, и лакше се може проширити додавањем још једног стандарда.

- *Побољшана ефективност* – IMS се фокусира на потребе предузећа и тиме пружа додатне вредности предузећу зато што компанија поново процењује захтеве и предузима оне активности које поспешује пословање. Другим речима, стандарди се интерпретирају на такав начин да компанија испуњава и захтеве система и потребе компаније. Општи циљеви и мисија се остварују кроз јединствени систем менаџмента. С обзиром да IMS мора због тога добро да се осмисли и детаљно имплементира, то повећава ефективност предузећа. Поред тога, интегрисани систем менаџмента је економичнији и функционалнији, што побољшава безбедност организације, а такође и промовише имиџ и кредибилитет компаније.
- *Смањени трошкови* – Повећана ефективност доводи до смањења трошкова. Јефтиније је имплементирати један IMS него више одвојених система менаџмента. Мање времена се одваја за одржавање система, а штеде се и време и новац након успостављања интегрисаног система менаџмента.
- *Мање редундантности и мање супротних елемената* – Интеграција система менаџмента смањује редундантности и супротне елементе који се јављају када се користе два или више одвојених система. Квалитетно одрађене процедуре садрже и кључне захтеве различитих процеса, што омогућава запосленима да боље разумеју захтеве у оквиру једног сета процедура.

Као што је већ речено, користи имплементирања IMS-а могу се извести из мотива који су довели до интеграције. На основу истраживања (Funck et al 2001), закључено је да су користи интеграције, на основу интегрисане документације и јасније представљених одговорности, следеће: смањење трошкова, уштеда времена, више транспарентности при пословању, боља структура процеса, смањење проблема везаних за координацију. Такође, у другој студији (Brobek & Sokovic 2006), наведене користи IMS-а јесу: побољшани учинак пословања, побољшани тимски рад и интерне методе менаџера, већа мотивисаност особља, мањи број различитих ревизија различитих система, повећано поверење од стране клијената, и смањени трошкови.

Имајући у виду наведене предности интеграције система менаџмента, јасно је зашто све више организација жели да се сертифиције према одређеним међународним

стандардима. Такође, због све веће глобализације, све више организација уводи међународне стандарде који ће им пружити сигурност и предност на тржишту. Наравно да све организације треба да воде рачуна о квалитету пословања, због чега је управо ISO 9001:2015 један од основних стандарда који се уводе. Са друге стране, модерне организације морају да обрате пажњу и на сигурност информација у данашње време када количине и вредности података константно расту и када постоје више претњи по те информације помоћу информационих технологија. Због тога организације одлучују да уведу ISO/IEC 27001:2013 помоћу којег ће клијенти видети да се довољно пажње посвећује питању сигурности информација. На крају, у време када се доста пажње посвећује одрживом развоју, треба размотрити и препоруке и упутства из стандарда ISO 26000:2010. Тема овог рада ће управо бити интеграција ова три стандарда у компанији која која се бави компјутерским делатностима.

2. Преглед литературе

Ефективно управљање у глобализованом свету захтева ефективни, ефикасни и флексибилни систем менаџмента. Како би систем био ефективан, треба да се позабави свим релевантним захтевима стејкхолдера у контексту друштвене одговорности (*engl. Social Responsibility*). Како би систем био ефикасан, треба да обавља одређени посао или задатак са малом потрошњом ресурса. Како би систем био флексибилан, систем треба да буде такав да се измењени услови и нови захтеви могу лако укључити. Многе организације већ послују са интегрисаним системима менаџмента. Треба размотрити до ког нивоа та интеграција покрива горепоменуте захтеве и да ли треба увести неке измене ако је потребно. Могућности развоја потпуно интегрисаних система менаџмента треба размотрити из перспективе управљања потребама стејкхолдера, при чему се може користити ISO 26000:2010 као смерница.

Глобализација и повећани фокус на одрживи развој доводе нове стејкхолдере и потребе стејкхолдера које компаније треба да узму у обзир. У данашње време добрих комуникација и повећане транспарентности, погрешно управљање наизглед неважног стејкхолдера може довести до озбиљне штете по имиџ компаније. Корпоративни учинак са тачке гледишта корпоративне друштвене одговорности огледа се на пољима економије, околине и друштвене одговорности. Што се тиче учинка организације са тачке гледишта одрживости, захтеве треба описати преко система менаџмента који је оријентисан према стејкхолдерима. Повећавање вредности стејкхолдера дугорочно гледано уз истовремено одржавање равнотеже међу интересима свих стејкхолдера од кључне је важности за остваривање најбољих резултата свих процеса (Garvare & Isaksson 2001). Тако би, између осталог, интеграција подразумевала да општи пословни систем менаџмента представља део интегрисаног система и она би представљала одрживи начин балансирања између интереса стејкхолдера. Питање на који начин треба извршити интеграцију и до ког нивоа анализирано је у претходним истраживањима (Bernardo et al. 2009, Karapetrovic & Casadesús 2009, Karapetrovic 2002 и Wilkinson & Dale 1999). Међутим, већина ових студија има ограничен распон када је реч о потребама свих релевантних стејкхолдера. С обзиром да данас многе организације имају неколико различитих стандарда и одговарајућих система менаџмента, интеграција тих система постаје све уобичајенија. Као што је наведено у студији Zutshi & Sohal (2005), неопходно

је интегрисати појединачне системе менаџмента у један систем како би се у потпуности реализовале потенцијалне користи сваког појединачног система.

Што се саме интеграције тиче, проблеми који су анализирани у литератури су питања да ли је потребна интеграција или не, питање нивоа интеграције, питање предмета и подручја примене интеграције (типови система менаџмента које треба укључити), контекст, питање имплементације, и остала. Ова питања су анализирана у радовима Hansson et al. (2006), Karapetrovic & Casadesús (2009) и Asif et al. (2008), између осталих.

Када је реч о *предмету и подручју примене интеграције*, већина радова се бави интеграцијом система менаџмента квалитетом, система управљања заштитом животне средине и система менаџмента заштитом здравља и безбедношћу на раду. Неки од радова укључују и усвајање стандарда који се односи на друштвену одговорност (Asif et al. 2008). Стандард ISO 26000:2010 наводи да је друштвена одговорност блиско повезана са одрживим развојем и да су идентификација и укључивање стејкхолдера од кључне важности за друштвену одговорност једне компаније. Интерпретација појма стејкхолдера према овом стандарду прилично је широка и обухвата све оне стране на које пословање организације може утицати, без обзира да ли су они тога свесни или не. Ово би могло сугерисати на то да све организације у будућности треба да управљају свим потребама стејкхолдера, истовремено имајући у виду све потенцијалне ризике и прилике. Самим тим, ако све потребе стејкхолдера треба узети у обзир, онда предмет и подручје примене IMS-а треба да укључи све системе менаџмента, како је наведено у студији Jörgensen et al. (2006). Ако би се IMS осмислио тако да укључи све потребе стејкхолдера у мрежи снабдевања (од првог добављача до последњег корисника), онда би било могуће предложити концептуални оквир који представља могућност за потпуну интеграцију система менаџмента. Овај оквир се онда може користити за поређење са стварним распоном интеграције како би се уочили евентуални пропусти. Идеални распон подручја примене био би диктиран преко анализе стејкхолдера (анализе ризика и прилика).

Ниво интеграције описује до ког нивоа су различити системи постали један и он варира од ниског нивоа интеграције са неком врстом координације до потпуног спајања. На основу студија одређених аутора (Karapetrovic, 2002), могу се разликовати три различита нивоа интеграције. Први ниво се тиче интеграције документације. Другим речима, то је заједничко упутство са одређеним процедурама које различите области у

IMS-у захтевају. Други ниво се тиче усаглашавања централних процеса, циљева и ресурса. Трећи ниво се тиче стварања универзалног система који контролише све претходне системе у организацији. Hansson & Eriksson (2005) говоре о неким факторима који утичу на избор нивоа интеграције, а то су: карактеристике организације (величина, хијерархијска структура, култура запослених у смислу жеље за сталним напредовањем, укљученост менаџера), контекст организације (број стејкхолдера, њихови захтеви по питању усклађености са стандардима неких система) и пословне норме које се тичу различитих аспеката (квалитет и животна средина, број и развијеност постојећих система менаџмента).

Обим интеграције се односи на делове организације на које се IMS односи. IMS може да се односи на део организације, на целу организацију или на цели ланац снабдевања. Обим интеграције се може дефинисати преко различитих потреба стејкхолдера које треба задовољити. На пример, мултинационална компанија са глобално распоређеним добављачима и корисницима мора да рачуна на то да ће њен рад пратити друге организације. Постоје неколико примера компанија које су критиковане јер су користиле добављаче који су друштвено неприхватљиви. Један од примера је Икеа која је купила тепихе који су израдила деца. Компаније и њихов имиџ могу бити оштећени због неког даљег добављача. Због тога су такве компаније под притиском да прате процесе у ланцу снабдевања. Због оваквог широког начина посматрања проблема, прате се производи у смислу места на коме ће завршити, у каквом стању и са којом ценом. У контексту одрживог развоја и пословне етике да се разумно управља ресурсима, од компанија се може очекивати да управљају ресурсима тако да не онемогуће будућим генерацијама да их и оне користе. Самим тим, може се рећи да су и будуће генерације у виду корисника, друштва и запослених, такође стејкхолдери. У контексту IMS-а, ово значи да стратегијско планирање треба да има дугорочнију перспективу него што је до сада био случај у пракси. На крају, ово сугерише да ће компаније, и то нарочито компаније које послују на глобалном нивоу, имати повећан обим интегрисаних система менаџмента.

Као што је већ речено, неколико студија сугеришу да интеграција постаје све чешћа у поређењу са појединачним системима – на пример, Bernado et al. (2009) и Karapetrovic & Casadesús (2009). На основу оваквих студија, многе организације које су усвојиле одређене стандарде накнадно су увеле и интегрисане системе менаџмента. Многа истраживања у овом пољу указују на потенцијалне користи коришћења интегрисаног приступа - Wilkinson & Dale (1999), Karapetrovic (2003), Zutshi & Sohal (2005). Повећана

ефикасност, могућност да се повежу аспекти који се односе на квалитет и животну средину са пословном етиком и профитабилношћу организације, могућност да се развију системи менаџмента који боље одговарају интересима стејкхолдера само су неки од разлога у корист интеграције. Општи утисак на основу објављених студија јесте да има више предности него мана када је реч о интеграцији система менаџмента (Karapetrović 2002). На основу прегледане литературе, може се приметити да су неке важне предности IMS-а коришћење процесног приступа, коришћење PDCA циклуса (*engl. Plan – Do – Check – Act*, што значи: *Планирај – Уради – Провери – Делуј*), интегрисане ревизије и заједнички систем документације са заједничком структуром процедура и рутина.

Када је реч о интеграцији, дефинисању политике и циљева фирме, доста аутора препоручује да треба узети у обзир захтеве и очекивања стејкхолдера приликом тих процеса. Ко су стејкхолдери које треба узети у обзир? Стејкхолдери су овде дефинисани као сви они који утичу или на које утиче организација укључујући и будуће генерације и природу. Примери стејкхолдера су власници, запослени, добављачи, клијенти, корисници, банке, општине, представници владе, представници власти, и други. Неким захтевима стејкхолдера је дата пажња преко стандардизованих система менаџмента. Осталим захтевима се даје пажња преко генералних пракси пословања. Неки од примера су:

- Клијенти – ISO 9001
- Клијенти / власници / јавност – управљање безбедношћу хране – ISO 22000
- Природа, ресурси и околина – ISO 14000
- Глобална одговорност према људима и природи – OECD правила (*engl. The Organisation for Economic Co-operation and Development*)
- Заједнице уопштено гледано и заједнице у области пословања организације – ISO 26000 и SA 8000 (*engl. Social Accountability*)
- Клијенти / власници – економска сигурност / транспарентност – AA 1000 (*engl. Account Ability*)
- Интелектуална својина / подаци о запосленима / интегритет клијената – ISO 27001

У процесном приступу, коначан излаз, односно, исход, био би задовољство стејкхолдера. Самим тим битно је идентификовати различите стејкхолдере и њихове потребе и начин на који њима треба управљати, што се може урадити помоћу ISO

26000:2010 стандарда. Након што се идентификују жељени исходи, они се могу превести у одређене индикаторе које треба пратити у одређеним стадијумима процеса.

О стандарду ISO 26000:2010 ће бити речи даље у раду али треба напоменути следеће. Стандард садржи сугестије које се односе на извештавање о учинку на пољу друштвене одговорности, побољшавање кредибилитета фирми помоћу друштвено одговорних иницијатива, праћење, ревидирање и побољшавање пракси и активности које се односе на друштвену одговорност. С обзиром да је при сачињавању овог стандарда размотрена перспектива више група стејкхолдера, може се рећи да стандард представља мулти-стејкхолдерску иницијативу процеса стандардизације, што у неком погледу представља нову генерацију колаборативног управљања (Rasche 2010). Међутим, упркос инклузивној природи развојног процеса овог стандарда и амбиција и циљева стандарда, ISO 26000:2010 добио је и одређене критике (Moratis 2016). Критичари су се фокусирали на следеће проблеме и недостатке: ограничен материјални садржај стандарда који се односи на мала и средња предузећа (Perera 2008); релативно одсуство малих и средњих предузећа у развојном стадијуму стандарда (Egyedi & Toffaletti 2008); ризик од непоклапања друштвених очекивања и стварног утицаја на одрживи развој (Johnston 2011); стандард је превише општег карактера да би био од користи у контексту специфичних индустрија и сектора пословања (Hemphill 2013). Такође, ISO 26000:2010 не дефинише захтеве који се односе на пословне процесе или нивое учинка фирме уз помоћ PDCA оквира који би организације могле да прате.

3. Преглед стандарда ISO 9001:2015

ISO 9001 је стандард који дефинише захтеве за систем менаџмента квалитетом (*engl. Quality Management System – QMS*). Он помаже предузећима и организацијама да буду ефикасније и да побољшају задовољство корисника. Недавно је објављена нова верзија стандарда – ISO 9001:2015, која је заменила претходну верзију ISO 9001:2008. ISO стандарди се ревидирају сваких пет година што им омогућава да и даље буду од користи организацијама на тржишту с обзиром да се тржиште и услови пословања константо мењају. На пример, све већа глобализација је променила начин на који организације обављају своје послове јер су сада ланци снабдевања сложенији него у прошлости. Поред тога, повећана су очекивања корисника и других заинтересованих страна, а та очекивања се лакше преносе сада због већег и лакшег приступа информацијама. Самим тим, ISO 9001 треба да осликава ове промене како би остао релевантан на тржишту. Организације које су сертифицизоване према стандарду ISO 9001:2008, имају рок од три године од датума издавања нове верзије (до септембра 2018. године) да се сертифицикују према новој верзији.

Најбитнија промена у оквиру стандарда је његова структура. ISO 9001:2015 сада прати исту општу структуру као и други стандарди, што је олакшица свима који користе више система менаџмента и желе да их интегришу (то је такозвана *структура високог нивоа*). Још једна битна разлика је стављање фокуса на размишљање засновано на ризику. Оно је одувек било део стандарда, али је овом питању дато на значају у новој верзији. Додатне измене подразумевају повећану ангажованост највишег руководства у систему менаџмента, повећан фокус на контекст организације, више флексибилности по питању документације, и друго.

Нова верзија стандарда доноси корисницима неколико користи:

- Већа пажња је посвећена укључивању лидера.
- Организациони ризици и прилике се разматрају преко структурног приступа.
- Језик и термини који се користе у стандарду су упрошћени, што је од помоћи организацијама које користе више система менаџмента.
- Питање управљања ланцем снабдевања се разматра на ефективнији начин.
- Боље је прилагођен организацијама које се баве услугама и знањем.

Увођење система менаџмента квалитетом ће помоћи организацијама да:

- процене општи контекст своје организације да би дефинисали на кога утиче њихово пословање и шта они очекују од организације, што ће омогућити организацији да јасно наведе своје циљеве и идентификује нове пословне прилике;
- ставе своје потрошаче на прво место и да константно испуњавају њихове потребе и превазилазе њихова очекивања, што може довести до нових и лојалних потрошача, што ће за узврат повећати пословање организације;
- делују на ефикаснији начин јер ће сви процеси бити усклађени и разумеће их сви у организацији, што ће повећати продуктивност и ефикасност а смањити интерне трошкове;
- испуне неопходне статутарне и регулаторне захтеве;
- се прошире на нова тржишта јер неки сектори и клијенти захтевају ISO 9001 пре почетка сарадње;
- идентификују и размотре ризике који се односе на организацију.

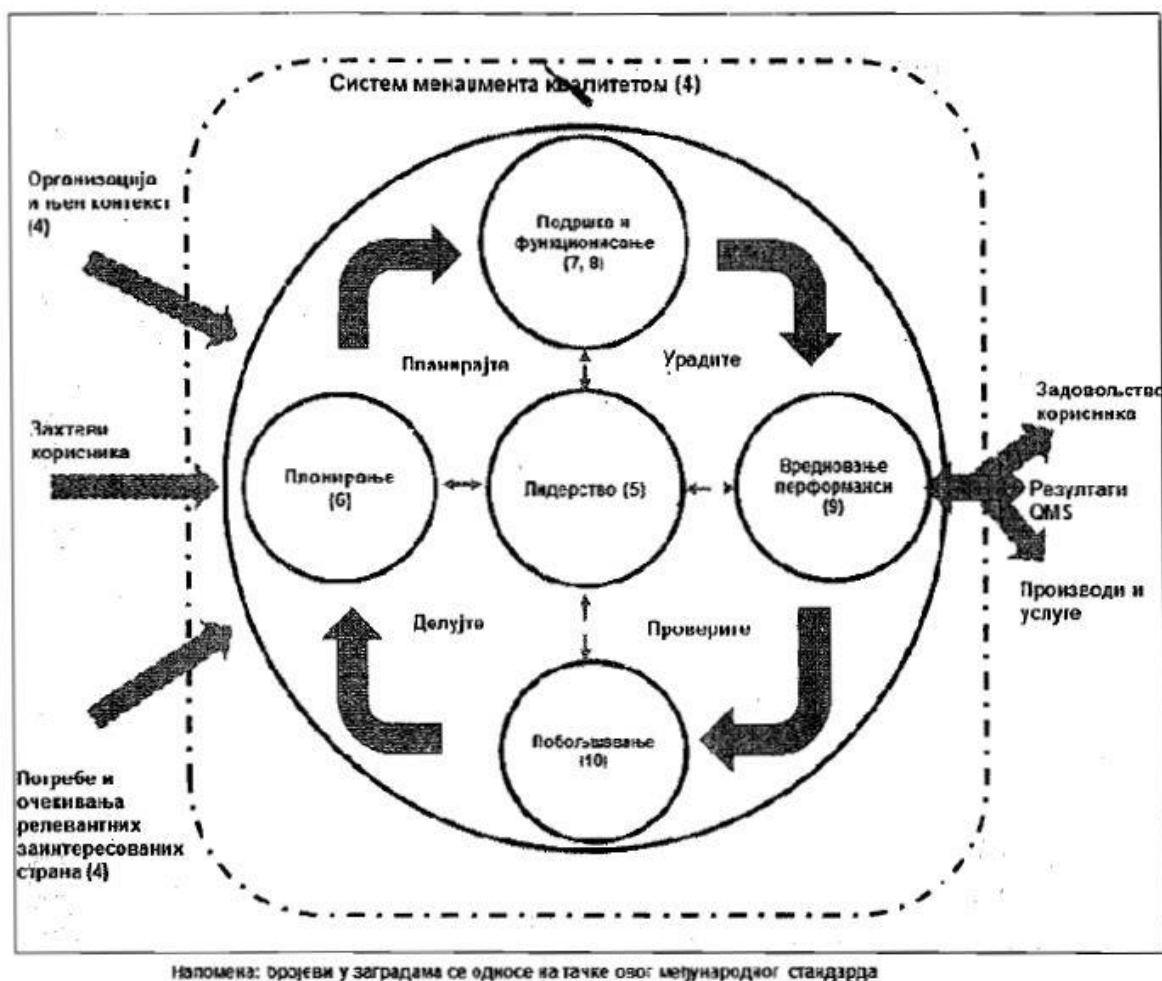
ISO 9001:2015 се заснива на седам принципа менаџмента квалитетом. Ако организације поштују ове принципе, то ће им омогућити да константно стварају нове вредности за своје потрошаче. Седам принципа менаџмента квалитетом су:

1. **Усредсређеност на корисника** – Испуњавање и превазилажење потреба корисника јесте примарни фокус менаџмента квалитетом и оно ће допринети дугорочном успеху организације. Битно је привући али и задржати поверење корисника, због чега је од кључне важности прилагодити се њиховим будућим потребама.
2. **Лидерство** – Уједињено вођство и јединствена мисија који произилазе из јаких лидера изузетно су важни како би се осигурало да сви у организацији разумеју шта се жели постићи.
3. **Ангажовање људи** – Стварање вредности за кориснике ће бити лакше ако организација има способне и ангазоване људе на свим нивоима пословања организације.
4. **Процесни приступ** – Схватање активности као процеса који су повезани и заједно функционишу као један систем омогућава организацији да постигне доследније и предвидљивије резултате. Људи, тимови и процеси не постоје у вакууму, због чега је битно да су сви упознати са активностима организације како би се повећала ефикасност.

5. **Побољшавање** – Успешне организације се увек фокусирају на побољшавање које се јавља као реакција на интерно и екстерно окружење. Ово је од нарочите важности данас када се услови пословања мењају веома брзо.
6. **Доношење одлуке на основу чињеница** – Доношење одлука никада није лак процес и природно обухвата један ниво несигурности, али ако су одлуке засноване на анализи и процени, веће су шансе да ће се добити жељени резултат.
7. **Менаџмент односима** – Данашња предузећа и организације не послују у вакууму. Одрживи успех се може осигурати ако се идентификују све важне везе које постоје са заинтересованим странама.

Најважнији концепт принципа QMS-а је свакако интеграција. Целокупни систем управљања најбоље функционише када је успешно интегрисан. Када се ови принципи примењују у интегрисаним системима менаџмента, они доводе до знатно бољих перформанси – свакако бољих од перформанси свих активности појединачно.

Овај међународни стандард усваја процесни приступ уз помоћ PDCA циклуса и размишљања заснованог на ризику. Процесни приступ омогућава организацијама да достигну дефинисане циљеве тако што ће да планирају процесе, изводе их по плану, процењују перформансе и побољшавају процесе. Конзистентни и предвидљиви резултати се постижу много ефективније и ефикасније када се активностима управља као међусобно повезаним процесима који функционишу као кохерентан систем. Преко овог приказа могу да се прате улази у процес и жељени излази, као и ресурси које треба одвојити за реализацију жељених циљева. Што се тиче размишљања заснованог на ризику, у претходној верзији стандарда оно је било имплицитно поменуто у контексту превентивних мера и решавања неусаглашености. Сада је том питању дат већи значај јер омогућава организацијама да анализирају потенцијалне ризике и прилике, што доводи до боље реализације циљева и бољих резултата, односно, боље продуктивности и ефикасности. Боље разумевање свих фактора процеса омогућава организацији да оптимизује систем и његов учинак. На Слици 1 се може видети приказ PDCA циклуса међународног стандарда ISO 9001:2015.



Слика 1 – PDCA циклус стандарда ISO 9001:2015 (ISO 9001:2015)

Поред тога, имајући у виду конкуренцију на тржишту, треба размотрити и питање иновација у вези са системом менаџмента квалитета. Мотивација која стоји иза имплементације стандарда серије ISO 9001 треба да има утицаја на иновације производа. Организације могу да одлуче да имплементирају ISO 9001:2015 из екстерних или интерних разлога. Могу да одлуче да се сертифицију због екстерних разлога као што је, на пример, притисак од стране корисника, тржишта или власти. Са друге стране, разлози могу бити и интерни, на пример, жеља да се повећају продуктивност и ефикасност (Martínez-Costa et al. 2008). Ови мотивациони фактори могу утицати на перформансе иновација на неколико начина. Екстерна мотивација може усмерити организације да се фокусирају на очекивања и потребе корисника, што може повећати ниво иновација. Са друге стране, интерна мотивација подстиче организације да се више фокусирају на продуктивност и ефикасност. Може се претпоставити да ће правилно примењивање принципа менаџмента квалитетом такође повећати ниво иновација у организацији.

Стога, може се закључити да и интерна и екстерна мотивација повећавају иновације, само због различитих разлога.

У најновијој верзији стандарда задржан је исти примарни циљ: да се континуирано побољшава квалитет и да се осигура да производи и услуге доследно испуњавају захтеве корисника. Уз помоћ размишљања заснованог на ризику у процесном приступу и PDCA циклусу, организације могу на бољи начин да достигну наведене циљеве, осигурају доследност квалитета излаза из процеса и створе вредност за кориснике.

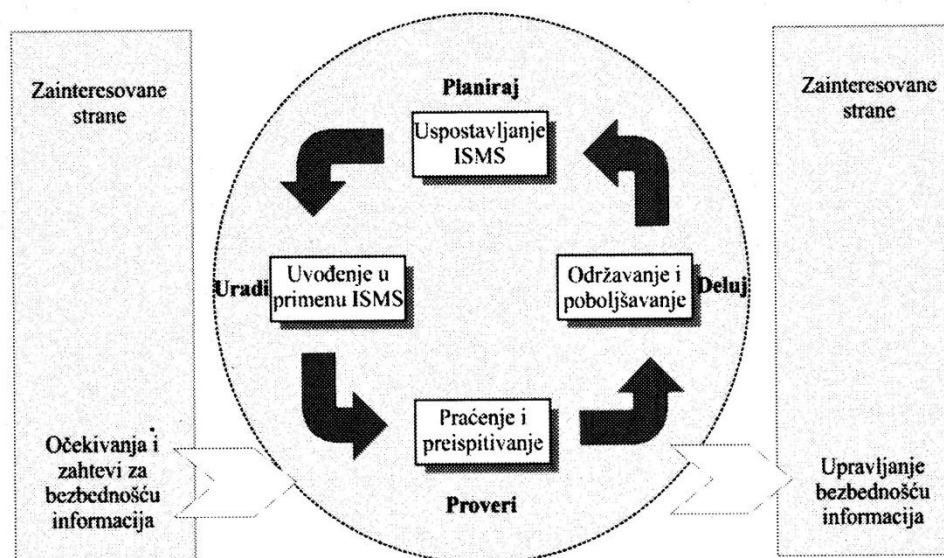
4. Преглед стандарда ISO/IEC 27001:2013

ISO/IEC 27001:2013 (*engl. – Information technology – Security techniques – Information security management systems – Requirements*) обухвата захтеве који су неопходни за успостављање, имплементацију, примену, праћење, преиспитивање, одржавање и побољшавање система менаџмента безбедности информација – ISMS. То је међународни стандард који се односи на заштиту и безбедност информација. Овај стандард има широко подручје примене у процесима који се односе на сигурност информација, као што су: политика сигурности, сигурност организације, сигурност запослених, сигурност материјалних добара, развој и одржавање разних система, и слично. Стандард садржи захтеве који се односе на процену и третирање ризика по информациону сигурност у контексту дате организације. Као што је случај и са осталим стандардима, захтеви су општег карактера и могу се примењивати у свим организацијама, без обзира на њихов тип, величину или природу пословања.

ISO/IEC 27001:2013 усваја процесни приступ, који охрабрује своје кориснике да нагласе важност (Arsovski et al. 2013):

- разумевања захтева информационе сигурности једне организације и потребу да се утврди политика и циљеви информационе сигурности,
- контроле примене и функционисања да би се управљало ризицима информационе сигурности једне организације у контексту укупних пословних ризика организације,
- надзора и провере учинка и ефикасности ISMS-а и
- сталног побољшавања базираног на објективном мерењу.

Стандард усваја PDCA приступ који се примењује на структуру свих ISMS процеса. Процеси као улаз узимају захтеве заинтересованих страна за информационом безбедношћу, и након спровођења одређених активности и подпроцеса, као излазе дају безбедност информација која је у складу са захтевима и очекивањима корисника. У *Планирај* фази, успоставља се ISMS. У овој фази се такође дефинишу предмет и подручје примене ISMS-а, заинтересоване стране, окружење, ресурси и технологија. У *Уради* фази се имплементира и примењује ISMS. У *Провери* фази се ISMS прати и ревидира, а у *Делуј* фази се ISMS одржава и побољшава. На Слици 2 се може видети PDCA приступ примењен на ISMS процесе.



Слика 2 – PDCA приступ примењен на ISMS процесе (Arsovski et al. 2013)

Контроле у оквиру ISO/IEC 27001:2013 стандарда представљају мере за модификовање ризика. ISO/IEC 27001:2013 захтева стварање сета докумената и сертификат да је ISMS заснован на овим документима. Промене у организацији или у технологији такође морају да буду у складу са документованим ISMS захтевима. Поред тога, стандард захтева периодичне ревизије како би ISMS био ефективнији. Ове ревизије се такође спроводе користећи документоване ISMS захтеве. Стандард ISO/IEC 27001:2013 захтева да се одлуке менаџера које се односе на пружање подршке за успостављање и одржавање ISMS-а такође документују. Детаљна документација о одлукама треба да садржи поступак како је свака одлука донета и колико ресурса је одређено за примену те одлуке (Beckers et al. 2013).

Предности увођења ISO/IEC 27001:2013 јесу:

- конкурентска предност;
- смањење ризика од оштећења и губитка информација, а самим тим и трошкова;
- усаглашеност са важећим законским прописима;
- веће поверење свих укључених страна због знања да су њихови подаци безбедни;
- постојање одговорности за безбедност информација од стране свих и на свим нивоима у организацији.

Сврха серије међународних стандарда ISO 27000 јесте да омогуће организацијама свих величина да на прави начин уведу, примењују и одржавају системе информационе

безбедности. Првенствено се користи у оним делатностима где се организације баве информацијама и информационим системима, и то највише у предузећима која се баве информационим технологијама и у предузећима која се баве финансијама и економијом.

Усвајањем овог стандарда и уз помоћ сертификације, предузеће показује клијентима и заинтересованим странама да је свесно важности заштите података, како својих тако и података других страна. Самим тим, предузеће стиче већи углед и код својих запослених и код клијената. Такође, предузеће добија шансу да има бољу позицију на тржишту у односу на конкуренцију.

Такође је битно напоменути да је ова серија стандарда у вези са другим стандардима који се баве безбедношћу информација. Ови стандарди наглашавају да није могуће у потпуности искључити ризик по питању безбедности информација, али уз помоћ примене ових стандарда, предузећа могу успоставити критеријуме и процедуре којима ће на најбољи начин заштити податке. Свакако треба напоменути да је успостављање ISMS-а тежак задатак јер се састоји од неколико тешких корака, као што су идентификација вредних информација, анализа претњи и ризика, разматрање безбедности, и слично. Такође, стандард захтева поштовање закона и прописа, као и питања приватности. Сви ови захтеви представљају изазове из различитих дисциплина за инжењере који се баве информационом сигурношћу.

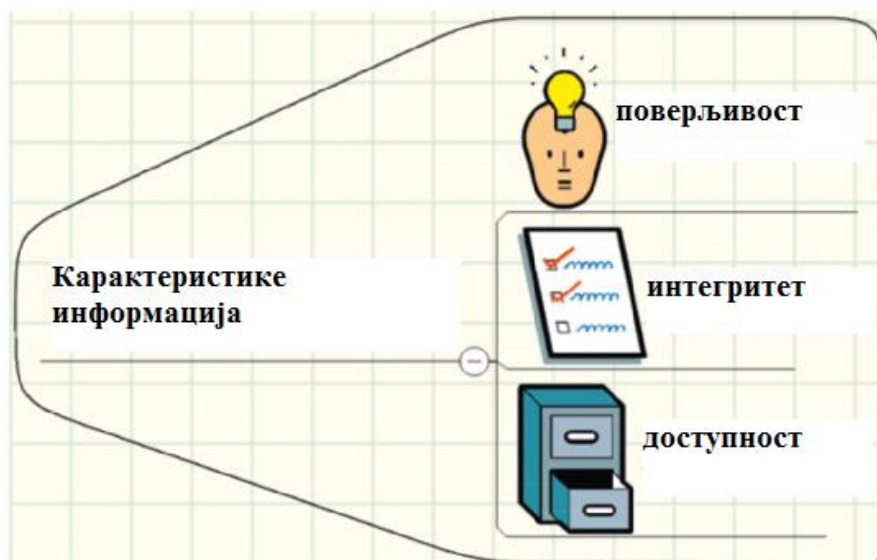
Као што је већ речено, сигурност информација је од круцијалне важности у свим организацијама у финансијском сектору, као и у организацијама у компјутерској делатности, где нарушавање безбедности може проузроковати знатну штету по питању поверења и конкурентности организације у питању. Сигурност информација је најважнији оперативни ризик са којим се суочавају банке, фирме које се баве инвестирањем и осигурањем, софтверске фирме. Њихова конкурентност зависи од ефикасности и нивоа професионализма са којим се запослени суочавају са таквим ризицима. ISO/IEC 27001: 2013 омогућава компанијама да смање потенцијални ризик и повећају поверење својих клијената. Као што је већ речено, нарушавање безбедности може скупо коштати компанију. Истраживање о безбедности на интернету које је спровео Институт за ИТ управљање (IT Governance Institute 2004) наводи: „Резултати показују да је објављивање вести о нарушавању безбедности на интернету негативно повезано са вредности те фирме на тржишту. У анализираном узорку, фирме којима је

нарушена безбедност изгубиле су, у просеку, 2,1% своје тржишне вредности у року од два дана након објаве. “ (ISO Management Systems 2009).

Иако се сигурност информација не односи само на компјутере, софтвер и информационе системе, развој сигурности информација је подстакнут све већом комплексношћу информационих технологија и све већим ослањањем на информационе технологије. Данас у свету постоји много методологија за управљање сигурношћу информација, од којих су неке предмет међународних стандарда. Једна од предложених методологија заснована је на следећа четири принципа:

1. Организацијама је потребно систематско решење, тј. ефективни ISMS.
2. ISMS треба да буде заснован на концептима управљања ризиком.
3. ISMS треба да буде интегрисан у оперативни систем менаџмента ризиком организације.
4. Концепти система менаџмента сигурношћу информација морају да буду уграђени у корпоративну културу организације.

Иако се сигурност информација обично повезује са компјутерским вирусима и хакерима, имплементација сигурности информација је много шири појам од једноставног инсталирања антивирус програма и енкрипције података. Пружање информационе безбедности подразумева заштиту сигурности *свих информација једне организације*. У контексту терминологије ISO/IEC 27001:2013, све оно што има неку вредност за организацију и повезано је са информацијама – софтвер, документација, сервери, компјутери, базе података, запослени, и остало – представља информацију која треба да се заштити. У практичном примеру у банкарству, скоро је немогуће наћи банкарски процес који не садржи неку врсту информација – трансакције се обављају преко информационих система, резултати финансијских радњи се чувају у документацији, и слично. Безбедност информација, како је дефинисана у ISO/IEC 27001:2013, представља чување три кључне карактеристике информације – поверљивост, доступност и интегритет (*engl. Confidentiality, Availability, Integrity*), чији се приказ може видети на Слици 3.



Слика 3 – Три кључне карактеристике информација (ISO Management Systems 2009)

Ниво до којег поверљивост, доступност и интегритет информације у стварности одговара жељеном нивоу заправо представља стање сигурности те информације. У контексту ризика, може се рећи да су ризици догађаји који мењају нивое поверљивости, доступности и интегритета информације, што доводи до непредвиђених трошкова и губитака за предузеће. Зато је неопходно познавати ризике по питању безбедности информација, као и процедуре управљања ризиком. Што се тиче идентификовања потенцијалних ризика, може се рећи да постоје три главна извора од којих се могу добити те информације, а то су: *запослени, клијенти и резултати интерних процена*. Управо у овим случајевима ISO/IEC 27001:2013 може бити од користи јер пружа препоруке како идентификовати безбедносне ризике и мере како умањити те ризике. С тим у вези је управо и веза са захтевом ISO 9001 који се односи на корективне и превентивне мере – реч је о процедури која обухвата идентификовање оперативног ризика, процену, креирање радне групе, одређивање рањивих места у систему и узрока настанка ризика, одређивање начина управљања ризиком, и поновно разматрање ефективности имплементиране стратегије управљања ризиком. Наравно, ове опште кораке треба прилагодити типу ризика о коме је реч. Уопштено гледано, логички ток процеса управљања оперативним ризицима може се илустровати приказом на следећем дијаграму – Слика 4. Два кључна процеса за идентификацију ризика по безбедности информација – управљање информацијама и управљање ризицима по информације – успостављају основну логику ISMS-а.



Слика 4 – Ток процеса управљања оперативним процесима (ISO Management Systems 2009)

Овај процес пружа одговор на питање шта треба да се заштити. Ради потпуне идентификације ризика по безбедност информација, потребно је да постоји инвентар свих информација, ранжираних по критичности. Процедура „Класификација информација“ може се увести за ову сврху. С обзиром да ризици по безбедност информација доводе до промена у карактеристикама информација, њихов инвентар мора бити доступан члановима одговарајућег тима за безбедност, као и власницима предузећа и запосленима на нивоу топ менаџмента. Такав инвентар треба да садржи следеће карактеристике: нивое поверљивости, интегритета и доступности, резултујући ниво критичности, власника и кориснике информације у питању. Пример се може видети у Табели 1.

Табела 1. Инвентар информација

Назив	Поверљивост	Интегритет	Доступност	Критичност	Власник	Корисници
База података клијента	Висок ниво	Висок ниво	Висок ниво	Висок ниво	Директор продајне дивизије	Продајна дивизија

Анекс А стандарда ISO/IEC 27001:2013 наводи листу стандардних контрола, односно, процедура које се могу применити како би се систематски ублажили уобичајени ризици. Како је наведено у тексту самог стандарда, контролни циљеви и контроле наведени у Табели А.1 директно су изведени и усаглашени са онима наведеним

у ISO/IEC 27001:2013, у Тачкама 5 до 18 и треба да се користе у контексту са Тачком 6.1.3. Дакле, кључне процедуре које су наведене у Анексу А овог стандарду јесу следеће:

Табела 2. Стандардне контроле из Анекса А стандарда ISO/IEC 27001:2013

A.5 Политике о безбедности информација
A.5.1 Смернице за менаџмент сигурношћу информација
A.6 Организација информационе безбедности
A.6.1 Интерна организација
A.6.2 Мобилни уређаји и рад на даљину
A.7 Безбедност људских ресурса
A.7.1 Пре запослења
A.7.2 Током запослења
A.7.3 Прекид радног односа и промена послодавца
A.8 Управљање ресурсима
A.8.1 Одговорност за ресурсе
A.8.2 Класификација информација
A.8.3 Управљање медијумима
A.9 Контрола приступа
A.9.1 Пословни захтеви контроле приступа
A.9.2 Управљање корисничким приступом
A.9.3 Одговорности корисника
A.9.4 Контрола приступа систему и апликацијама
A.10 Криптографија
A.10.1 Криптографске контроле
A.11 Физичка безбедност и безбедност животне околине
A.11.1 Обезбеђена подручја
A.11.2 Опрема
A.12 Оперативна безбедност
A.12.1 Оперативне процедуре и одговорности
A.12.2 Заштита од штетних програма
A.12.3 Сигурносна копија (<i>engl. backup</i>)
A.12.4 Прављење логова и надзор
A.12.5 Контрола оперативног софтвера
A.12.6 Управљање техничким рањивостима
A.12.7 Разматрање ревизија у односу на информационе системе
A.13 Безбедност комуникација

A.13.1 Управљање безбедношћу мреже
A.13.2 Трансфер информација
A.14 Аквизиција, развој и одржавање система
A.14.1 Безбедносни захтеви информационих система
A.14.2 Безбедност у развојним процесима и процесима подршке
A.14.3 Подаци тестирања
A.15 Односи са добављачима
A.15.1 Безбедност информацију у односима са добављачима
A.15.2 Управљање испоруком услуга у договору са добављачима
A.16 Управљање безбедносним информационим инцидентима
A.16.1 Управљање безбедносним информационим инцидентима и побољшањима
A.17 Аспекти безбедности информација управљања континуитетом пословања
A.17.1 Континуитет безбедности информација
A.17.2 Редундансе
A.18 Усаглашеност
A.18.1 Усаглашеност са правним и уговорним захтевима
A.18.2 Прегледи стања безбедности информација

5. Преглед стандарда ISO 26000:2010

Стандард ISO 26000:2010 Упутство о друштвеној одговорности (*engl. Guidance on Social Responsibility*) није систем менаџмента и он садржи смернице уместо захтева, па се предузећа не могу сертифициовати према њему за разлику од других стандарда. Уместо тога, овај стандард има за циљ да појасни појам друштвене одговорности, помаже предузећима и организацијама да преведу принципе у ефективне активности и даје примере најбоље праксе у свету у вези са друштвеном одговорношћу у оквиру Анекса 1. Стандард је објављен од стране Међународне организације за стандардизацију 2010. године након петогодишњих преговора између различитих група стејкхолдера широм света, укључујући следеће групе:

1. потрошачи
2. влада
3. индустрија
4. организације рада
5. невладине организације
6. групе које укључују пружање услуга, подршке, истраживања, и других.

Пре свега, треба дефинисати друштвену одговорност. Европска комисија у својим Смерницама за политику друштвене одговорности предузећа (EC White Paper on Corporate Social Responsibility, 2003), друштвену одговорност предузећа дефинише као „концепт према којем предузеће на добровољној бази интегрише бригу о друштвеним питањима и заштити животне средине у своје пословне активности и односе са заинтересованим странама (власницима, деоничарима, запосленима, потрошачима, добављачима, владом, медијима и широм јавношћу)“ (ISO 26000, 2016). Даље, у одељку стандарда Термини и дефиниције, друштвена одговорност дефинише се као (ISO 26000:2010): „одговорност организације за ефекте њених одлука и активности на друштво и животну околину, кроз транспарентно и етичко понашање које:

- доприноси одрживом развоју, здрављу и добробити друштва;
- узима у обзир очекивања стејкхолдера;
- постоји у сагласности са применљивим законом и доследан је међународним нормама понашања; и
- јесте интегрисано у оквиру организације и примењивано у њеним везама.“

У опису настанка идеје о друштвеној одговорности у оквиру овог стандарда наведено је: „Идеја да је друштвена одговорност применљива на све организације појавила се јер су различити типови организација, не само оне у пословном свету, увиделе да и оне имају одговорности да допринесу одрживом развоју.“ Када је реч о друштвеној одговорности, она се, једноставно речено, заснива на принципима и правилима понашања који се сматрају правилним, односно, моралним, у контексту дате ситуације. Овакво друштвено одговорно понашање треба да буде у служби једног већег циља а то је одрживи развој и добробит друштва. Иако не постоји потпуна листа принципа друштвене одговорности, у оквиру стандарда се наводе следећих седам принципа:

1. одговорност,
2. транспарентност,
3. етичко понашање,
4. поштовање интереса стејкхолдера,
5. поштовање правне државе,
6. поштовање међународних норми понашања,
7. поштовање људских права.

1. Принцип одговорности наводи да организација треба да буде одговорна за сопствене утицаје на друштво и животну околину. Овај принцип се заснива на фундаменталном концепту да организација прихвата моралну обавезу да буде одговорна за своје поступке. Организација треба да одговара за резултате одлука и активности организације, укључујући значајне последице, макар оне биле и нежељене или непредвиђене и треба да одговара за битне утицаје одлука и активности организације на стејкхолдере.

2. Принцип транспарентности наводи да организација треба да делује на транспарентан начин по питању својих одлука и активности које утичу на друге. Организација треба да открије своје политике, одлуке и активности за које је одговорна, укључујући стварне и потенцијалне ефекте на друштво и животну околину на јасан, балансиран и истинит начин, до оне мере којом је то разумно довољно. Организација треба да буде транспарентна по питању: начина на који доноси одлуке и примењује исте, укључујући дефинисање улога и одговорности у оквиру организације; стандарда и критеријума на основу којих организација оцењује свој учинак; сврхе, природе и места

обављања својих активности; познатих или вероватних ефеката својих одлука на друге; и по питању својих стејкхолдера.

3. Принцип етичког понашања наводи да се организација у сваком тренутку мора понашати етички исправно. Понашање организација треба да осликава признате етичке принципе или правила дужности. Организација треба да усвоји и примењују стандарде етичког понашања који одговарају њеној сврси и њеним активностима. Организација треба да обавља своје послове тако да промовише етишко понашање у оквиру организације међу својим запосленима и у интеракцијама са другима.

4. Принцип поштовања интереса стејкхолдера наводи да организација треба да поштује и узима у обзир интересе својих стејкхолдера. Појединци и групе који имају један или више интереса по питању било којих активности или одлука организације могу се сматрати њеним стејкхолдерима, односно, заинтересованим странама. Организација треба да: идентификује своје стејкхолдере; узме у обзир и поштује интересе и потребе својих стејкхолдера: размотри однос интереса стејкхолдера и ширих интереса друштва и одрживог развоја; и размотри како нека одлука или активност може утицати на њих.

5. Принцип поштовања правне државе наводи да организација мора да поштује правила закона. Организација треба да буде свесна важећих захтева и прописа, да осигура да релевантни чланови организације буду њих свесни и да се постара да се поштују закон и прописи. Самим тим, активности и одлуке организације треба да буду у оквиру важећег правног оквира.

6. Принцип поштовања међународних норми понашања наводи да организација треба да поштује релевантне међународне норме када су оне повољније по питањима одрживог развоја и добробити друштва. Међународне норме су принципи, очекивања или стандарди понашања који су универзално признати и који су засновани на међународно прихваћеним принципима закона.

7. Принцип поштовања људских права наводи да организација треба да призна и значај и универзалност људских права. Организација треба да поштује права наведена у Универзалној декларацији о људским правима; прихвати да су ова права универзална; у ситуацијама где људска права или одређене законске норме нису признате, поступа по моралним начелима и ради на унапређењу ситуације колико је то у њеној могућности.

Као што је наведено у Уводу стандарда ISO 26000:2010, пословање организације у односу на друштво у којем обавља своје делатности и у односу на њен утицај на животну околину постало је критични фактор у мерењу свеукупног учинка те организације и њене могућности да настави да успешно обавља своје делатности. Јавља се дугорочна потреба да се осигурају здрави екосистеми, друштвена једнакост и добро пословање организације. Самим тим, утисак о друштвеној одговорности једне организације може да утиче на (ISO 26000:2010):

- конкурентну предност организације,
- репутацију организације,
- способност организације да привуче и задржи раднике, муштерије, клијенте или кориснике,
- одржавање мотивисаности, посвећености и продуктивности запослених,
- мишљење о организацији које о њој имају инвеститори, власници, донатори, спонзори и финансијка заједница, и
- везу организације са компанијама, владом, медијима, добављачима, сарадницима, муштеријама и заједницом у којој послује.

Овај међународни стандард пружа смернице о најбитнијим принципима друштвене одговорности, при чему је пажња посвећења укључивању стејкхолдера у препознавању значаја и остваривању друштвене одговорности. Циљ овог стандарда је да се схвати значај резултата и побољшања учинка по питању друштвене одговорности. Такође, као што је и случај са осталим стандардима, овај стандард треба да буде од користи свим типовима организација у приватном, јавном и непрофитном сектору, без обзира на величину организације, и без обзира на то да ли та организација послује у развијеним земљама или у земљама у развоју. Поред тога, ове смернице могу користити организацијама које тек почињу да се баве питањем друштвене одговорности, али и оним организацијама које већ имају нешто више искуства по том питању. Главна идеја овог стандарда је да се уведе друштвено одговорно понашање у саму организацију и њено пословање, користећи дате смернице. Као што је већ речено, битно је напоменути да се организације не могу сертифициовати према овом стандарду. Такви искази, да је организација *сертифициована* према ISO 26000:2010, представљају погрешну интерпретацију и намеру овог међународног стандарда. Општи преглед овог стандарда се може видети у Табели 3 (ISO 26000:2010):

Табела 3. Преглед стандарда ISO 26000:2010

Назив тачке	Број тачке	Опис садржаја тачке
Предмет и подручје примене	Тачка 1	Дефинише предмет и подручје примене овог међународног стандарда и идентификује одређена ограничења и искључења.
Термини и дефиниције	Тачка 2	Идентификује и пружа кључне термине који су од фундаменталног значаја за разумевање друштвене одговорности и за коришћење овог међународног стандарда.
Разумевање друштвене одговорности	Тачка 3	Описује важне факторе и услове који су утицали на развој друштвене одговорности и који настављају да утичу на природу и праксу овог питања. Такође описује сам концепт друштвене одговорности – шта она подразумева и како се примењује у организацијама. Ова тачка укључује смернице за мала и средња предузећа по питању коришћења овог међународног стандарда.
Принципи друштвене одговорности	Тачка 4	Уводи и објашњава принципе друштвене одговорности.
Препознавање друштвене одговорности и укључивање стејкхолдера	Тачка 5	Односи се на два начина примене друштвене одговорности: препознавање своје друштвене одговорности у оквиру саме организације, и идентификовање исте и ангажовање њених стејкхолдера. Пружа смернице о вези између организације, њених стејкхолдера и друштва; о препознавању кључних области и питања друштвене одговорности; и о пољу утицаја организације.
Смернице о кључним областима друштвене одговорности	Тачка 6	Објашњава које су кључне области и повезана питања која се односе на друштвену одговорност. За сваку кључну област дају се информације о предмету и подручју примене, вези теме са друштвеном одговорношћу, повезаним принципима и додатним разматрањима, и повезаним активностима и очекивањима.
Смернице о интеграцији друштвене одговорности у оквиру организације	Тачка 7	Пружа смернице о практиковању друштвене одговорности у оквиру организације. Ово подразумева смернице у вези са: разумевањем друштвене одговорности организације, интеграцијом друштвене одговорности у оквиру организације, комуницирањем у вези са друштвеном одговорношћу, побољшањем кредибилитета организације по питању друштвене одговорности, напретком

		ревидирања и побољшањем учинка и процењивањем добровољних иницијатива по питању друштвене одговорности.
Примери добровољних иницијатива и алата за примену друштвене одговорности	Анекс А	Представља некомплетну листу добровољних иницијатива и алата везаних за друштвену одговорност који се баве аспектима једне или више кључних области или интеграцијом друштвене одговорности у оквиру организације.
Скраћени термини	Анекс Б	Садржи скраћенице које се користе у овом међународном стандарду.
Библиографија		Садржи референце које се односе на међународне инструменте и стандарде који се помињу као извори у тексту овог међународног стандарда.

Како би организација идентификовала предмет и подручје примене друштвене одговорности и правилно одредила своје приоритете, она прво мора да идентификује релевантне кључне области и повезана питања. Седам кључних области друштвене одговорности и релевантна питања дата су у Табели 4 (Arsovski et al. 2013):

Табела 4. Седам кључних области друштвене одговорности и релевантна питања

1. Управљање организацијом	
2. Људска права: • признање за рад • ризичне ситуације у вези са људским правима • избегавање саучесништва • решавање увреда • дискриминација и осетљиве групе • цивилна и политичка права • економска, социјална и културна права • основна права на раду	5. Фер пословна пракса: • анти-корупција • одговорно политичко учешће • фер конкуренција • промоција друштвене одговорности у сфери утицаја • поштовање права својине
3. Радна пракса: • запошљавање и односи код запошљавања • услови рада и социјална заштита • социјални дијалог • здравље и безбедност на раду • развој људи и обука на радном месту	6. Заштита потрошача: • фер маркетинг, чињенично и непристрасно информисање и фер уговорна пракса • заштита здравља и безбедност корисника • одржива потрошња • услуга и подршка кориснику и решавање спорова

4. Животна средина: • спречавање загађења • одрживо коришћење ресурса • ублажавање климатских промена и прилагођавање • заштита животне средине, биодиверзитета и обнављање природних станишта	• заштита података корисника и приватност • приступ основним услугама • образовање и свест 7. Укључивање заједнице и развој: • укључивање заједнице • образовање и култура • креирање радних места и развој вештина • развој технологије и приступ технологији • стварање богатства и прихода • здравље • инвестиције у друштво
---	---

Бављење кључним областима треба да буде засновано на принципима друштвене одговорности. Иако је већина кључних области повезана, природа кључне области *Управљање организацијом* јесте нешто другачија. Ова област описује процес доношења одлука и процесе који олакшавају деловање по питању осталих кључних области. Организација треба да идентификује и да се позабави оним кључним областима и питањима које су релевантне за њене одлуке и активности. Такође, организација треба да посматра кључне области на холистички начин, односно, треба да размотри све кључне области и питања и њихову међузависност, а не само да се концентрише на једну област без разматрања потенцијалних ефеката њених активности на остале области.

Претходна истраживања су приказала разне предности које организације могу да искусе због друштвене одговорности. На пример, доказано је да друштвена одговорност позитивно утиче на одговоре потрошача о производима и лојалност потрошача (Du et al. 2011), задовољство потрошача (Luo & Bhattacharya 2006), перцепције о компетентности предузећа и остало. Када се ради о компетентности, један од кључних аспеката јесу иновације зато што оне омогућавају предузећу да одговара на захтеве тржишта који се стално мењају, а самим тим утичу на профитабилност и дугорочни опстанак сваке организације (Hauser et al. 2006).

Може се претпоставити да предузећа која имају више друштвено одговорних активности имају и шири приступ екстерном знању различитих екстерних стејкхолдера због тога, а то знање може увећати иновације. Такође се може претпоставити да однос између активности друштвене одговорности и иновација може утицати на

карактеристике фирме (нарочито ниво истраживања и развоја) и на стање на тржишту (нарочито конкурентност) (Luo & Du 2014).

Програми и активности друштвене одговорности стварају нове везе и ојачавају постојеће. Самим тим, организације могу да створе нове везе са стејкхолдерима – потрошачима, запосленима, инвеститорима. Такође, кроз примере добре праксе, организације могу да побољшају свој имиџ а самим тим и поверење које постојећи стејкхолдери имају. Друштвено одговорне фирме уживају веће поверење, веће нивое задовољства и лојалности међу разним стејкхолдерима, укључујући потрошаче, запослене, инвеститоре, пословне partnere и заједнице (Du et al. 2011).

Као последица тога, фирме са ширим и бољим мрежама имају бољи приступ идејама и знањем које се налазе у мрежама стејкхолдера. Јаке везе између стејкхолдера и фирме ће подстаћи стејкхолдере да добровољно деле информације и ресурсе са фирмом, што ће њој омогућити да искористи тај извор екстерног знања (Jansen et al. 2006). Екстерно знање стејкхолдера и њихова стручност могу да допуне интерно знање фирме, а самим тим и да поспеше иновације.

Као што је већ речено, два кључна индикатора пословних исхода насталих због друштвене одговорности јесу истраживање и развој и конкурентност. Дакле, док истраживање и развој утичу на способност фирме да створи иновативне исходе из активности друштвене одговорности, конкурентност на тржишту утиче на мотивацију фирме да то учини. Фирме које имају јаку конкуренцију морају да буду веома ефективне у проналажењу нових потреба тржишта и старању нових производа и услуга. Самим тим, конкуренција ће мотивисати фирму да обрати више пажње на екстерно знање и да га радо искористи како би створила нове идеје и нове иновације. Такође, улагање у истраживање и развој ће побољшати способност фирме да усваја и користи екстерно знање добијено из активности друштвене одговорности и новонасталих мрежа између стејкхолдера.

Када је реч о имплементацији ISO 26000:2010, организација прво треба да размотри карактеристике друштвене одговорности и њену везу са одрживим развојем (Тачка 3), након чега треба да размотри принципе друштвене одговорности наведене у Тачки 4. При практиковању друштвене одговорности, организације треба да поштују ове принципе, заједно са принципима који се односе на појединачне кључне области (Тачка 6). Али, пре него што анализира кључне области и повезана питања, као и релевантне

акције и очекивања (Тачка 6), организација треба да размотри два фундаментална начина практиковања друштвене одговорности: препознавање своје друштвене одговорности у оквиру своје сфере утицаја и идентификовање и укључивање својих стејкхолдера (Тачка 5). Када организација разуме принципе и идентификује кључне области и релевантна и битна питања друштвене одговорности, онда организација може да настоји да интегрише исте у своје пословне одлуке и активности, користећи смернице и упутства наведена у Тачки 7. Ово подразумева: интегрисање друштвене одговорности у политику, организациону културу, стратегије и пословање организације; изградњу интерних компетентности за питање друштвене одговорности; обављање интерних и екстерних разговора о овом питању; и регуларно ревидирање активности повезаних са друштвеном одговорношћу. На крају, организација увек треба имати у виду да је општи циљ друштвене одговорности да максимално допринесе одрживом развоју.

6. Интеграција захтева стејкхолдера у предузећу „Интранеа решења“

6.1 Основни подаци о предузећу „Интранеа решења“

Назив организације је: ИНТРАНЕА РЕШЕЊА друштво са ограниченом одговорношћу, Крагујевац.

ПИБ : 104876715

Матични број :20257032

Шифре делатности: 1729,1813,4690,4791

„Интранеа решења доо“ послује од 20.02.2007. године. По броју запослених спада у мала предузећа.

Седиште: Индустијска 7, 34000 Крагујевац, Србија

Тел.: +381 34 300 081,

Емаил: info@datastation.com,

web: www.datastation.com

Делатност : Рачунарско програмирање (шифра: 6201).

Квалитетно пружање услуге и њено усавршавање као стални процес, основна је обавеза сваког запосленог у ИР.

Пословни мото ИР је: *Идејама до иновативности и унапређења*

Основни портфолио обухвата купце и кориснике са којима ИР развија добре пословне односе и који чине суштину пословања. ИР има купце и кориснике из преко 40 земаља.

ИР сарађује и са домаћим и иностраним компанијама.

Софтвер ИР је DS-DataStation.

Апликације (сегменти софтвера) – Управљање идејама – Idea Station, Развој/иновирање нових производа и услуга – Launch Station, Праћење тржишног пословања – Market Station (Слика 5).

Idea Station даје моћ организацији – клијенту да ствара, уређује и управља великим бројем идеја за нове производе и услуге кроз ефикасну сарадњу запослених, повезан ток рада и моћне идејне функционалности.

Launch Station је последња генерација Cloud-базираног софтвера за управљање развојем нових производа и услуга. Launch Station комбинује ефикасне методологије развоја нових производа са предностима цлоуд цомпутинг технологије и бизнис интелигенције. Овај спој даје моћ да се имплементирају модерни изазови убрзаним лансирањем нових производа и услуга.

Market Station омогућује праћење тржишта и ефеката пласмана новог производа.

DataStation праве иноватори за иноваторе. Од 2007. године, компанија је расла и развијала се, инвестирајући доста средстава у водећи софтвер за управљање иновацијама, као и у услуге пружања консалтинга. Фокус компаније је стављен на иновирање и сарађивање. Компанија помаже организацијама да повећају приходе кроз одрживо стварање и унапређење производа и услуга. Софтвер који прави компанија је различит јер се своди на свакодневне иновације и на оптимизације већ постојећих идеја.



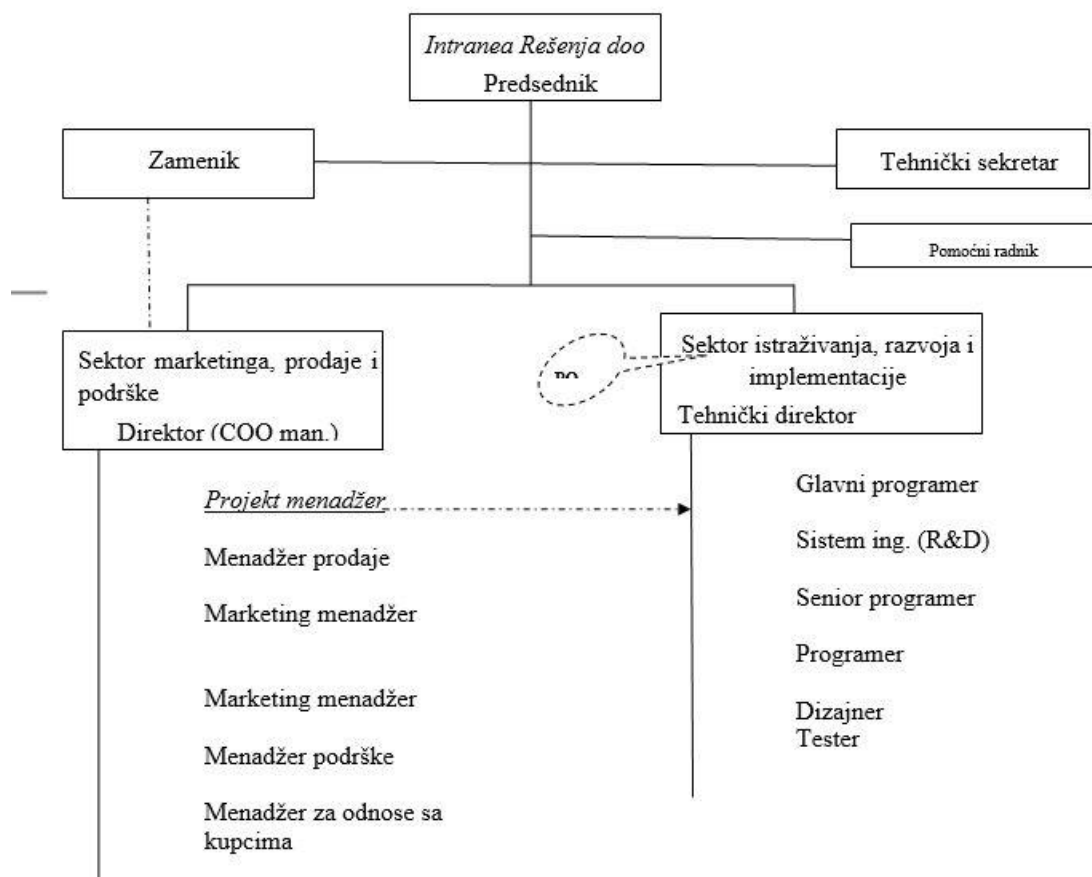
Слика 5 – Компоненте DataStation (Пословник о квалитету ИР)

Што се тиче тренутног стања по питању сертификације у овом предузећу, предузеће „Интранеа решења“ је сертифициковано према стандарду ISO 9001:2008. У блиској будућности је у плану и сертификација према најновијој верзији стандарда ISO 9001:2015. Што се тиче стандарда ISO/IEC 27001:2015, предузеће још увек није сертифициковано према овом стандарду, али је стандард усвојен и део је интегрисаног система менаџмента предузећа, а предузеће је на путу да добије и званични сертификат. При увођењу система менаџмента безбедношћу информација, предузеће је ангажовало консултанте из Института за безбедност информација из Новог Сада. Судећи по речима

директора пословних операција, мотивација за увођење овог стандарда била је међународна потврда коју ће сертификат донети да предузеће послује по највишим стандардима који се захтевају од фирме у ИТ сектору, што је битно за ову конкретну фирму која развија софтверска решења за управљање иновацијама, што је по питању безбедности врло осетљив процес. Такође, речима директора: „Увођење прописаних полиса и процедура довело је до унапређења квалитета услуге коју пружамо, до веће релевантности наше фирме у преговорима са потенцијалним клијентима, као и до реафирмације квалитета услуге коју пружамо остојећим клијентима.“ (Савети за мала предузећа у Србији, 2016). Речима техничког директора: „Увођењем QMS-а и ISMS-а у складу са захтевима међународних стандарда ISO/IEC 27001 и ISO 9001 компанија је омогућила стално унапређење квалитета и ефикасности у вези са сигурносним техникама и решењима за даљи развој безбедности, што свакако доприноси бољем брендирању и тржишним могућностима ове успешне компаније на пољу развоја софтвера за управљање иновацијама у организацији.“ Даље, када је реч о стандарду ISO 26000:2010, предузеће још увек није усвојило и имплементирало одређене праксе и активности наведене по питању друштвене одговорности. Тренутно, активност коју предузеће организује у овом пољу јесте едукација средњошколаца и рад на едукацији у средњим школама. На овај начин се побољшава квалитет образовања у локалној заједници, а дугорочно гледано, стварају се будући контакти који могу пружити ново, иновативно знање предузећу.

Организацијска структура „Интрanea решења“ приказана је на Слици 6. У контексту организацијске структуре предузећа „Интрanea решења“ и друштвене одговорности, може се размотрити једна од кључних области друштвене одговорности, а то је *Управљање организацијом*. Како је наведено у стандарду, управљање организацијом представља систем помоћу којег организација доноси и примењује одлуке. Управљање организацијом је јединствена област јер је истовремено и кључна област коју треба размотрити и начин на који организација може повећати своју способност да примењује друштвено одговорно понашање. С тим у вези, неке од активности у оквиру ове области јесу: подстицање запослених да учествују у процесу доношења одлука; делегирање обавеза и одговорности онако како је то одређено у структури предузећа (видети Сliku 6); ефикасно коришћење финансијских, природних и људских ресурса уз фер заступљеност мањина (укључујући и жене) на вишим позицијама у организацији (у овом

случају, припадница женског пола на вишој позицији јесте само представница руководства за безбедност података).

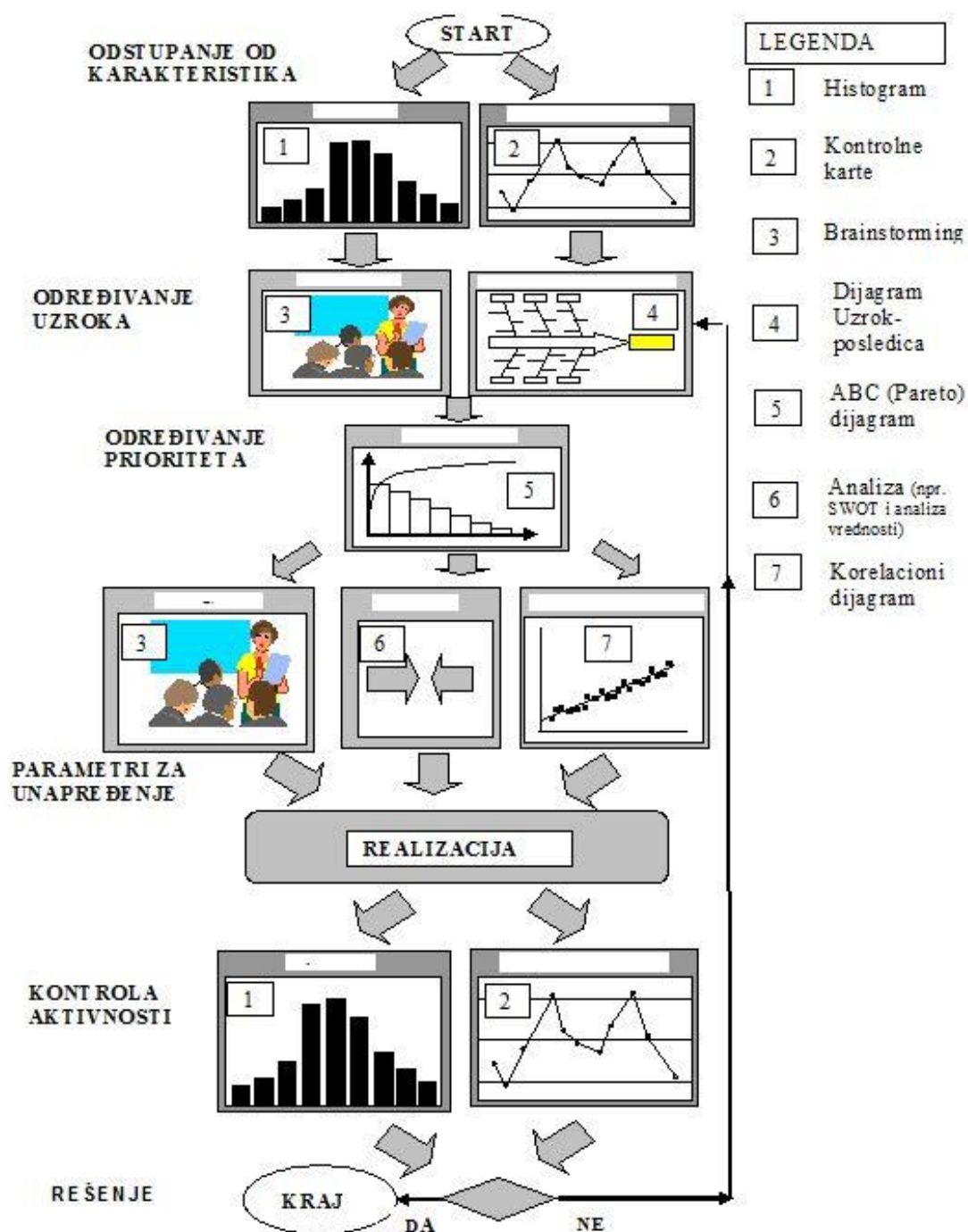


Слика 6 – Организацијска структура предузећа „Интранета решења“ (Пословник о квалитету ИР)

Када је реч о мерењу, праћењу и побољшавању рада, системски заснован и систематски вођен процес сталног унапређења квалитета услуга и процеса рада, са циљем повишења сопствене компетитивности и ефективнијег задовољења потреба купаца и корисника, представља важан део активности у подручју квалитета.

Даје се значај развоју и примени алата - метода и техника за достизање високог нивоа квалитета и његово стално унапређење, за шта су одговорни руководиоци. Потребе за применом статистичких и других метода у процесима рада утврђене су у виду: сталних активности - у процесима реализације делатности на бази одговарајуће методологије и повремених активности - у случају посебно пројектованих захвата на унапређењу квалитета услуга и процеса рада, дефинисаних од стране руководиоца,

првенствено директора, и могућностима апликација. Углавном се примењују основни алати квалитета приликом овог процеса (Слика 7).



Слика 7 – Основни алати квалитета (Пословник о квалитету ИР)

6.2 Преглед стандарда

У стандарду ISO 26000:2010 је наведено да друштвена одговорност може да се уведе у организацију без неких драстичних промена у структури организације. Друштвена одговорност треба да се интегрише у постојеће системе, политике и структуре. Такође, цела Тачка 7 овог стандарда се односи на увођење пракси друштвене одговорности у организацију, а нарочито Тачка 7.4. где је наведено да друштвена одговорност треба да буде део стратешког оквира организације. Са тачке гледишта стејкхолдера, треба размотрити питања која се односе на њихове интересе и захтеве. Наравно, прво треба идентификовати стејкхолдере организације и њихове потребе. Приказ потреба стејкхолдера и релевантних области може се наћи у следећој табели.

Табела 5. Однос стејкхолдера и њихових потреба

Стејкхолдери	Потребе стејкхолдера	Одговорност	Транспарентност	Етичко понашање	Економска добит	Безбедност и здравље	Квалитет	Животна средина	Сигурност посла
Власник					X				
Запослени						X			X
Добављачи		X	X	X					
Корисници		X		X			X		
Инвеститори		X	X	X	X		X		
Суседне заједнице				X				X	
Општине		X	X	X	X			X	X
Власти		X	X	X		X		X	

Табела 6 приказује везу између потреба стејкхолдера и постојећих, односно, уведених стандарда. Из табеле се може приметити да управљање свим потребама стејкхолдера може представљати изазов. Зато би требало, након идентификације стејкхолдера и њихових потреба, истима дати приоритет, након чега треба искористити постојеће стандарде и смернице да се изгради IMS.

Табела 6. Веза између потреба стејкхолдера и релевантних стандарда

Потребе	Стандарди и упутства	ISO 9001:2015	ISO/IEC 27001:2013	ISO 26000:2010
Одговорност				X
Транспарентност			X	X
Етичко понашање				X
Економска добит				
Здравље и безбедност		X		X
Квалитет		X		
Животна средина				X
Сигурност посла				X

У следећој табели (Табела 7) дата је веза захтева између стандарда ISO 9001:2015 и стандарда ISO/IEC 27001:2013.

Табела 7. Веза између захтева стандарда ISO 9001:2015 и стандарда ISO/IEC 27001:2013

ISO 9001:2015	ISO 27001:2013
1. Предмет и подручје примене	1. Предмет и подручје примене
2. Нормативне референце	2. Нормативне референце
3. Термини и дефиниције	3. Термини и дефиниције
4. Контекст организације 4.1 Разумевање организације и њеног контекста 4.2 Разумевање потреба и очекивања заинтересованих страна 4.3 Утврђивање предмета и подручја примене система менаџмента квалитетом 4.4 Систем менаџмента квалитетом и његови процеси	4. Контекст организације 4.1 Разумевање организације и њеног контекста 4.2 Разумевање потреба и очекивања заинтересованих страна 4.3 Утврђивање предмета и подручја примене система менаџмента сигурношћу информација 4.4 Систем менаџмента сигурношћу информација
5. Liderство 5.1 Liderство и посвећеност	5. Liderство 5.1 Liderство и посвећеност

5.2 Политика 5.3 Организационе улоге, одговорности и овлашћења	5.2 Политика 5.3 Организационе улоге, одговорности и овлашћења
6. Планирање 6.1 Мере које се односе на ризике и прилике 6.2 Циљеви квалитета и планирање за њихово остваривање 6.3 Планирање промена 7. Подршка 7.1 Ресурси 7.2 Компетентност 7.3 Свест 7.4 Комуницирање 7.5 Документоване информације	6. Планирање 6.1 Мере које се односе на ризике и прилике 6.2 Циљеви сигурности информација и планирање за њихово остваривање 7. Подршка 7.1 Ресурси 7.2 Компетентност 7.3 Свест 7.4 Комуницирање 7.5 Документоване информације
8. Функционисање 8.1 Планирање и управљање функционисањем 8.2 Захтеви за производе и услуге 8.3 Пројектовање и развој производа и услуга 8.4 Управљање екстерно набављеним процесима, производима и услугама 8.5 Производња и пружање услуге 8.6 Пуштање производа и услуга 8.7 Управљање неусаглашеним излазним елементима 9. Вредновање перформанси 9.1 Праћење, мерење, анализа и вредновање 9.2 Интерна провера 9.3 Преиспитивање од стране руководства	8. Функционисање 8.1 Планирање и управљање функционисањем 9. Вредновање перформанси 9.1 Праћење, мерење, анализа и вредновање 9.2 Интерна провера 9.3 Преиспитивање од стране руководства
10. Побољшавање 10.1 Опште 10.2 Неусаглашености и корективне мере 10.3 Стално побољшавање	10. Побољшавање 10.1 Неусаглашености и корективне мере 10.2 Стално побољшавање

Приступ интеграцији је описан у табели. Након тога, требало би проучити примену овог система преко различитих процеса, целе организације и мреже снабдевања. Затим, треба пратити резултате помоћу индикатора који би упоредили стварне излазе из процеса са жељеним исходима. Жељени исходи би свакако обухватили задовољство стејкхолдера. Побољшавање система би се онда спровело праћењем индикатора и њиховог развоја током одређеног периода, након чега би се одлучило које измене треба увести.

6.3 Приказ мапе и метрике свих процеса и приказ интеракција између процеса

ИР успоставља, документује, примењује и одржава QMS и побољшава његову ефективност у складу са захтевима стандарда SRPS ISO 9001:2008, кроз документа QMS (DQMS), неговањем добре праксе и сталном оријентацијом ка купцима.

Ради повећања задовољења захтева купаца/корисника и побољшања управљања, примењује се процесни приступ. Активност која користи ресурсе и којом се обавља менаџмент да би се трансформисали улазни елементи у излазне, сматра се процесом (ознака "P").

Процеси су дефинисани у Пословнику, разрађени су у процедурама QMS, у којима је приказан стандардни поступак одвијања процеса, идентификовани су њихови “власници”, улази и излази и одговорност осталих учесника.

За пословање ИР, идентификоване су три групе процеса (P) са аспекта QMS-а:

- Менаџмент,
- Основни процеси и
- Процеси подршке (помоћни процеси).

Менаџмент процеси (P1) подразумевају све активности у погледу управљања, руковођења и планирања, анализе ризика, а у циљу функционисања и развоја друштва.

Основни процеси (главни процеси) представљају примарне процесе који директно утичу на захтеве купаца/корисника и одржавају (осликавају) делатност организације (друштва).

Процеси подршке (подржавајући процеси) подразумевају процесе који имају утицаја на перформансе (карактеристике) главних процеса и који су њихова подршка у извршењу својих функција и циљева.

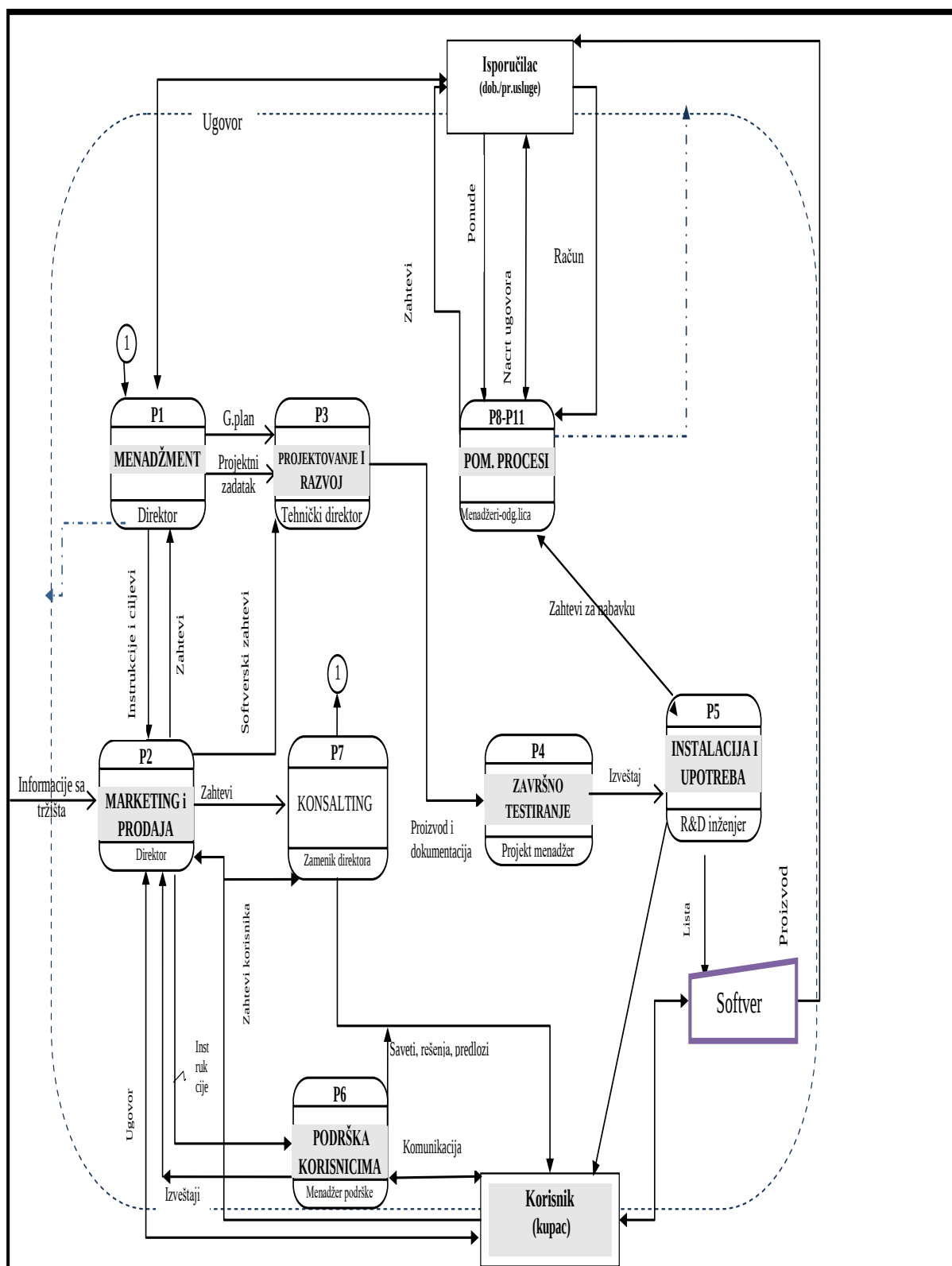
Аутсорс процес је завршно тестирање.

Процесе које примењују ИР, а који су неопходни за QMS, односно реализацију делатности, приказани су на слици 8 (мапа/мрежа процеса).

Мрежом процеса приказан је редослед и међусобно деловање процеса. Међусобно деловање процеса представља се преко производа процеса, који су излаз из једног а улаз у други/наредни процес.

У зависности од комплексности процес се структурира на подпроцесе, а они даље на активности. Процес се графички приказује заобљеним "троделним" правугаоником. У првом делу уписује се ознака процеса, у средишњем назив процеса и на крају одговорни субјект за реализацију процеса.

Процедурама се прописују следећа одређења процеса: важније информације о процесу, ток и извршење процеса, дијаграм тока (за комплексније процесе) и мерење/надгледање (праћење) процеса (важније карактеристике процеса, мерење и праћење карактеристика, оцењивање учинка процеса).



Слика 8 – Мапа свих процеса у предузећу „Интрanea решења“ (Пословник о квалитету ИР)

Праћење и мерење перформанси (важнијих карактеристика) процеса одвија се у складу са одређењима регулативе процеса (процедура).

На састанцима запослених утврђују се карактеристике процеса битне за њихово оцењивање. Користи се запис – Извештај о остваривању/оцењивању циљева квалитета.

Учесталост и одговорност за оцењивање карактеристика процеса дефинише се у процедурама које описују те процесе.

Власник процеса управља процесом, тако да одржава вредност параметара процеса у дозвољеним границама око циљне вредности и по потреби предузима одговарајуће корективне мере.

На основу процедура и планираних циљева квалитета, примењују се одговарајуће методе за праћење и мерење перформанси процеса QMS–а.

Директор врши стално праћење реализације продаје, преиспитује остварење плана и доноси одговарајуће мере.

Један од елемената за мерење успешности функционисања система менаџмента и пословања је и праћење информација од стране купаца/корисника о томе да ли је ИП испунио њихова очекивања.

Извори информација су:

- проблеми/жалбе (тежња ка смањењу),
- подаци добијени директном комуникацијом са купцима (корисницима),
- повратне информације од корисника (позитивне),
- анкетни упитник (IP.02),
- информације од купаца (путем имејла),
- подаци и информације од организације потрошача,
- налази инспекције.

Други извори информација јесу интерне провере, које се спроводе као редовне и као ванредне. Редовне интерне провере, изводе се према Запису – Годишњи план редовних интерних провера. Ванредне провере покрећу се у случају настанка посебних околности, нпр: услед учесталих приговора купаца, корисника услуга, промене у унутрашњој организацији, проблеми у раду и функционисању QMS-а, сертификација/ресертификација итд.

6.4 Преглед одабраних процеса и захтева стандарда који се на њих односе

У наредном делу, у Табели 8 дат је преглед процеса заједно са захтевима стандарда који се на њих односе.

Табела 8. Преглед одабраних процеса и захтева стандарда који се на њих односе

ISO 9001:2015	ISO 27001:2013	Маркетинг и продаја	Пројектовање и развој
1. Предмет и подручје примене	1. Предмет и подручје примене		
2. Нормативне референце	2. Нормативне референце		
3. Термини и дефиниције	3. Термини и дефиниције		
4. Контекст организације	4. Контекст организације	X	X
4.1 Разумевање организације и њеног контекста	4.1 Разумевање организације и њеног контекста	X	X
4.2 Разумевање потреба и очекивања заинтересованих страна	4.2 Разумевање потреба и очекивања заинтересованих страна	X	X
4.3 Утврђивање предмета и подручја примене система менаџмента квалитетом	4.3 Утврђивање предмета и подручја примене система менаџмента сигурношћу информација		
4.4 Систем менаџмента квалитетом и његови процеси	4.4 Систем менаџмента сигурношћу информација		
5. Liderство	5. Liderство		
5.1 Liderство и посвећеност	5.1 Liderство и посвећеност		
5.2 Политика	5.2 Политика		
5.3 Организационе улоге, одговорности и овлашћења	5.3 Организационе улоге, одговорности и овлашћења	X	X
6. Планирање	6. Планирање	X	X
6.1 Мере које се односе на ризике и прилике	6.1 Мере које се односе на ризике и прилике	X	X
6.2 Циљеви квалитета и планирање за њихово остваривање	6.2 Циљеви сигурности информација и планирање за њихово остваривање	X	X
6.3 Планирање промена		X	X
7. Подршка	7. Подршка		
7.1 Ресурси	7.1 Ресурси	X	X

7.2 Компетентност	7.2 Компетентност		
7.3 Свест	7.3 Свест		
7.4 Комуницирање	7.4 Комуницирање	X	
7.5 Документоване информације	7.5 Документоване информације		
8. Функционисање	8. Функционисање	X	X
8.1 Планирање и управљање функционисањем	8.1 Планирање и управљање функционисањем		
8.2 Захтеви за производе и услуге		X	X
8.3 Пројектовање и развој производа и услуга			X
8.4 Управљање екстерно набављеним процесима, производима и услугама			X
8.5 Производња и пружање услуге			
8.6 Пуштање производа и услуга			
8.7 Управљање неусаглашеним излазним елементима			
9. Вредновање перформанси	9. Вредновање перформанси	X	X
9.1 Праћење, мерење, анализа и вредновање	9.1 Праћење, мерење, анализа и вредновање	X	X
9.2 Интерна провера	9.2 Интерна провера	X	X
9.3 Преиспитивање од стране руководства	9.3 Преиспитивање од стране руководства	X	X
10. Побољшавање	10. Побољшавање	X	X
10.1 Опште			
10.2 Неусаглашености и корективне мере	10.1 Неусаглашености и корективне мере	X	X
10.3 Стално побољшавање	10.2 Стално побољшавање	X	X

6.5 Маркетинг и продаја

У овом процесу који обухвата активности са купцима и крајњим корисницима, циљ је утврђивање, преиспитивање и задовољење њихових потреба, као и праћење оствареног задовољења корисника (купца).

Преписке, интеракције и комуникација са корисницима остварују се ради:

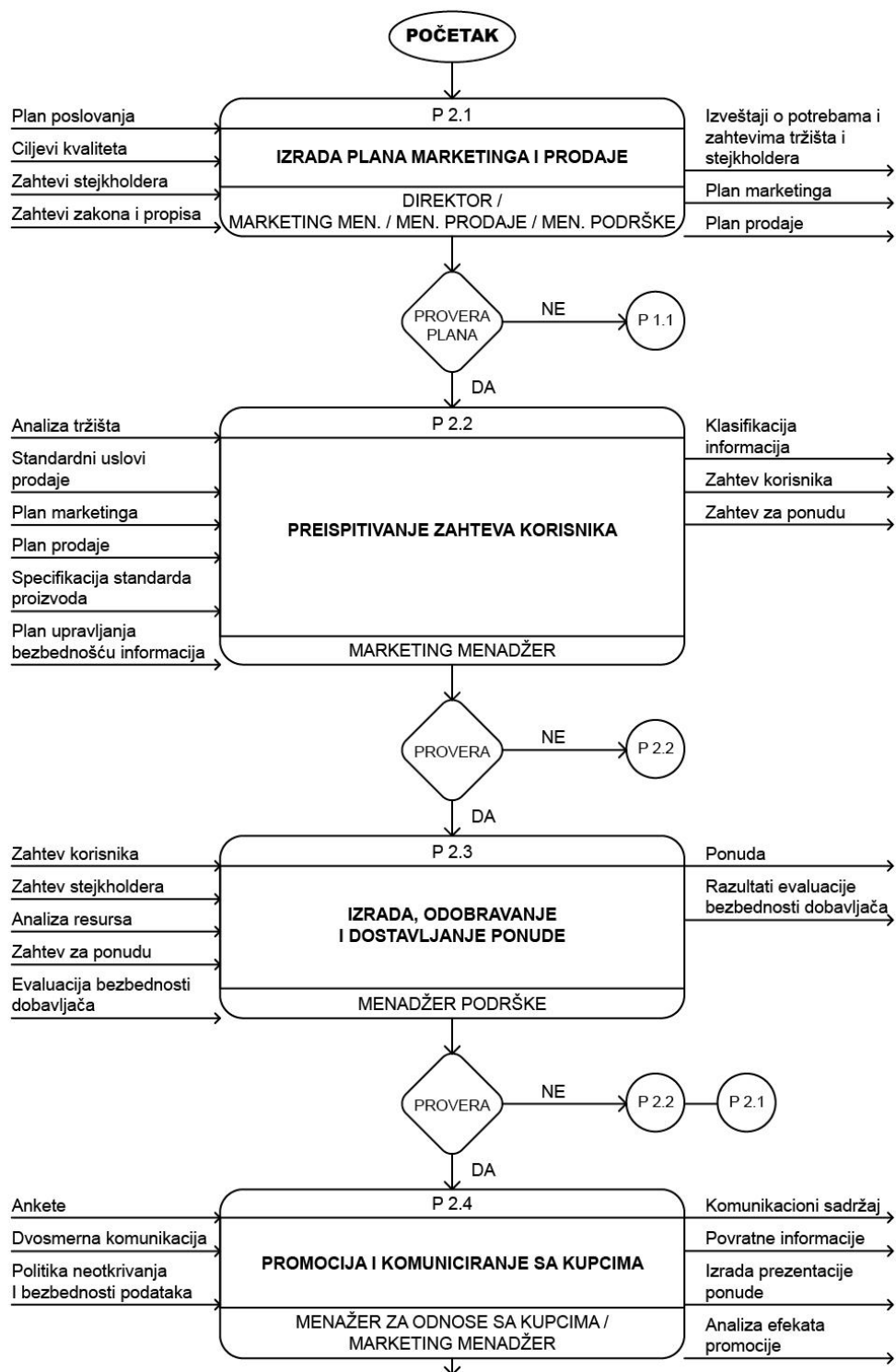
- утврђивања захтева и презентација понуда,
- реализације захтева/уговора и
- утврђивања нових захтева после реализације производа (процеси подршке купцима).

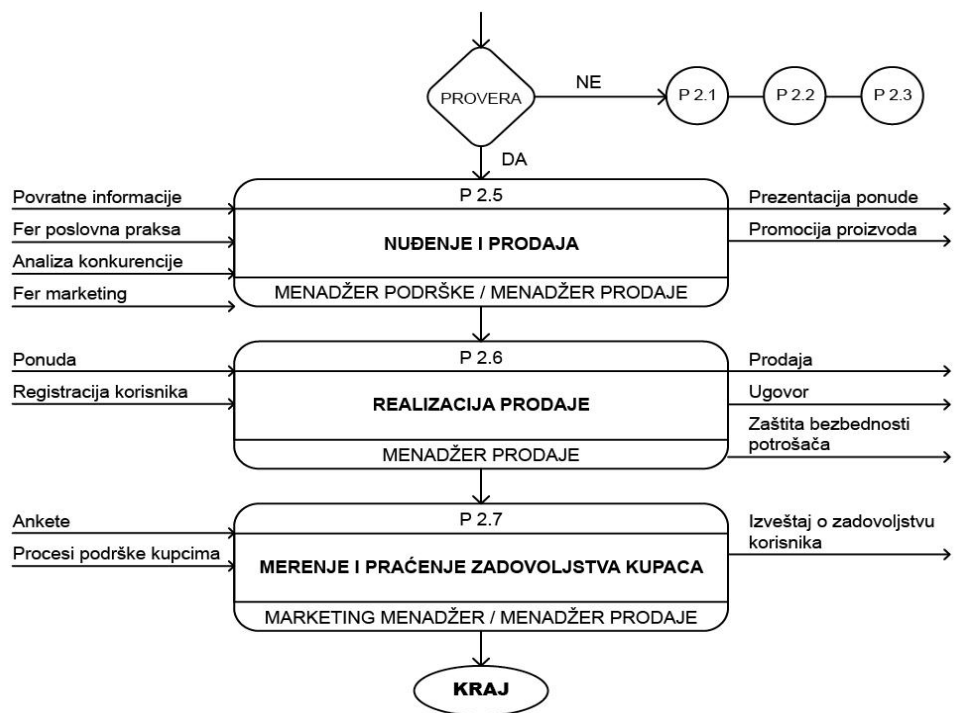
Циљ екстерног комуницирања је прикупљање свих релевантних информација које могу допринети подизању нивоа квалитета и задовољења купца и преношење свих оних информација на купце које су битне за њихово разумевање понуда и поступање са производима који им се нуде.

Кроз истраживање и анализу маркетинг менаџер даје идеје везане за промене апликације, истражује недостатке код купаца, захтеве код потенцијалних купаца, врши и праћење рада код корисника.

Када се формира нова верзија апликације, менаџер продаје, координира да сви постојећи клијенти добију документацију и информације о променама.

На слици 9 приказана је мапа процеса.





Слика 9 – Мапа процеса Маркетинг и продаја (извор: аутор)

6.5.1 Мерење и праћење процеса

У табели 9 приказане су карактеристике Р2 – Маркетинг и продаја. Подаци за К1 се добијају из Анкета-Извештаја, за К2 проценом реализације плана маркетинга, за К3 проценом реализације плана продаје, за К4 из књиговодствене документације, за К5 на основу листе захтеваних и имплементираних безбедносних технологија. Интервал мерења је на “пословном” годишњем нивоу (одговоран: маркетинг менаџер).

Табела 9. Метрика процеса Р2 – Маркетинг и продаја

К1 Задовољство корисника / купца	К2 (%) Реализација плана маркетинга	К3 (%) Реализација плана продаје	К4 (%) Трошкови маркетинга у односу на приход	К5 (%) Ниво безбедносних технологија	□ Карактеристике квалитета
10	>95	>95	< 0,5	>95	10
9	85-95	85-95	0,5 – 0,8	85-95	9
8	75-85	75-85	0,8 -1,0	75-85	8
7	65-75	65-75	1,0 – 1,2	65-75	7
6	60-65	60-65	1,2 – 1,4	60-65	6
5	55-60	55-60	1,4 – 1,6	55-60	5
4	50-55	50-55	1,6 – 2,0	50-55	4
3	40-50	40-50	2,0 – 2,5	40-50	3
2	30-40	30-40	2,5 – 3,0	30-40	2
1	30<	30<	> 3	30<	1
0,2	0,2	0,2	0,2	0,2	ponder

1,6	1,4	1,6	1,2	1,4	вредност
					7,2
					укупна вредност

6.6 Пројектовање и развој

Процедуром IP.03 приказују се пројектовање и развој. Документом се прописује планирање кључних активности у процесу пројектовања и развоја, начин припреме полазних елемената за пројекат, излази из процеса, верификационе и валидационе активности у процесу развоја и начин вршења измена у пројекту развоја апликативних компоненти (софтвера DataStation).

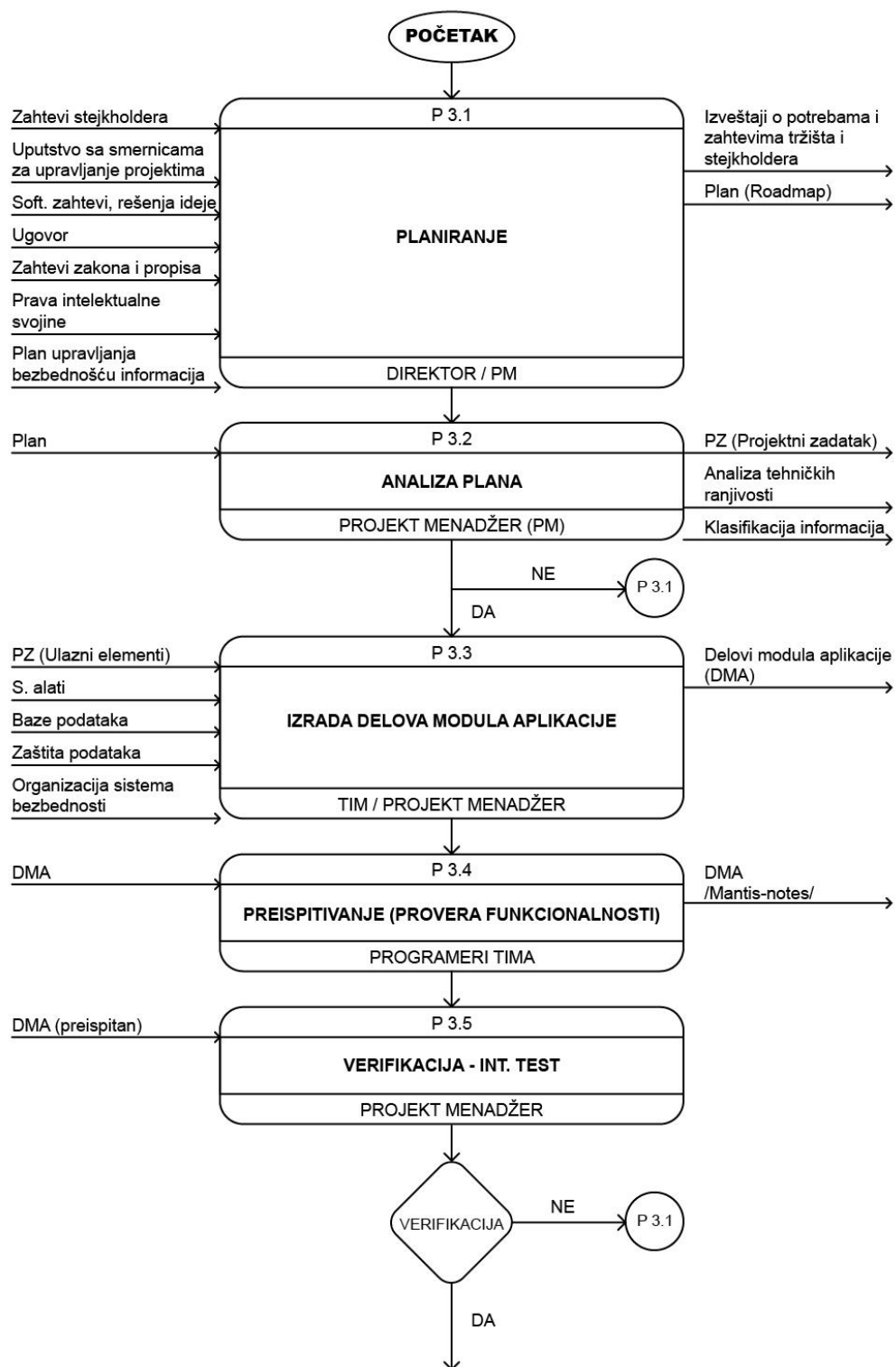
У одговарајућим фазама развоја обавља се систематско преиспитивање (после извршења задатка), верификација (после провере од стране програмера) и валидација (након интеграције).

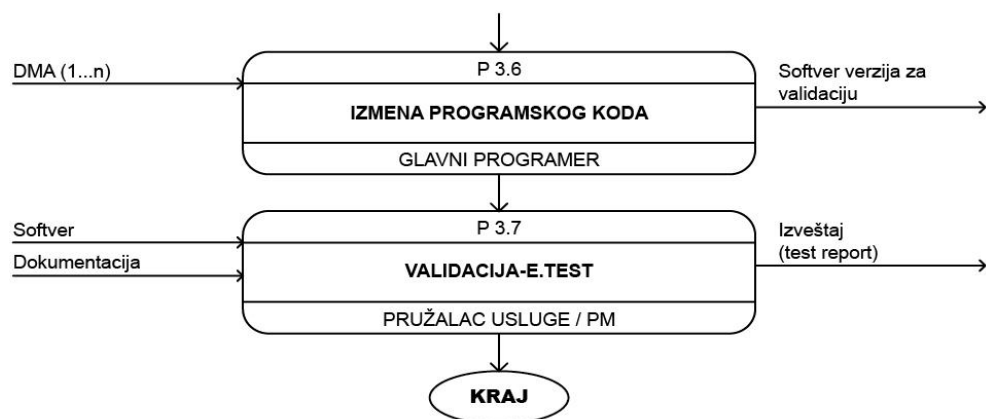
Валидације се спроводи према IP.04 – Завршно тестирање.

Провера исправности апликације, односно тестирање грешака и испитивања софтвера, се могу сматрати успешним када се прође кроз следеће активности:

- Тестирање софтвера - симулација
- Начин провере (структурни и функционални)
- Тестирање перформанси– укључује *stress*, *volume*, сигурност, *timing* и *recovery*
- Провера исправности, интегралности и функционалности
- Тест прихватљивостиса аспекта безбедности.

На слици 10 приказана је мапа процеса.





Слика 10 – Мапа процеса Пројектовање и развој (извор: аутор)

6.6.1 Мерење и праћење процеса

У табели 10 приказане су карактеристике РЗ – Пројектовање и развој. Подаци за К1 се добијају из *Mantis* апликације – test report, за К2 из *Mantis* апликације – roadmap, за К3 из *Mantis* апликације – Управљање и праћење, за К4 на основу листе захтеваних и имплементираних безбедносних технологија. Интервал мерења је на “пословном” годишњем нивоу (одговоран: технички директор).

Табела 10. Метрика процеса РЗ – Пројектовање и развој

К1 (%) Проценат побољшања по пројекту	К2 Нереализовани задаци у року (кашњење реализације)	К3 (%) Ефективност пројекта (однос:планирано/утрошено време)	К4 (%) Ниво безбедносних технологија	□ Карактеристике квалитета
>95	10	100	>95	7
85-95	11-15	90-80	85-95	6
75-85	16-18	80-70	75-85	5
65-75	19-20	70-60	65-75	4.5
60-65	21-25	60-50	60-65	4
55-60	26-30	50-40	55-60	3.5
50-55	31-40	40-30	50-55	3
40-50	41-50	30-20	40-50	2.5
30-40	51-55	20-10	30-40	2
30<	>55	<10	30<	1

0,3	0,2	0,2	0,3	ponder
-----	-----	-----	-----	--------

1,5	1,2	1,4	2,1	вредност
				6,2
				укупна вредност

6.7 Процедура за процес Маркетинг и продаја

- **Сврха**

Овом процедуром дефинишу се процеси маркетинга и продаје у циљу продаје апликативних компоненти (софтвера DataStation) и пружања услуга.

- **Одговорност за примену**

Примарну одговорност за примену овог документа има маркетинг менаџер, а затим и директор, менаџер продаје и менаџер подршке.

- **Термини, дефиниције и скраћенице**

Купац. Као корисник из стандарда ISO 9001:2008, је прималац производа од стране ИР.

Захтев купца (упит купца). Писани документ којим купац дефинише предмет и услове будућег уговора тј. договореног посла.

Промоција (пропаганда). Давање довољних информација и емоција купцу/кориснику како би донео одлуку о куповини производа или коришћењу услуга.

Задовољење корисника (купца). Мишљење корисника о степену до којег су испуњени његови захтеви и очекивања.

Истраживање тржишта. Системски процес прикупљања, анализе и интерпретације релевантних информација, неопходних у процесу доношења одлука.

Софтвер. DS – DataStation (намењен за Иновирање и пласман производа)

Апликације (сегменти софтвера) – Управљање идејама – Idea station, Развој/иновирање нових производа и услуга – Launch station, Праћење тржишног пословања – Market station.

ИР. Интранеа Решења доо.

- **Опис процеса**

Важније информације о процесу

Назив процеса: Маркетинг и продаја – P2

Основни процес који се структурира на подпроцесе:

1. израда плана маркетинга и продаје
2. преиспитивање захтева корисника,
3. израда, одобравање и достављање понуде,
4. промоција и комуницирање са купцима
5. нуђење и продаја
6. реализација продаје
7. мерење и праћење задовољства купца/корисника.

Веза са претходним и наредним процесима: Процесу претходи процес менаџмента, а следе процеси: развоја, подршке и консалтинга.

- **Израда плана маркетинга и продаје**

План маркетинга и план продаје са финансијског аспекта јесу компонентни планови Плана пословања друштва.

Директор ИР (друштва) врши глобално планирање маркетинга на годишњем нивоу.

План маркетинга обухвата промотивно-пропагандне активности, истраживање и анализу. За планирање надлежан је директор. План се ради у оквиру документа план маркетиншких активности. При изради плана директору оперативно помажу маркетинг менаџер, менаџер продаје и менаџер подршке.

План маркетинга се формира до краја текуће за наредну годину.

Оперативне планове маркетинга, на бази годишњег плана, анализе ефеката, одлуке директора, конкретних кампања израђује маркетинг менаџер.

При формирању годишњег плана активности промоције уносе се у плавој боји, а истраживања у зеленој боји.

План маркетинга се састоји од следећих елемената:

- Назив активности/метод (начин истраживања или метода промоције)
- Циља/Циљно тржиште (купце),
- Место реализације активности,
- Период реализације активности,
- Планирани буџет,

- Одговорности за истраживање/промоцију и
- Подацима о реализацији са образложењем ако нешто није реализовано, као и о ефектима.

План продаје представља планску одлуку предузећа о томе колико софтверских производа жели да прода, у ком временском периоду на одређеном тржишту.

- **Преиспитивање захтева корисника**

Циљ комуникација са купцима и крајњим корисницима је утврђивање и задовољење њихових потреба, као и праћење оствареног задовољења корисника (купца).

Комуникације са корисницима остварује се у фази:

- утврђивања захтева и презентација понуда,
- реализације захтева/уговора и
- после реализације захтева (процеси подршке купцима).

Комуникације са купцима спадају у групу екстерних комуникација.

Циљ екстерног комуницирања је прикупљање свих релевантних информација које могу допринети подизању нивоа квалитета и задовољења купца и преношење свих оних информација на купце које су битне за њихово разумевање понуда и поступање са производима који им се нуде.

Комуникације запослених са корисницима мора бити двосмерно, како би се у обезбеђењу квалитетних производа који се нуде/продају купцима остварио циљ да производи ни на који начин не могу да изазову њихово незадовољство.

- **Израда, одобравање и достављање понуде**

Овај подпроцес обухвата:

- Класично истраживање,
- Утврђивање и преиспитивање захтева са тржишта,
- Израду статистике,
- Анализу ефеката промоције/резултата,
- Анализу конкуренције,
- Евалуацију безбедности добављача.

Учесници у реализацији промотивно-пропагандних активности у обавези су да после њихове реализације изврше анализу са свим позитивним и негативним показатељима. Анализом се мора указати на ефекте реализоване активности и на оцену саме промотивно-пропагандне активности.

У начелу анализа се ради у слободној форми и доставља директору. Уколико директор сматра довољним, анализа му може бити саопштена и усмено. Резултати анализе морају укратко бити забележени и у плану промотивно-пропагандних активности.

На глобалном нивоу, користећи *google* аналитику и податке о посећености странице (“свест” о бренду), број захтеваних демо-а, број повратних информација, број потенцијалних купаца (контаката), менаџер маркетинга формира/ажурира: Статистику ефеката промоције.

На основу овог документа директор доноси одлуку о неопходним мерама и даје инструкције за оперативне планове маркетинга.

Кроз ове активности маркетинг менаџер и даје идеје за променама апликације, истражује недостатке код купаца, захтеве код потенцијалних купаца, врши и праћење рада код корисника.

Када се формира нова верзија апликације, менаџер продаје, координира да сви постојећи клијенти добију документацију и информације о променама.

У оквиру евалуације безбедности добављача, циљ је проверити контроле које се односе на заштиту података које користи добављач. Зависно од типа сарадње, од добављача се може захтевати следеће:

- Добављач мора имати Политику о безбедности информација која је у складу са одговарајућим стандардима, законима и прописима.
- Улоге и одговорности које се тичу информационе безбедности морају бити јасно дефинисане.
- Добављач мора потписати Уговор о неоткривању података пре него што добије приступ релевантним информацијама из предузећа.
- Добављач мора бити информисан о класификацији битних информација и мора да користи одговарајуће процедуре за њихову класификацију.

- Сви запослени, радници под уговором на одређено време, и треће стране морају бити подвргнути проверама које су у складу са законом како би се утврдило да су погодни за посао.
- Добављач мора имати успостављену контролу приступа, како би се спречили неodobrenи приступи, нежељена откривања, модификације или брисање података.
- Физичка контрола приступа и безбедност локација мора бити обезбеђена.
- Администратори система морају имати адекватну обуку како би одржавали сигурну мрежну инфраструктуру.
- **Промоција и комуницирање са купцима**

Врсте промоције

Друштво реализује две врсте промоције, тј. канале дистрибуције: онлајн маркетинг и офлајн – класична промоција.

Врсте онлајн маркетинга су:

I – Бренднинг оглашавање (на разним другим странама, комерцијално-промотивне природе),

II – Контекстуално оглашавање (II.1 Преко кључних речи: нпр. Идеја, иновација; преко претраживача или вести, II.2 “Бесплатно” оглашавање – оптимизација претраживача),

III – Имејл маркетинг (инфовести путем истраживања и промоције, са циљем информисања о бенефитима и информисања о погодности употребе),

IV – SMM (маркетинг преко друштвених мрежа) и Вирални маркетинг,

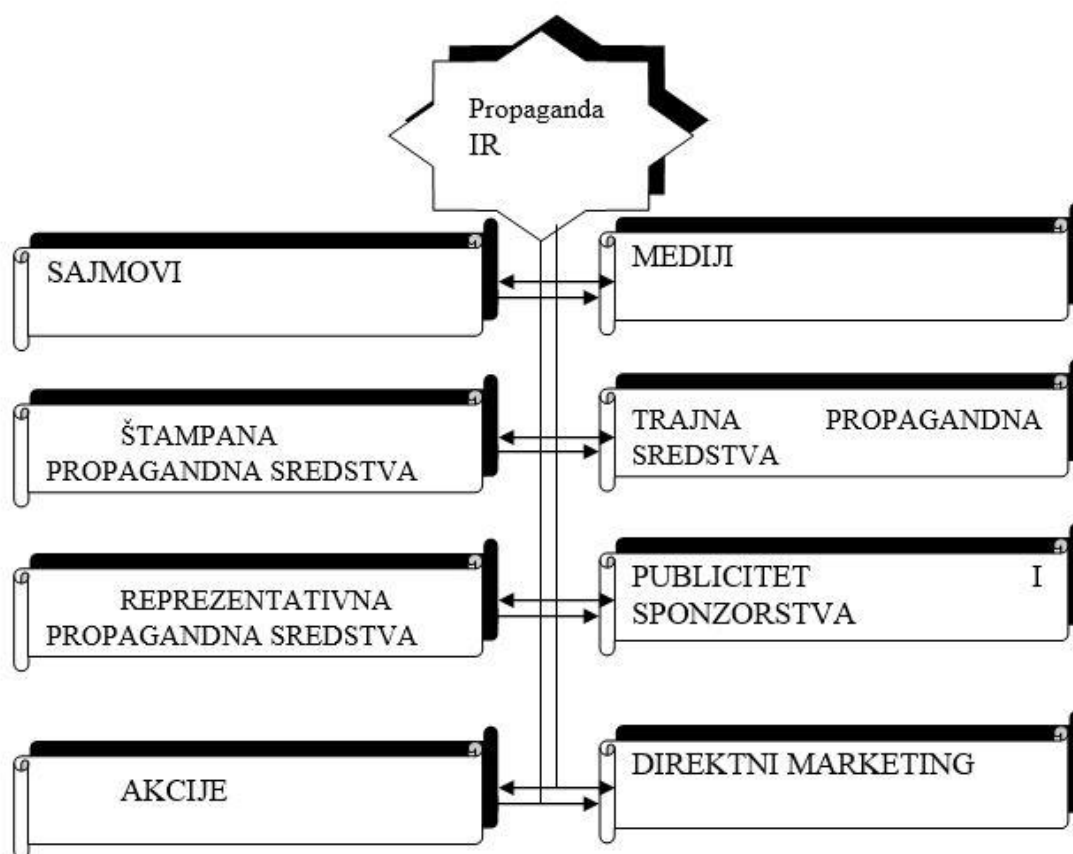
V – RIM (повратни маркетинг),

VI – Праћење рекламе.

Методе и средства “класичне” промоције дата су на слици 11. То су:

- Сајмови (Домаћи сајмови, Међународни сајмови),
- Масовни медији (Оглашавање, ТВ спот),
- Штампана пропагандна средства (Проспекти, Постери, Фасцикле),

- Трајна пропагандна средства (Светлеће рекламе, Спецификације производа, ЦД),
- Публицитет и спонзорства,
- Репрезентативна пропагандна средства (Ситни предмети пажње, Ексклузивни предмети пажње),
- Акције,
- Директни маркетинг (преко посредника).



Слика 11 – Промотивне активности (извор:Процедура Маркетинг и продаја, ИР)

• Реализација промотивно-пропагандних активности

За реализацију промотивно-пропагандних активности одговорно је лице (или лица) одређено планом. Пре реализације активности, одговорно лице обавезно је да изврши адекватну припрему. Основни елемент припремних активности је разрада акционог програма за конкретну промотивно-пропагандну активност.

Разрадом програма морају бити обухваћене све потребне активности и ресурси (материјални, финансијски, људски и временски) како би се остварили постављени

циљеви. Разрада програма се ради у пригодној форми за дату промотивно-пропагандну активност.

У току реализације промотивно-пропагандних активности мора се водити евиденција о свим запажањима која су битна за остварење циљева и доношење пословних одлука. За ово је одговорно лице које је задужено за те активности, и сви други који у томе учествују. Запажања се евидентирају у радним бележницама учесника.

Промотивно-пропагандне активности служе, између осталог, и за прикупљање информација о потребама тржишта па такве информације такође треба забележити. Ове информације постају елемент истраживања тржишта.

За уређење и ажурирање вебсајта (www.datastation.com) одговоран је маркетинг менаџер. Инструкције добија од и од директора и менаџера подршке.

- **Нуђење и продаја**

За ентитет демо, потенцијални корисник се пријављује електронским путем или директним контактом. Менаџер подршке позива заинтересовано лице, нуди „прилагодљиву“ демо верзију том клијенту.

Када се из претходне активности, и из процеса истраживања и промоције, створи захтев за понуду, купац се упућује на менаџера продаје, који формира понуду и нуди промоцију електронским путем. Уколико је корисник заинтересован договара термин и опсег презентације.

Након тога формира се понуда и иста доставља потенцијалном клијенту. Понуда садржи: корисничку лиценцу (структура понуде, цена), цену имплементације, цену подршке и предности коришћења софтвера DS.

Ценовник, односно, цене одређује директор, сагледавајући тржишне сегменте, број запослених/број корисника код купца, обим подршке.

Када се купац сагласи са понудом, формира се уговор (одговоран директор). Предложени уговор је „моделског типа“, где се анексима дефинишу врсте апликација, број корисника и обим подршке (одговоран менаџер продаје).

Уговор се формира у 4 примерка (по два за уговорну страну). Примерци у ИР: један у архиви уговора (одлаже технички секретар), други код књиговође.

- **Реализација продаје**

Приликом регистрације нових корисника, одговорно лице мора бити упознато са својим одговорностима и са документом Упутство за заштиту личних података. Контрола приступа подацима мора бити јасно дефинисана. Сваки корисник приликом регистрације мора да прихвати Политику приватности и Политику безбедности информација.

Пре потписивања уговора, корисник мора потписати Уговор о неоткривању података.

- **Мерење и праћење задовољства купаца/корисника**

Један од елемената за мерење успешности функционисања система менаџмента и друштва је и праћење информација од стране купаца/корисника о томе да ли је ИР испунио њихова очекивања.

Извори информација су:

- рекламације/жалбе (тежња ка непостојању жалби),
- подаци добијени директном комуникацијом са купцима (позитиван контекст),
- повратне информације од купаца (позитивне),
- анкетни листићи
- информације од корисника (путем имејла),
- подаци и информације од подршке.

Слање анкета, пријем и обрада обавеза је ADQ.

Одређивање термина (периода) анкетирања у надлежности је PQ (мин једном годишње).

Администратор QMS-а врши статистичку обраду кроз – Извештај о задовољству купаца, за који доставља представнику руководства (PQ), за потребе преиспитивања од стране руководства, и директору. Прописивање мера је од стране директора и PQ.

Рекламације/примедбе решавају се кроз процес подршке и поступак управљања неусаглашеностима, корективне и превентивне мере.

6.8 Процедура за процес Пројектовање и развој

- **Сврха**

Предмет ове процедуре је пројектовање и развој, којом се прописује планирање кључних активности у процесу пројектовања и развоја, начин припреме полазних елемената за пројекат, излази из процеса, верификационе и валидационе активности у процесу развоја и начин вршења измена у пројекту развоја апликативних компоненти (софтвера DataStation).

- **Одговорност за примену**

Процедура је намењена пројектном тиму као смерница код спровођења активности при пројектовању и развоју апликативних компоненти софтвера. Примарну одговорност за примену овог документа има технички директор.

- **Термини, дефиниције и скраћенице**

Пројектовање и развој. Скуп процеса који претвара захтеве у специфициране карактеристике или у спецификације производа (нпр. апликације софтвера), процеса или система.

НАПОМЕНА 1 Термини "пројектовање" и "развој" понекад се користе као синоними, а понекад се користе за дефинисање различитих фаза укупног процеса пројектовања и развоја.

НАПОМЕНА 2 Да би се указало на природу онога шта се пројектује и развија, може се користити атрибут (на пример: пројектовање и развој производа или пројектовање и развој процеса).

Преиспитивање пројекта и развоја. Активност која се предузима да би се утврдила погодност, адекватност и ефективност пројекта за постизање постављених циљева.

Напомена: Преиспитивање се обавља да би се:

- а) вредновала могућност резултата пројектовања и развоја да испуњавају захтеве и
- б) идентификовали сви проблеми и предложили мере неопходне за њихово решавање.

Верификација. Потврђивање пружањем објективног доказа да су испуњени специфицирани захтеви (како би се обезбедило да излазни елементи пројектовања и развоја испуњавају улазне елементе)

Напомена: Термин "верификован" се користи да означи одговарајући статус.

Валидација. Потврђивање пружањем објективног доказа да су испуњени захтеви за специфичну предвиђену употребу или примену.

Напомена: Услови за валидацију могу бити стварни или симулирани.

Софтвер. DS – DataStation (намењен за Иновирање и пласман производа)

Апликације (сегменти софтвера) – Управљање идејама – Idea station, Развој/иновирање нових производа и услуга – Launch station, Праћење тржишног пословања – Market station.

ПМ. Пројект менаџер.

ИР. Интранеа Решења доо.

- **Опис процеса**

Важније информације о процесу

Процес РЗ: Пројектовање и развој

Претходе процеси менаџмента и маркетинга, а следи процес завршног тестирања.

Основни процес који се структурира на подпроцесе:

1. Планирање
2. Анализа плана
3. Израда делова модула апликације
4. Преиспитивање
5. Верификација
6. Измена програмског кода
7. Валидација

- **Планирање пројектовања и развоја**

План развоја софтверских апликација проистиче из глобалног плана пословања, идеја, захтева корисника/купаца. Идеје могу настати као резултат: истраживања тржишта, захтева купаца, промена у техничком смислу, измена, идеја од запослених, података добијених кроз подршку купцима/корисницима. Идеје о побољшањима апликација се прикупљају путем платформе, при чему руководиоци праве прву селекцију идеја и списак селектираних идеја достављају директору који врши другу селекцију. Резултат друге селекције је списак (листа) задатака које треба реализовати у наредном периоду (уврштава се у roadmap-у).

План је везан за годишњи квартал („пословни“ ИР). Значи да се четири пута годишње развијају нове верзије апликација (табела 11). Избор апликација, дефинисање задатака, односно формирање плана – roadmap-е спроводе: директор, технички директор, ПМ и менаџер подршке (до 7 дана пре почетка рада на новој верзији).

Табела 11. Периоди развоја апликација (илустрација за 2013. годину)

Фаза	Термини	Завршни тест	Квартал 2013
13.10	15.11.2012.-15.02.2013.	01-15.02.2013.	I
13.20	15.02.2013.-15.05.2013.	01-15.05.2013.	II
13.30	15.05.2013.-15.08.2013.	01-15.08.2013.	III
13.40	15.08.2013.- 15.11.2013	01-15.11.2013.	IV

Roadmap садржи и следеће елементе:

R.број задатка:xxxxxxx – узима се почев од редног броја 0000001, па надаље.

[део апликације] Назив задатка (извршилац-власник процеса), Статус задатака-

Статуси задатака зависе од врсте и фазе завршетка, и могу бити:

- *New* – нови,
- *Feedback* – потребне инструкције,
- *Acknowledged* – потврда пријема задатака
- *Unclear* – нејасно (редефинисање/појашњење)

- *Ready for testing* – спремно за тестирање (верификацију)
- *Needs rework* – потребна дорада,
- *Resolved* – решено (завршено, по верификацији)
- *Closed* – обрисан задатак,

На основу Roadmap-е, пројект менаџер генерише Пројектни задатак. Пројектни задатак садржи: назив, термине, елементе, задатке тима, факторе успеха. У ентитет задаци тима, приоритет додељује пројект менаџер уз консултације са директором. Процену времена дају програмери (запослени у сектору развоја). Нови задатак се додељује у случају: прерасподеле посла, дораде или новог посла. Задатак се у одређеном кварталу може брисати због немогућности завршетка, промене, пролонгирања за наредне фазе.

- **Класификација информација и анализа техничких рањивости у оквиру анализе плана**

Класификација информација треба да постоји у виду инвентара информација који треба да садржи следеће елементе: нивое поверљивости, интегритета и доступности, резултујући ниво критичности, власника и кориснике информације у питању. Овај инвентар мора бити доступан члановима одговарајућег тима за безбедност, као и власницима предузећа и запосленима на нивоу топ менаџмента.

Процедура за идентификовање и анализу техничких рањивости овухвата следеће стадијуме:

- Екстерну процену,
- Интерну процену,
- Процену заштитног зида (*engl. firewall*),
- Процену бежичне конекције,
- Процена социјалног инжењеринга.

При екстерној процени, прво се идентификују рањивости повезане са интернет инфраструктуром и мрежним системима и серверима.

При интерној процени, анализира се интерна мрежна инфраструктура. Тестирање се врши на насумичном узорку од пет рачунара. Циљ активности је да се провери да ли имплементиране безбедносне технологије пружају одговарајући извор заштите.

При процени заштитног зида примарни циљ јесте анализа заштитног зида који је успостављен ради заштите од спољних напада.

Процена бежичних конекција се спроводи на серверима којима је приступ омогућен преко бежичне мреже. Тестирање треба да се обави на једној локацији уз предвиђање могућих тачака приступа у околини локације.

Процена социјалног инжењеринга подразумева анализу контроле приступа информационим системима и сигурносним локацијама. Тестирање ће се спровести у виду покушаја да се омогући приступ безбедним локацијама и заштићеним серверима и мрежама.

Након анализа и процена, администратори система спровode корективне и превентивне мере како би се умањиле техничке рањивости.

- **Израда, измене и праћење задатака**

Израда задатака обухвата писање кода, на основу Интерног стандарда за писање кода, других стандарда и методологија, софтверских алата и програмских језика.

Излаз из „задатка“ је програмски код („промењени“).

Листа праћења задатака је *Mantis* апликација.

Главни елементи-поља *Mantis* апликације: Главни поглед; Мој поглед; Преглед задатака; Пријава задатака; Дневник измена/напредовања, План-роадмап; Кумулативни извештај; Управљање и праћење; Подешавање апликације; Подешавање кроз налоге; Ентитет времена: планирано/утрошено; Излаз. Ентитет статус мојих задатака приказује: р. бр. задатка; део апликације; значајност; статус; последњу измену; време; назив-опис задатка.

Задатак обухвата: израду/писање програмског кода за одређену компоненту или функционалност софтвера.

Програмер израђује и документује свој задатак за спољашњи интерфејс елемената софтвера, интерфејс између компонената софтвера и између софтверских јединица. Детаљан пројекат интерфејса мора да дозволи кодирање не захтевајући даље информације.

Програмер дефинише и документује податке о провери и испитивању софтверских јединица.

Пројект менаџер мора водити рачуна о следљивости захтева за елемент софтвера, конзистентности са архитектуром, конзистентности између компонената софтвера и софтверских јединица, погодности коришћених стандарда и метода у развоју, изводљивост тестирања, изменама, изводљивости експлоатације и одржавања.

Главни програмер је одговоран за интеграцију софтверских компоненти у главну апликацију. Главни програмер анализира израђене софтверске компоненте и проверава да ли су програмиране у складу са архитектуром апликације.

Измене у извршењу задатака тј. развоју, могу се покренути од извршиоца (током рада или преиспитивања); од пројект менаџера (у току рада или при верификацији), од пројект менаџера после валидације. Измене одобрава/прописује ПМ; назнака у *Mantis* апликацији: *needs rework*, боје маслинастозелене. Следи даљи ток као израда задатака.

Организациони облик који се користи је тимска организација, чија је карактеристика да се пројектовање/развој одвија у оквиру тима чији су чланови („програмери“) запослени у сектору развоја. Информације и комуникације теку у правцу: Директор-Руководилац пројекта (пројект менаџер) – тим и обрнуто (путем *Mantis* апликације/*collab* платформа). Технички директор комуницира линијски и бочно. Комуникација је и путем интерних састанка. Белешка о овом састанку уноси се у *Mantis* апликацију – *notes* (одговорни: ПМ или менаџер подршке, у зависности од теме/проблема састанка).

- **Преиспитивање, верификација и валидација**

У одговарајућим фазама развоја обавља се систематско преиспитивање (после извршења задатка), верификација (после провере од стране програмера) и валидација (након интеграције). Главне одреднице ових фаза приказане су у табели 12.

Табела 12. Преиспитивање, верификација и валидација

Активност – опис:	Извршилац (извршиоци)	Елемент	Објективни доказ	Запис
<u>Преиспитивање:</u> Провера од стране програмера. <i>Начин/метод:</i> Провера зависи од конкретног задатка („правила струке“). <i>Циљ:</i> Провера функционалности	Програмери	Задатак – део модула апликације	Поље Mantis апликације–NOTES (Белешка) садржи: време провере и тест за конкретни ентитет	Лист праћења (Mantis)
<u>Верификација:</u> Провера од стране ПМ. Начин/метод: Улазак у DS – на „локацију“ задатка и контролисање <i>Циљ:</i> Провера сагласности са улазним подацима-задатком	Пројект менаџер	Део модула апликације	Поље Mantis апликације–NOTES	Лист праћења (Mantis)
<u>Валидација:</u> Тестирање нове верзије. <i>Начин/метод:</i> Екстерно (пужалац услуге). <i>Циљ:</i> Провера функционалности, интегралности, перформанси и симулација (проба рада)	Пужалац услуга	Апликација	Извештај о тестирању (симулацији) /Test report	Извештај о тестирању (од пужоца услуге)

7. Закључци

У свакој организацији, без обзира на величину и област делатности, присутни су одређени системи менаџмента. Имајући у виду да је скупо пројектовати сваки систем менаџмента појединачно, постаје јасно да је данас неопходно интегрисати све системе менаџмента који су присутни у одређеном предузећу. Можда је то понекад тежак процес јер се односи на поновну конструкцију структуре пословних циљева и стратегије, али интеграција система менаџмента у многим аспектима представља битан корак за предузеће.

Како би интеграција система менаџмента била успешна, потребно је знање о процесима, менаџменту, методама, информационим системима. Интеграција не помаже предузећу само у економском и ресурсном погледу, већ знатно утиче на ефективност и ефикасност производње производа или пружања услуга. Уз помоћ интегрисаних система менаџмента, предузеће има бољу конкурентност на тржишту.

Предузеће „Интранеа решења д.о.о.“ има успостављене интегрисане системе менаџмента (ISO 9001:2008 и ISO/IEC 27001:2013) већ пар година. Та чињеница такође показује да је мото предузећа заиста „идејама до иновативности и унапређења.“ Адекватно управљање сопственим системима менаџмента омогућава предузећу да на прави начин управља идејама и другим аспектима пословања. „Интранеа решења“ константно улаже у унапређење свог пословања јер је циљ овог предузећа да буду успешни на тржишту софтвера за управљање идејама.

Самим тим, препорука за даљи рад и унапређење квалитета пословања била би да се узме у обзир међународни стандард ISO 26000:2010 Упутство о друштвеној одговорности. Треба размотрити могуће начине да ово иновативно предузеће још више допринесе друштву и заједници у којој послује, а дугорочно посматрано, и начине на које се може допринети општој добробити друштва и одрживом развоју.

Литература

1. Arsovski S., i drugi (2013), *Integrirani sistemi menadžmenta*, Univerzitet u Kragujevcu, Fakultet inženjerskih nauka, Centar za kvalitet
2. Asif, M. & de Bruin, E.J. & Fisscher, O.A.M. (2008). *Process embedded design of integrated management systems*. International Journal of Quality & Reliability Management, 25(3): 261-282.
3. Beckers, K., Cote, I., Faßbender, S., Heisel, M. & Hofbauer, S. (2013), "A pattern-based method for establishing a cloud-specific information security management system", Requirements Eng Vol. 18, pp. 343–395
4. Bernardo, M., Casadesus, M., Karapetrovic, S. & Heras, I. (2009). "How integrated are environmental, quality and other standardized management systems? An empirical study" Journal of Cleaner Production 17(8): 742–750
5. Bobrek, M. and Sokovic M. (2006) *Integration concept and Synergetic effect in Modern Management*. Journal of Materials Processing Technology, Volume 175, Issues 1-3, 1 June 2006, Pages 33-39
6. Dalling (2007) "Integrated Management Definition", Chartered Quality Institute Integrated Management Special Interest Group, Issue 2.1
7. Du, S., Bhattacharya, C. B., & Sen, S. (2011). Corporate social responsibility and competitive advantage: overcoming the trust barrier. Management Science, 57(9), 1528–1545.
8. Egyedi, T. and Toffaletti, S. (2008), "Standardising social responsibility: analysing ISO representation issues from an SME perspective", in Jakobs, K. and Soederstroem, E. (Eds), Proceedings 13th EURAS Workshop on Standardisation, Wissenschafts Verlag Mainz, Aachen, pp. 121-136.
9. Funck D. and vonAhsen A. (2001), Integrated management systems - Opportunities and risks for corporate environmental protection. Corporate environmental strategy, vol 8, issue 2, July 2001, pages 165-176
10. Garvare, R & Isaksson, R. (2001). Sustainable Development: Extending the Scope of Business Excellence Models. R. Measuring Business Excellence, 5(3): 11-15.
11. Hansson, J. and Eriksson, H. (2005). "Integrated management systems - theoretical and practical implications" QMOD 2005 "Quality Management for Organizational and Regional Development" 29 June – 1 July 2005. Palermo, Italy

12. Hansson, J. Garvare, R. and Klefsjö, B. (2006). Stakeholder Oriented Integration of Management Systems, ICIT, Proceedings of the 11th International Conference on ISO 9000 & TQM (11-ICIT), Hong Kong, China, 10-12 April, 2006
13. Hauser, J., Tellis, G. J., & Griffin, A. (2006). Research on innovation: a review and agenda for marketing science. *Marketing Science*, 25(6), 687–717.
14. Hemphill, T. (2013), “The ISO 26000 guidance on social responsibility international standard: what are the business governance implications?”, *Corporate Governance*, Vol. 13 No. 3, pp. 305-317.
15. *International Journal of Electronic Commerce*, Vol 9, No.1, Fall 2004, referenced in the 2nd edition of *Information Security Governance : Guidance for Boards of Directors and Executive Management*, published by the IT Governance Institute. Web www.itgi.org
16. ISO 9001:2015 Quality management systems – Requirements
17. ISO 26000:2010 Guidance on social responsibility
18. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
19. ISO Management Systems, “Russian bank improves information security with ISO/IEC 27001”, September – October 2009
20. Jansen, J. J. P., Van Den Bosch, F. A. J., & Volberda, H. W. (2006). Exploratory innovation, exploitative innovation, and performance: effects of organizational antecedents and environmental moderators. *Management Science*, 52(11), 1661–1674.
21. Johnston, A. (2011), “Constructing sustainability through CSR: A critical appraisal of ISO 26000”, Working Paper No. 2011-33, University of Oslo Faculty of Law Research, University of Oslo, Oslo.
22. Jørgensen, T. H. & Remmen, A. & Mellado, M. D. (2006). Integrated management systems – three different levels of integration. *Journal of Cleaner Production*. 14, 713-722.
23. Karapetrovic, S. (2002) Strategies for the integration of management system and standards. *The TQM Magazine*, 14(1): 61-67.
24. Karapetrovic, S. (2003). "Musings on integrated management systems." *Measuring Business Excellence* 7(1): 4-13.

25. Karapetrovic, S. & Casadesús, M. (2009). Implementing environmental with other standardized management systems: Scope, sequence, time and integration. *Journal of Cleaner Production*, 17, 533-540.
26. <http://www.kvalitet.org.rs/standardi/iso-26000>, приступљено 4.11.2016.
27. Luo, X., & Bhattacharya, C. B. (2006). Corporate social responsibility, customer satisfaction, and market value. *Journal of Marketing*, 70, 1–18.
28. Luo, Xueming and Shuili Du. (2014) "Exploring The Relationship Between Corporate Social Responsibility And Firm Innovation". *Marketing Letters* 26.4: 703-714
29. Martínez-Costa, M., Martínez-Lorente, Á.R., (2008) Does quality management foster or hinder innovation? An empirical study of Spanish companies. *Total. Qual. Manag. Bus. Excell.* 19 (3), 209–221.
30. Moratis, L. (2016), "Signaling strategies for ISO 26000: a firm-level approach", *International Journal of Operations & Production Management*, Vol. 36 Iss 5 pp. 512 – 531
31. Perera, O. (2008), *How Material is ISO 26000 Social Responsibility to Small and Medium-Sized Enterprises?*, IISD, Winnipeg.
32. Prilog iz preduzeća – IP.02 Marketing i prodaja, Intranea rešenja, Kragujevac
33. Prilog iz preduzeća – IP.03 Projektovanje i razvoj, Intranea rešenja, Kragujevac
34. Prilog iz preduzeća – Poslovnik o kvalitetu Intranea rešenja, Kragujevac
35. Rasche, A. (2010), "Collaborative governance 2.0", *Corporate Governance*, Vol. 10 No. 4, pp. 500-511.
36. Saveti za mala preduzeća, http://big.co.rs/upload/Edition/Download/2016-05/Saveti_za_mala_preduzeca_Uspesne_price.pdf, приступљено 14.11.2016.
37. Salomone, R. (2007), Integrated management systems; Experiences in Italian organizations. *Journal of cleaner production*.
38. Wilkinson, G. and Dale, B. G. (1999). "Integrated management systems: an examination of the concept and theory." *The TQM Magazine* 11(2): 95-104.
39. Zutshi, A. & Sohal, A.S. (2005). Integrated management system – The experience of three Australian organisations. *Journal of Manufacturing Technology Management*, 16(2): 211-232.