Универзитет у Крагујевцу
Факултет инжењерских наука

Назив студијског програма: Индустријско инжењерство
Ниво студија: Мастер академске студије
Модул: Пословни информациони системи
Предмет: Интегрисани системи менаџмента
Број индекса: 626/2015

Милица С. Фржовић

Развој интегрисаних система менаџмента квалитетом, безбедношћу информација и ризиком у пружању финансијских услуга

Мастер рад

Комисија за преглед и одбрану:

1.Проф. Др Славко Арсовски - Ментор

2. _____

3. _____

Датум одбране:_____

Оцена:_____

У оквиру овог завршног рада кандидат треба да проучи препоручену, домаћу и страну литературу из области интеграције система менаџмента квалитетом, безбедношћу информација и ризиком у пружању финансијских услуга. На основу стеченог знања и прикупљених информација треба да установи све чињенице потребне за одређивање и ближе дефинисање самих процеса квалитета, безбедности информација и ризика ISO стандардизације. Потребно је сагледати како стандарди ISO 9001, ISO 27001 и ISO 31000 утичу на пружање финансијских услуга. Такође, потребно јеприказати и интеграцијустандардана конкретном примеру једне финансијске организације.

Препоручена литература:

[1]Арсовски, С., Мапирање пословних процеса, Машински факултет у Крагујевцу, 2010.

[2] Арсовски, С., Менаџмент процесима, Машински факултет у Крагујевцу, 2007.

[3] Seuring, S., Miler, M., Standardization like support, Journal of Production, 2008.

Крагујевац, 2016. Ментор:

Проф. Др Славко Арсовски

Изјава о самосталној изради рада

Изјављујем да сам овај мастер рад урадио самостално, служећи се стеченим знањем и искуством као и наведеном литературом.

626/2015 Милица С. Фржовић

_____

(потпис)

Резиме рада: У савременим условима пословања, квалитет производа и услуга представља доминантан фактор конкурентности и престижа на светском тржишту.Да би се постигао квалитет у било ком сегменту тржишта, како светског тако и домаћег, неопходна је примена савременог концепта пословања који укључује стандардизацију пословних процеса и успостављање система менаџмента квалитетом.Систем менаџмента квалитетом обухвата све пословне функције и има за циљ стално побољшање свих процеса који утичу на квалитет производа и услуга. Свакако, организација која жели да унапреди своје пословање не може да се задржи само на примени стандарда ISO 9001 – то је тек први корак у процесу континуираног унапређења, аостали кораци су други стандарди попут стандарда ISO/IEC 27001 – Систем менаџмента безбедношћу информацијаи ISO 31000 – Систем менаџмента ризиком. Имплементација ових стандарда у финансијским организацијама даје основ за развој интегрисаног система менаџмента, који представља добар начин за ефективно и ефикасно управљање пословном организацијом.

Кључне речи: квалитет, стандард, интеграција

Apstract: In the modern business environment, quality of products and services is the dominant factor of competitiveness and prestige in the world market. To achieve qualityin any segment of the market, both domestic and global, it is necessary the application of modern business concept that involves the standardization of business processes and establishing quality management systems. The quality management system covers all businessfunctions and aims at continuous improvement of all processes affecting the quality of products and services. Certainly, an organization that wants to improve its business cannot be withheld solely on the implementation of ISO9001 standard - this is only the first step in the process of continuous improvement, and other steps are other standards like ISO/IEC 27001 - Information Security Management System and ISO 31000 - The System of Risk Management.The implementation of these standards in financial organizations provides the basis for the development of integrated management system, which is a good way to effectively and efficiently manage a business organization.

Keywords: quality, standard, integration

Садржај:

1. Уводна разматрања

У савременим условима пословања, постизање високог степена квалитета све више добија на значају због све веће конкурентности на глобалном светском тржишту. Квалитет производа и услуга данас представља доминантан фактор конкурентности и престижа на светском тржишту. Опште је прихваћено мишљење да је у последњих двадесетак година потпуно нов приступ квалитету производа и услуга, суштински највећи домет у глобалном настојању да се унапреди квалитет живота савременог човека.

Да би се постигао квалитет у било ком сегменту тржишта, како светског тако и домаћег, неопходна је примена савременог концепта пословања који укључује стандардизацију пословних процеса и успостављање система менаџмента квалитетом. Систем менаџмента квалитетом обухвата све пословне функције и има за циљ стално побољшање свих процеса који утичу на квалитет производа и услуга.

Базу готово свих актуелних разматрања и конкретних активности у области квалитета производа и услуга, чине објективан и мултидисциплинарни приступ проблематици. Уз то, нова научна сазнања, као и импресиван развој аналитичких метода, инструменталне технике, информационих система и технологија, омогућавају успешну реализацију савремене концепције о интегралности квалитета. Ово омогућава афирмацију нове пословне стратегије о управљању.

Нова филозофија квалитета није једино, мада јесте значајно, изражена самим чином доношења прве серије стандарда ISO9000 за интерно управљање квалитетом и екстерно обезбеђење квалитета, пре двадесет година. Њена афирмација се, пре свега, огледа кроз готово општу прихваћеност и широку променљивост савремене концепције о интегралности квалитета, али и захтева поменутих стандарда (у свим деловима света и у свим областима рада и пословања).

Остварење концепције о интегралности квалитета кроз превентиван и мултидисциплинарни приступ и ефикасну контролу, обавезно подразумева објективно и поуздано испитивање, односно прецизно дефинисање нивоа истражености најважнијих, одабраних и за сваки производ специфичних својстава квалитета.

Серија стандарда ISO9000 је назив за скуп више стандарда који се односе на организационо-управљачке процесе унутар организације која купцима испоручује производе и услуге. Стандарди ове серије не односе се на техничка својства производа или процеса. Стандарди су настали као последица потребе да се утврде захтеви које неки испоручилац треба да испуни да би га купац сматрао погодним за дугорочну сарадњу.

Погодно је онда да се дефинише један минимални скуп захтева који би гарантовао уједначеност квалитета испоручених производа и спречио да производ са одступањима доспе до купца. Стандард ISO 9001 управо је томе намењен – он штити купца тиме, што од произвођача тражи да обезбеди ресурсе и примени систем управљања процесима рада да би се осигурали усаглашеност и задовољење захтева корисника.

Појавом организација за сертификацију, које оцењују усаглашеност са стандардом, смањила се потреба да сваки купац за себе проверава поузданост добављача. Тако стандард и систем сертификације служи свим заинтересованим странама, а сам сертификат служи као потврда да организација ефективно управља својим интерним процесима рада.

Мора се нагласити, међутим, да сертификат ништа не говори о постизању потребног нивоа квалитета производа, јер стандард ISO 9001 томе није ни намењен. Такође, треба истаћи да је стандард ISO 9001 доста ограничен, јер не поставља захтеве који за купца нису битни. На пример, нема захтева у погледу задовољства запослених или управљања финансијама, тако да организација која жели да унапреди своје пословање не може да се задржи само на примени стандарда ISO 9001 – то је тек први корак у процесу континуираног унапређења, аостали кораци су други стандарди попут стандарда ISO/IEC 27001 – Систем менаџмента безбедношћу информација, OHSAS 18001 – Систем менаџмента заштите здравља и безбедности на раду, ISO 31000 – Систем менаџмента ризиком и други.

Дакле, увођење ISO стандарда је веома битно и значајно, првенствено као доказ квалитета и то како у органицацијама које се баве производним делатностима, тако и у компанијама које се баве услужним делатностима, као што су банкарске и друге финансијске институције.

Имплементација ових стандарда у финансијским организацијама даје основ за развој интегрисаног система менаџмента,који представљадобар начин за ефективно и ефикасно управљање пословном организацијом.

2. Основи стандардизације

Стандард је документ у коме се дефинишу правила, смернице или карактеристике за активности или њихове резултате (производ или услуга могу бити тај резултат) ради постизања оптималног нивоа уређености[1].

Стандарди у великој мери имају позитиван утицај на већину аспеката живота. Они обезбеђују жељене карактеристике производа и услуга као што су квалитет, позитивно деловање на животну средину, безбедност, поузданост, ефикасност и заменљивост.

Када су производи и услуге у складу са очекивањима, то се узима здраво за готово и нико није ни свестан улоге стандарда. Међутим, ако стандарди не би постојали, то би се веома брзо приметило. Сметало би то што су производи лошег квалитета, што нису одговарајући, односно некомпатибилни, или су непоуздани и опасни. Када производи, системи, машине и уређаји раде добро и безбедно, то је углавном зато што испуњавају захтеве стандарда.

Стандарди помажуразвој, производњу и дистрибуцију производа ефикаснијим, безбеднијим и чистијим; усклађују трговину између земаља; омогућавају размену технологије и добре управљачке праксе; шире иновације; осигуравају купце и кориснике производа и услуга; чине живот једноставнијим тиме што дају решења за свакодневне проблеме.

ISO је невладина организација и нема ауторитет да наметне имплементацију стандарда. ISO не доноси ни прописе ни законе. Међутим, државе могу да одлуче да усвоје ISO стандарде – пре свега у области здравља, безбедности и утицаја на животну средину – као законски обавезне или да се на њих позивају у прописима[1]. Иако су ISO стандарди добровољни, они постају захтев тржишта, као на пример ISO 9001 серија стандарда.

ISO стандарди се развијају према потребама тржишта. Посао претежно обављају експерти из сектора индустрије, технике и пословања у којима се покаже потреба за стандардима. Они су базирани на интернационалном консензусу између стручњака у одређеној области. Сви стандарди се периодично прегледају и то најмање једном у пет година, како би се одлучило да ли је потребно да буду измењени и допуњени или укинути. ISO стандарди су технички споразуми који обезбеђују оквир за компатибилност технологије у целом свету. Они су дизајнирани да буду глобално значајни и корисни било где у свету[2].

Према Закону о стандардизацији, стандардизација је „активност наутврђивању одредби за општу и вишекратну употребу у односу на стварнеили потенцијалне проблеме, у циљу постизања оптималног нивоа уређеностиу датом контексту“, која укључује процес формулисања, издавања и применестандарда и то на националном, европском и

међународном нивоу[3]. Резултат стандардизације су стандарди као званична документа, са захтевима којисе односе на производ, процес у коме производ настаје или предузеће каопословни систем основан ради обављања одређене делатности која стваравредност (производ или услугу) за тржиште (кориснике и крајње купце) иза власнике.

Стандардизација може да има један или више циљева који омогућавајуда производи, процеси и услуге буду усклађени са својом наменом. Општи циљеви стандардизације могу бити остваривање спремности за намену, компатибилности, заменљивости, смањења броја варијанти, безбедности, заштите животне средине и заштите производа.

Други циљеви могу битии заштита здравља, узајамно споразумевање, побољшање економских перформанси, уклањање препрека у трговини и друго. Основни принцип стандардизације је да се стандарди не доносенаредбом „одозго", већ њих припремају заинтересоване стране (индустрија, потрошачи, органи власти, стручна и пословна удружења, тела заоцењивање усаглашености и др.) када истовремено постоји објективнапотреба за њима и жеља заинтересованих страна да учествују у њиховом формулисању.

Другим речима, стандардизација је инструмент техно-економске саморегулације који припада свим учесницима у националној, регионалној, односно светској привреди (економији) и служи стварањујавног добра[3].

Имајући у виду да циљеви стандардизације и користи од ње представљајуопшту корист за привреду, безбедност и заштиту, али и бољу комуникацију, стандардизација се базира на неколико основних начела[4]:

- Консензус као општи споразум о било ком значајном питању постигнутна начин да се узму у обзир аспекти свих заинтересованих страна. Иакоје неопходно усагласити сва супротстављена становишта, консензус неподразумева и једногласност.
- Укључивање свих заинтересованих страна чиме све укључене странедобровољним учешћем доприносе процесу израде стандарда.
- Заједнички интерес који се манифестује кроз спречавање појединачнихинтереса над заједничким интересом заинтересованих страна.
- Потпуна транспарентност, односно отвореност и прегледност процесастандардизације и доступност стандарда јавности.
- Кохерентност која подразумева да збирка стандарда мора бити међусобнокомпатибилна, тј. да стандарди не могу бити противречни. То значи дадоношење новог стандарда за одређену област стандардизације захтеваповлачење старог стандарда.
- Степен развоја технике се односи на услов да стандард треба да одсликавастепен развоја технике у датом времену, те да је исти утемељен напровереним научним, техничким и искуственим сазнањима.

- Спречавање настанка препрека у трговини чиме се указује да стандарди нису припремљени, донети или примењени са циљем стварања неоправданих препрека у међународној трговини. Због тога је, када годје то могуће, пожељно користити међународне стандарде или њихове одговарајуће делове као основу за израду националних стандарда.

2.1.Стандард ISO 9001:2008-Систем менаџмента квалитетом

ISO 9001 је погодан за све организације које желе да побољшају начин управљања, без обзира на величину или далатност организације. Сврха овог стандрда је повећање ефикасности организације кроз примену процесног приступа и његова основна предност је обезбеђивање веза између појединачних процеса, сектора и њихове интеракције. Дефинисањем улазних и излазних елемената свих процеса и дефинисањем потребних ресурса, ствара се полазна основа за планирање као и повратна информација о задовољству купаца. Овакав модел повећава поверење клијената у производ/услугу и води ка бољем позиционирању на тржишту.

ISO 9001 прецизира основне захтеве за систем управљања квалитетом, које организација мора да испуни како би показала своју способност да своје производе доследно производи (који укључују услуге), чиме се повећава задовољство корисника и испуњавају важеће законске регулативе[5].

Ефективан систем менаџмента квалитетом способан је да обезбеди оквир и услове за стално побољшавање чиме се повећава вероватноћа да се постигне боље задовољење корисника[6]. Изузетно је важно да сви запослени буду свесни значаја испуњавања захтева корисника и остваривања квалитета производа/услуге.

Корисници захтевају производе и услуге које задовољавају њихове потребе и очекивања. Своје потребе и очекивања корисници најчешће исказују у одговарајућим спецификацијама.

Захтеви корисника могу бити специфицирани у уговору, али их може утврдити и организација. У оба случаја корисник је тај који на крају утврђује да ли су производ или услуга прихватљиви или не. Конкуренција и технички развој условљавају сталне промене потреба и очекивања корисника, па су организације приморане да стално побољшавају своје производе, услуге и процесе.

Систематски приступ менаџменту квалитетом подстиче организацију да[7]:

- Анализира захтеве корисника;
- Доследно испуњава захтеве и очекивања корисника;

- Утврди процесе који доприносе реализацији производа/услуге који испуњавају захтеве корисника;
- Управља тим процесима;
- Решава проблеме који се односе на квалитет.

Обавезе највишег руководства не ограничавају се само на доношење стратешке одлуке о увођењу система менаџмента квалитетом, већ је потребно њихово активно укључивање у успостављање, документовање, примену, одржавање и стално побољшавање ефективности система менаџмента квалитетом.

Током успостављања и примене система менаџмента квалитетом организација мора да [8]:

- Утврди потребе и очекивања корисника и осталих заинтересованих страна;
- Утврди политику квалитета и циљеве квалитета;
- Утврди процесе и овлашћења и одговорности неопходне за остваривање циљева квалитета;
- Утврди и обезбеди ресурсе неопходне за остваривање циљева квалитета;
- Утврди методе мерења ефективности и ефикасности сваког процеса;
- Примењује утврђене методе ради верификовања ефективности и ефикасности сваког процеса;
- Утврди начине за спречавање неусаглашености и елиминисање њихових узрока;
- Утврди систем мониторинга и преиспитивања;
- Утврди и примењује процесе сталног побољшавања система менаџмента квалитетом.

Систем менаџмента квалитетом мора да одговара организацији, да буде погодан и ефективан. Успостављање, документовање, примена, одржавање и стално побољшавање ефективности таквог система захтева време, труд и ангажовање свих запослених.

Најзначајније користи од система менаџмента квалитетом су[9]:

- Побољшавање планирања свих пословних процеса;
- Стварање свести о квалитету у целој организацији;
- Побољшавање нивоа интерног и екстерног комуницирања;
- Повећавање задовољења корисника;
- Побољшавање организације пословања;
- Смањење трошкова неодговарајућег квалитета.

Принципи менаџмента квалитетом обухватају [10]:

- Усмеравање на кориснике – организација зависи од корисника па, према томе, треба да разуме актуелне и будуће потребе корисника, треба да испуни њихове захтеве и да настоји да пружи и више од онога што корисници очекују.

- Лидерство – лидери успостављају јединство циљева и вођења организације – они треба да стварају и одржавају интерно окружење и климу у којима запослено особље може у потпуности да учествује у остваривању циљева организације.
- Укључивање особља – особље на свим нивоима чини суштински део организације и њихово пуно укључивање омогућава да се искористе способности појединаца за остваривање добробити организације.
- Процесни приступ – остваривање жељених резултата знатно је ефикасније ако се менаџмент активностима и ресурсима остварује као процес.
- Системски приступ менаџменту – идентификовање и разумевање система међусобно повезаних процеса и менаџмент тим системом доприносе ефективности и ефикасности организације у остваривању утврђених циљева.
- Стално побољшавање – трајни циљ организације треба да буде стално побољшавање њених укупних перформанси.
- Одлучивање на основу чињеница – анализа података и информација представља основу за доношење ефективних одлука.
- Узајамно корисни односи са испоручиоцима – организација и њени испоручиоци су међусобно зависни – узајамно корисни односи повећавају способност и једних и других да стварају вредност.

Стандард ISO 9001 има 8 поглавља:

- Предмет и подручје примене,
- Нормативне референце,
- Термини и дефиниције,
- Систем менаџмента квалитетом,
- Одговорност руководства,
- Менаџмент ресурсима,
- Реализација производа,
- Мерење, анализа и побољшања.

Свако поглавље стандарда подељено је на тачке и подтачке које садрже одређене захтеве.

2.2. Стандард ISO 27001:2013 - Систем менаџмента безбедношћу информација

ISO/IEC 27001 је међународни стандард који својим захтевима дефинише систем менаџмента безбедношћу информација, чији је примарни циљ информационо-физичко-техничка заштита предузећа. Систем менаџмента безбедношћу информација ISO27001 је применљив на банкарске и финансијске институције, IT(информационе технологије) секторе, економске секторе, све јавне или приватне организације [11].

Безбедност информација је кључна компонента управљања IT. Попут информационе технологије, саме информације постају све више стратешки покретачи организационе активности, тако да ефективан менаџмент IT-а и информација постаје критична стратешка тачка многих компанија. Овај стандард ће омогућити предузећима да осигурају њихове стратегије безбедности IT координисане, кохерентне, јасне, да смањују трошкове и испуњавају њихове специфичне организационе и пословне потребе.

ISO/IEC27001 даје оквир који је неопходан за стварање сигурног система. Усаглашен системISO27001 ће обезбедити систематски приступ за идентификовање и борбу против читавог низа потенцијалних ризика којима су изложене информације организације.

Заштита и безбедност информација за данашњи свет бизниса је много важнији него икада раније. Данас, бизнис зависи од информационих технологија, комуникација путем мрежа,као и бежичних и мобилних комуникација. Обављање послова путем интернета и компјутера,подуговарање и коришћење услуга треће стране постају све чешћи видови савременогпословања. Ланац снабдевања постаје све сложенији и већи, а могућност компјутерскихпревара доводи до повећања ризика у свим областима пословања.

Успешан бизнис и доношење добре одлуке могуће је остварити само уз правовремени приступправим и сигурним информацијама које су за то неопходне. Заштита таквих информација постајепредуслов за остваривање претходно поменутог и зато јој треба прићи системски. Међународнистандарди серије ISO/IEC 27001, који се односе на информационе технологије, технике заштите исистем менаџмента безбедношћу информација, развијени су и донети са намером дапомогну системски приступ у обезбеђењу овог предуслова[11].

Да би се стекло поверење у тачност и поузданост потребних информација потребно је иматиповерење у систем менаџмента њиховом безбедношћу.Поузданост и поверење у систем менаџмента безбедношћу информација постиже сењеговом сертификацијом од независне и непристрасне треће стране, односно сертификационогтела, компетентног за обављање тог посла и које је своју компетентност, такође, доказало наадекватан начин.

Најподеснији начин потврђивања компетентности ових сертификационих телајесте акредитација коју спроводи национално акредитационо тело. Сертификацијом се потврђујеусаглашеност са захтевима дефинисаним у стандарду ISO/IEC 27001.

Процес сертификације стандарда ISO 27001 је у основи исти као онај који сеспроводи при сертификацији система менаџмента квалитетом према ISO 9001 или неког другогсистема менаџмента. Стандард дефинише критеријумеза сертификациона тела, која спроводе проверу и сертификацију било ког система менаџментанеке организације укључујући и систем менаџмента безбедношћу информацијама и онпредставља основ за акредитацију.

Намена стандарда серије ISO/IEC27001је да омогуће помоћ организацијамасвих врста и величина да развију и примене систем за управљање безбедношћу сопствених информација и да се припреме за независно и непристрасно оцењивање (сертификацију) тогсистема примењеног на заштиту информација, као што су, на пример финансијске информације, информације о интелектуалној својини, подаци о особљу или информације које су им поверене одкорисника или треће стране.

Серија стандарда ISO /IEC 27001 обухвата стандарде који: дефинишу захтеве за ISMS као и захтеве за тела којасертификују ISMS; обезбеђују подршку, детаљна упутства и инструкције за целокупан процеспланирај-уради-провери-делуј (PDCAкруг); даје специфична секторска упутства за ISMS и оцењивање усаглашености за ISMS.[12]

Ова серија стандарда је у вези и са многим другим ISO и ISO/IEC стандардима који се односена област безбедности информација и који обезбеђују специфичне захтеве, упутства и сл.ISO/IEC 27001 истиче да није могуће у потпуности елиминисати целокупан ризик у вези сабезбедношћу информација и омогућава организацијама да установе критеријуме који ћеуравнотежити могућности пословања, захтеве дефинисане у прописима, уговорне обавезе,цену контролисања безбедности информација и ризик.

Користи од имплементације система менаџмента безбедношћу информација у организацији су следеће [13]:

- Доказ да је усаглашено са захтевима који су изнети у Стандарду ISO 27001;
- Сагласност са најбољом праксом у менаџменту ризика у односу на власништво и безбедност информација;
- Усаглашеност са законима;
- Систематска заштита од опасних и потенцијалних трошкова злонамерне употребе компјутера, сајбер криминала и других негативних утицаја;
- Побољшање свог кредибилитета код особља, клијената и партнерских организација;
- Финансијске користи и побољшана продаја услуга;
- Практичне одлуке везане за сигурносне технике и решења за развој;

- Постојање одговорности за безбедност информација од стране свих и на свим нивоима у организацији;
- Боље тржишне могућности.

2.3.Стандард ISO 31000: 2009 - Систем менаџмента ризиком

Стандард ISO 31000дајеосновне принципе и смернице за менаџмент ризиком. Управљање ризиком представља процес мерења и процењивања ризика на основу чега се равија стратегија за отклањање или смањење ризика.[14]. Тачније, менаџмент ризика је процес кроз којим се организације припремају за суочавање са неодређеностима које могу да утичу на реализацију њихових циљева. Стога, управљање ризиком представља мултидиспинарни и системски процес.

Овај стандард може да користи било која организација, приватна или друштвена, затим удружење, група или појединац, што значи да се може применити на широк спектар активности, укључујући производе и услуге, стратегију и одлуке, процесе и функције.Овај стандард се, такође, може применити на сваку врсту ризика, ма каква да је његова природа, било да има позитивне или негативне последице.

СтандардISO 31000 препоручује да организација развија, имплементира и константно унапређује оквир, чија је сврха интеграција процеса управљања ризицима у читавој организацији.

Дакле, управљање ризицима може бити примењено на свим нивоима организације, од стратегијског нивоа, преко појединих организационих делова, па све до појединачних процеса и активности.

Менаџмент ризиком представља процес активног доношења одлука, чиме се елиминишу ризици пре него што они настану. Управљање ризиком директно утиче на побољшање процеса доношења одлука, нарочито оних који носе велике ризике, омогућавајући руководиоцима да боље разумеју окружење и ризике, да заштите себе и своју организацију и на тај начин постигну постављене циљеве. Стога је управљање ризиком реална претпоставка пословног успеха. С друге стране, управљање ризиком треба да обезбеди континуалну егзистенцију система. Документација проистекла из процеса менаџмента ризиком омогућава процес акредитације и ауторизације менаџмента ризиком.

Према стандарду ISO 31000, процес управљања ризиком обухвата[15]:

- Комуницирање и консултовање;

- Утврђивање контекста (Утврђивање елемената модула који дефинише основне параметре управљања ризицима и одређује области примене и критеријуме за остатак процеса);
- Идентификација ризика;
- Анализа ризика;
- Оцену (вредновање) ризика;
- Поступање са ризицима (третирање ризика);
- Мониторинг и преиспитивање.

Имплементацијом процеса управљања ризицима према ISO 31000, организација може имати вишеструке користи[15]:

- Повећање вероватноће остваривања постављених пословних циљева;
- Подстицање проактивног деловања менаџмента;
- Повећање свести и схватања потребе идентификације и третирања ризика у организацији;
- Унапређење способности идентификовања шанси и претњи;
- Повећано усклађивање са релевантним законским нормама и међународним стандардима;
- Унапређење управљања, извештавања, поверења и заинтересованих страна;
- Успостављање поуздане основе за доношење одлука и планирања;
- Снижавање губитака, ефикасније коришћење ресурса;
- Унапређење здравља и безбедности запослених, унапређења пословања, заштите животне средине;
- Унапређење отпорности организације према проблемима и др.

Основни концепт управљања ризиком дат у стандарду 31000 је у сагласности са традиционалном парадигмом управљања кавлитетом (PDCA)-планирај, уради, провери и изврши. Овај стандард је посебно применљив за оне компаније које желе да унапреде сопствени систем управљања ризиком, из разлога што такве компаније послују у турбулентном окружењу које нуди високе шансе и ризике, развијајући, при том, веома вредне и иновативне пословне пројекте који су дугорочно изложени ризику јер су базирани на савременим технолошким решењима.

Дакле, ефикасан систем менаџмента ризиком пружа корисницима главну основу за одређивање, анализу, оцену и контролу ризика, што га чини једним од најважнијих алата за управљање у било којој организацији.

Међународна Организација за стандардизацију (ISO) је 2005. године је пласирала развој интернационалног стандарда за менаџмент ризицима ISO 31000, а који је објављен 2009. године. Током 2010. године, почиње да се примењује као први међународни стандард за

управљање ризицима у свету, који је намењен да помогне оним организацијама које до тада нису примењивале систем менаџмента ризиком, као и компанијама које су своје стратегије прилагодиле захтевима и потребама менаџмента ризиком, али нису постигле још увек очекиване резултате.

Стандард није намењен да се користи ради сертификовања.

2.4.Значај интеграције ISO стандарда и њихова повезаност

Увођење интегрисаних система менаџмента захтева многобројне промене у компанији, од промена у процесима и процедурама до промена у читавој филозофији пословања и целокупној култури организације[16]. Интеграција менаџмент система је природан пут, који формално задовољава различите стандарде, а истовремено подиже ниво способности организације и њено приближавање циљевима изврсности. Побољшање свих перформанси организације има за циљ остваривање најважнијег задатка сваког пословања а то је опстати на тржишту.

Парцијални менаџмент системи су концентрисани на изолована подручја која су често међусобно у супротности, тако да код њихове примене може доћи до конфликата надлежности у организацији. Већ постоје искуства која потврђују да је тотални интегрисани менаџмент систем – квалитета, животне средине, здравља, безбедности информација и др. далеко продуктивнији и ефикаснији од појединачних стандардизованих система.

Издвојени системи управљања имају предност у томе што дају заокружен систем у потпуности прилагођен активностима којима се управља. Међутим, опасност која се јавља у оваквом прилазу управљања организацијом јесте постојање могућности да поједина решења у различитим системима буду међусобно супростављена и на тај начин стварају сметње у одвијању целокупног процеса. Интегрисани системи управљања нуде хармонизацију целокупног управљања, али исто тако могу носити и ризик уопштавања решења, при чему може доћи до занемаривања битних карактеристика појединих активности[16].

То се може избећи тако што ће се при интегрисању система сачувати део специфичних решења из сваког система појединачно. У том смислу најчешће се препоручује да се уместо покушаја да се испуне појединачни захтеви, изврши повезивање захтева и конкретно имплементирање на основу процесног модела. Унапређењем комуникација између различитих организационих целина, бољом кооперацијом, радом у процесима, а не

само у функцијама, створиће се услови да запослени теже тоталном менаџмент систему [17].

Посматрајући одвијање процеса и њихову међусобну условљеност може се доћи до закључка да ће примена IMS довести до значајних напредака. Интеграцијом система значајно се може утицати на повећање квалитета целокупних активности у оквиру предузећа. Овакви системи морају да развијају само оне алате који ће ујединити људе (и запослене и кориснике), све процесе и програме у организацији.

Фамилије стандарда ISO 9000 су најпознатији и најпримењиванији ISO стандарди до сада у свету. Верзија стандарда ISO 9001:2000 од 1996. и 2004 године су имплементиране у више од 1.200.000 организација у 101 држави. Поред наведеног, веома је значајна и серија стандарда ISO/IEC 27001 која се бави проблемима безбедности информација, као стандард ISO 31000 који се бави утврђивањем и отклањањем ризика у организацијама.

Интегрисани систем менаџмента је начин за ефективно и ефикасно управљање пословном организацијом. Руководство организације има обавезу да непрекидно одговара на захтеве тржишта и осталих заинтересованих страна власника, запослених, купаца, испоручилаца и друштва (да примењује законске и друге националне и међународне прописе).

Успостављање IMS-а у пословну праксу намеће потребу његовог дефинисања. Интеграција се посматра као суштински стандард највишег нивоа менаџмента са опцијама који покривају различите или специфичне захтеве. Повезивање подразумева паралелне стандарде система менаџмента који су специфични за поједине дисциплине уз висок ниво саобразности у структури и садржају[17].

Интеграцијом се захтева, да се од различитих стандарда за системе менаџмента добије шири, обухватнији и снажнији интегрисани систем менаџмента којим се на ефикаснији и ефективнији начин управља организацијом. Најприхватљивија дефиниција IMS са становиштанајвишег руководства организације гласи: Интегрисани систем менаџмента је све обухватни алат менаџмента који повезује све елементе пословног система у јединствен и целовит систем управљања процесима у организацији, ради задовољавања захтева заинтересованих страна и остваривања пословних циљева у складу са визијам и мисијом организације [18].

Веза између система менаџмента квалитетом, безбедношћу информација и ризиком дата је у следећој табели.

Табела 1. Веза између стандарда ISO 9001, ISO 27001 и ISO 31000.

ISO 9001:2008	**ISO 27001:2013**	**ISO 31000:2009**
0 Увод	0 Увод	
0.1 Општи принципи		
0.2 Процесни приступ		
0.3 Везе са осталим стандардима		
0.4 Компатибилност са другим системима менаџмента	0.2 Компатибилност са другим системима менаџмента	
1 Поље деловања	1 Поље деловања	
1.1 Општи приступ	1.1 Општи приступ	
1.2 Примена	1.2 Примена	
2.0 Референце	2.0 Референце	
3.0 Термини и дефиниције	3.0 Термини и дефиниције	
4.0 Систем менаџмента квалитетом	4.0 Систем менаџмента безбедношћу информација	4.0 Систем менаџмента ризиком
4.1 Општи захтеви	4.4. Информациони систем за управљање безбедношћу	4.1 Општи захтеви
4.2 Потребна документација	4.2 Потребна документација	4.2 Потребна документација
4.2.1 Општи принципи		
4.2.2 Квалитет процеса	4.3 Одређивање обима система управљања безбедношћу информација	5.2 Мандат и посвећеност
		5.3.2 Политика управљања ризиком
		5.3.3 Интеграција у организационе делове
4.2.3 Контрола документације		
4.2.4 Контрола записа		
5. Одговорности руководства	5. Одговорности руководства	
5.1 Обавезе менаџмента	4.2. Разумевање и потребе заинтересованих страна	5.3.1 Разумевање организације и њених контекста
5.2 Фокус на кориснике	5.2 Фокус на кориснике	
5.3 Контрола квалитета	5.3 Контрола квалитета	
5.4 Планирање		
5.5 Одговорност, ауторизација и комуникација		5.3 Дизајн структуре за управљање ризиком

5.5.1 Одговорност и овлашћења		5.3.4 Одговорност
5.5.2 Представник руководства		
5.5.3 Интерно комуницирање	7.4 Комуницирање	5.3.6 Успостављање интерне комуникације и механизама извештавања
5.6 Преиспитивање од стране руководства	9.3 Преиспитивање од стране руководства	
5.6.1 Општи принципи		
5.6.2 Улазни подаци		
5.6.3 Излазни подаци		
6 Менаџмент ресурсима		5.3.5 Ресурси
6.1 Обезбеђивање ресурса	6.1 Обезбеђивање ресурса	
6.2 Људски ресурси		
6.2.2 Обука, свест и компетентност	7.2 Надлежност и свест	
6.3 Инфраструктура		
6.4 радна средина		
7. Реализација производа		
7.1 Планирање реализације производа		
7.2 Процеси који се односе на кориснике		
7.2.1 Утврђивање захтева који се односе на производ		
7.2.2 Преиспитивање захтева који се односе на производ		
7.2.3 Комуницирање са корисницима		5.3.7 Успостављање екстерне комуникације и механизама извештавања
7.3 Пројектовање и развој		5.4 Увођење управљања ризиком
7.3.1 Планирање пројектовања и развоја		5.4.1 Развој плана за увођење
7.3.2 Улазни елементи пројектовања и развоја		
7.3.3 Излазни елементи пројектовања и развоја		
7.3.4 Преиспитивање пројектовања и развоја		

7.3.5 Верификација пројектовања и развоја		
7.3.6 Валидација пројектовања и развоја		
7.3.7 Управљање изменама пројектовања		
7.4 Набавка		
7.4.1 Процес набавке		
7.4.2 Информације о набавци		
7.4.3 Верификација производа који се набавља		
7.5 Производња и сервисирање		
7.5.1 Управљање производњом и сервисирањем		
7.5.2 Валидација процеса производње и сервисирања		
7.5.3 Идентификација и следљивост		
7.5.4 Имовина корисника		
7.5.5 Очување производа		
7.6 Управљање уређајима за праћење и мерење		
8. Мерења, анализе и побољшавања	9.1 Праћење, мерење, анализа и процена	6.2 Комуникација и консултације, праћење и преиспитивање
8.1 Опште одредбе		
8.2 Праћење и мерење		
8.2.1 Задовољење корисника		
8.2.2 Интерни аудит	9.2 Интерни аудит	
8.2.3 Праћење и мерење процеса	8.1 Оперативно планирање и контрола	5.5 Праћење и преглед структуре
8.2.4 Праћење и мерење производа	9.1 Праћење, мерење, анализа и процена	
8.3 Управљање неусаглашеним производом	10.1 Управљање неусаглашеностима и корективне мере	
8.4 Анализа података		
8.5 Побољшања	10. Побољшања	

8.5.1 Континуална побољшања	10.2 Континуална побољшања	5.6 Непрекидно унапређење структуре
8.5.2 Корективне мере		
8.5.3 Превентивне мере	6.1.1 Акције за решавање ризика и могућности	
	6.1.2 Процена ризика информационе безбедности	

Предности интеграције система менаџмента [17]:

- Привржености, пажња и укључивање највишег руководства далеко је извеснија када су интегрисани циљеви, ресурси и мере и када се врши заједничко преиспитивање IMS;
- Интеграција система менаџмента омогућује ефективније одвијање дневних операција без укључивања највишег руководства, остављајући му времена за стратешке активности;
- Адаптација основног менаџмент система према различитим стандардима је ефикаснија и јефтинија од градње и примене појединачних MS;
- Ефикаснији је интегрисан менаџмент систем са више фокуса од више парцијалних менаџмент система са по једним фокусом;
- Једноставиније и ефективније је управљање интегрисаним циљевима који имају више аспеката од управљања циљевима појединих MS;
- Ефективније је интегрисање IMS у стратегију и праксу организације од интегрисања појединачних MS;
- Примена и одржавање система кроз интегрисана испитивања, верификације, преиспитивања и валоризације, штеди време и новац;
- Ефикаснији је јединствен процес побољшања са више аспеката него више одвојених процеса побољшања;
- Јефтинији и ефективнији је реинжењеринг процеса који садржи више аспеката од вишеструких реинжењеринга са одређеног аспекта;
- Јефтинији и ефективнији је интерни аудит и припрема за сертификацију IMS од појединачних за сваки MS;
- Стицање поверења код купаца и позитиван имиџ на тржишту и у друштву;
- Интегрисани систем обезбеђује већи ниво менаџмент контроле, него када је успостављен менаџмент више различитих система;
- Оптимизација приоритета, када је један представник руководства фокусиран и задужен за IMS у односу на више особа задужених за различите системе који имају своје фокусе и приоритете;
- Јединствени програм обука за IMS штеди новац и време, а смањује појаву конфузије код запослених порукама из одвојених обука за различите системе.

3. Студија случаја примене система менаџмента квалитетом, безбедношћу инфорамција и ризика у Чачанској банци ад

3.1.Значај увођења стандарда ISO 9001, ISO 27001 и ISO 31000 у банкарском пословању

Увођење ISO стандарда у банкарским институцијама има за циљ побољшање ефикасности и квалитета пословања. То је веома сложена и комплексна активност, која пре свега зависи од бројних карактеристика пословне и организационе структуре саме институције.

Увођење стандарда у банкарским институцијама подразумева увођење процедура које ће бити ефикасне и економичне, што захтева стална улагања у људске и материјалне ресурсе.

Разлози увођења стандарда у банкарски сектор, заснивају се на следећим чињеницама[19]:

- брзих и ефикасних задовољења потреба корисника банкарских услуга;
- антиципирању њихових будућих потреба;
- минимизирању ризика;
- побољшању конкурентске позиције на тржишту и др.

У данашњим условима пословања, квалитет игра веома значајну улогу и то не само у када је у питање освајање нових тржишта, већ игра значајну улогу и у задржавању постојећих.Купци не очекују само квалитетан производ, већ захтевају и доказ да је организација способна да произведе квалитетне производе или пружи квалитетне услуге.

Присутност система менаџмента квалитета у производним и услужним делатностима и његов утицај на раст глобалне економије из дана у дан је све израженији.Овакав концепт квалитета даје основу за напредовање привредних субјеката кроз бољу конкурентност и компетентност, не нарушавајући, при том, основна правила конкуренције, заштите потрошача и слободног промета робаи услуга.

Основни захтеви који се намећу код стварања система квалитета у услужним делатностима, потичу од захтева Светске трговинске организације (WTO), чијим испуњавањем се обезбеђује отвореност глобалног тржишта роба и услуга.С тим у вези, све већи број организација из области финансијских услуга настоје да уведу систем менаџмента квалитетом према стандардима серије ISO 9001.

Стандарди серије ISO 9001 финансијским организацијама обезбеђују задовољење потреба и захтева корисника услуге, из разлога што се у први план ставља управо

корисник односно купац. Стандарди серије ISO 9001 су на тај начин оправдали своје појављивање и увођење, јер данас у свету има више од милион сертификованих организација.

С тим у вези, увођење система менаџмента квалитетом у банкарским организацијама је веома сложен и дуготрајан процес, који захтева ангажовање свих организацијских нивоа, како менаџмента тако и свих запослених.Задовољење захтева стандарда треба да обезбеди успостављање визије и мисије, дефинисање стратегије, идентификацију свих пословних процеса у систему и управљање документацијом, а све у циљу да се остваре основни принципи банкарског пословања а то су сигурност, ликвидност и ефикасност пословања.

Свака банка у свом пословању мора да испуни 3 главна циља која се односе на систем менаџмента квалитета[20]:

1) треба да постигне, одржава и континуално побољшава квалитет својих производа и услуга у односу на захтеве квалитета и да тако побољша квалитет сопствених активности на начин који ће омогућити стално испуњавање утврђених захтева клијената и других чинилаца из свог окружења;
2) треба да стекне поверење свог руководства као и других запослених да ће захтеви за квалитет бити постигнути и одржавани и да је побољшање квалитета присутан фактор и
3) треба да постигне поверење клијената да се захтеви за квалитет постижу или ће бити постигнути у испорученим производима односно услугама.

Свакако унапређење система менаџмента квалитетом једне банке јесте сигурно њена најбоља пословна стратегија и иста се мора посматрати као део пословне развојне стратегије са највишим степеном приоритета у реализацији.

У већини банака најчешће се појављују следећи елементи система квалитета[20]:

- документација система квалитета;
- организација банке за квалитет;
- преиспитивање система квалитета банке;
- планирање квалитета;
- утврђивање неусаглашености и корективне акције,
- контрола развоја новог банкарског производа;
- контрола опреме за мерења;
- контрола набављеног материјала;
- контрола процеса банкарских услуга;
- контрола односа са корисницима услуга;
- преиспитивање уговора;
- обука за квалитет.

У циљу обезбеђивања компетентности и усаглашености система квалитета, сви његови делови морају бити написани, документовани и одобрени од стране највишег руководства.

Стратегија увођења система квалитета је најважнији циљ који треба дефинисати у свакој банци. Сама стратегија увођења система квалитета треба да дефинише циљеве који прате остварење основних принципа менаџмента и то:

- усмерити пословање ка клијентима/корисницима услуга;
- обезбедити учешће свих сарадника/тимски рад;
- постићи разумевање токова активности у банци и обезбедити контролне механизме;
- обезбедити веродостојан приказ података;
- успоставити систем квалитета и
- вршити континуирано пословање.

Квалитет утиче на проширење тржишта, као и на повећање удела тржишта, из чега произилази пораст обима пословања што банци даје конкурентску предност у односу на друге конкуренте на тржишту.

Увођењем нових технологија у пословање банака који се односе на обављање банкарских послова, електронски захтева од банака да упоредо уводи и **системе за управљање безбедношћу информација** – **ISO 27001**. Технолошке промене су утицале да се понуда банкарских производа променила увођењем електронског пословања у обављању пословних процеса.Развој и све шира примена информационе и комуникационе технологије (ICT) у процесу обраде и преноса података и информација донела је крупне технолошке промене у функционисању банака и других финансијских институција[21].

Применом стандарда за безбедност и заштиту информација у електронском банкарском пословању стичу се следеће предности[22]:

- боље тржишне могућности;
- смањење ризика а самим тим и расхода;
- усаглашеност са важећим законским прописима;
- веће поверење клијената, запослених, сарадника и институција и свих заинтересованих страна због знања да су њихове информације и подаци максимално безбедни;
- постојање одговорности за безбедност информација од стране свих и на свим нивоима.

Главни разлог за увођење система менаџмента безбедношћу информација у банкарском сектору је жеља и потреба саме банке да уреди и стандардизује област безбедности информација у свом пословању. Банка настоји да своје информације и информациони

систем заштити, јер информације за банку представљају имовину која има вредност као и сва друга пословна имовина. Сигурношћу се информације штите од широког опсега претњи чиме банка осигурава континуитет у пословању, настоји да оствари пословни успех, а своје губитке сведе на минимум.

Сигурност информација банка обезбеђује увођењем одговарајућег скупа контрола које су у виду политика и процедура. Банка се стално суочава са претњама по њен информациони систем који укључује преваре уз коришћење рачунара, шпијунирање, саботаже, пожаре и поплаве. Извори оштећења као што су рачунарски вируси, као и напади пробијања у рачунаре и одбијања активирања функција постали су чешћи, амбициознији и усавршенији. С тим у вези, оцењивање ризика у вези информација је основа за успостављање система менаџмента безбедношћу информација и представља његову основну карактеристику[23].

Увођење стандарда ISO/IEC27001 банци даје вишеструке користи:

- идентификацију и смањење безбедоносних ризика на жељени ниво,
- побољшање пословних партнерстава (већа поверљивост међусобно размењених информација),
- боље инвестирање,
- конкурентску предност приликом уговарања послова,
- уређено управљање процесима у вези безбедности информација.

Како би се обезбедио систем сигурности и заштите информација, потребно је да се дефинишу захтеви за сигирност који произилазе из три главна извора.
Први извор се добија оцењивањем оперативних и других ризика у банци. Преко оцењивања ризика идентификују се претње по имовину, вреднују се рањивост и вероватноћа догађаја и процењују се могуће последице.
Други извор чине законски, статутарни и уговорни захтеви које банка, њени пословни партнери и даваоци услуга морају да испуне.
Трећи извор чини посебан скуп основних политика, циљева и захтева за обраду информација које су подршка пословним процесима [24].

Систем који банка користи за безбедност има три битне особине, то су:

- општост,
- могућност предвиђања и
- адекватност.

Систем безбедношћу информација банци омогућује[24]:

- поверљивост – осигуравање да информације буду на располагању само онима који су овлашћени да им приступају;

- интегритет – самозаштиту тачности и целовитости информација и метода за обраду;
- расположивост – осигуравање да овлашћени корисници имају приступ информацијама и припадајућој имовини када им је потребно.

Банка примењује стандард ISO27001 не само на информационе технологије и информације у електронском облику већ и на информације у свим могућим облицима и на свим медијима.
Оцењивање ризика у вези информација је основа за успостављање система менаџмента безбедношћу информација и представља његову основну карактеристику.

Поред ова два система, за банку и њену пословањејевеома битно да примењује и стандард **ISO 31000,** односно **систем менаџмента (управљања) ризиком.** Према ISO стандарду, "ризик је вероватноћа да ће се неки нежељени догађај десити као последица неког другог догађаја."

Систем менаџмента управљања ризиком омогућава банци идентификацију потенцијалних ризика као и предузимање адекватних мера за смањивање, ублажавање или елиминацију ризика. Такође, третира факторе који могу зауставити реализацију планираних задатака и самим тим спречава да дође до нежељених последица. Менаџмент ризиком покушава да предвиди проблеме и да испланира начине да смањи шансу за њихово избијање и ублажи последице могућих проблема.

Циљ банака је да остваре што већу контролу и управљање ризицима, што подразумева неколико фаза: процену ризика, управљање и контролу ризика и мониторинг ризика. Управљање ризиком подразумева примену сигурносних механизама и мера (бекаповање података, дигитални сертификат,инсталација заштитних зидова, антивирусна контрола, коришћење пинова, координацију интерне комуникације, вредновање и побољшање производа и услуга, примену мера за контролу ризика који се односе на спољне даваоце услуга и планирање непредвидивих околности.

Процес управљања ризицима у банци полази од пет међусобно повезаних елемената, односно фаза:

- идентификовање изложености ризику,
- оцена и процена ризика,
- контрола ризика,
- финансирање ризика и
- управљање ризиком.

Генерички приступ управљању ризицима, који наводи стандард ISO 31000:2009, пружа квалитетну основу за анализу, процену и обраду ризика.ISO 31000:2009 наводи да управљање ризицима у банкама треба да садржи следеће принципе[25]:

- учешће у стварању вишка вредности,
- саставни део осталих пословних процеса,
- учешће у доношењу одлука,
- систематичност, структурираност и правовременост,
- прилагођен потребама организације,
- организује и спроводи најбоље доступне информације,
- транспарентност,
- омогућавање сталног унапређења и побољшања организације.

Дакле, увођењем стандарда се у банкарским институцијама покривају заједнички елементи који омогућавају увођење нових технологија у различитим областима банкарског пословања.

Највеће користи које једна банка има од увођења и примене ISO стандарда су[26]:

- већа одговорност и свест запослених;
- већа лојалност купаца;
- боље искоришћавање времена и ресурса;
- повећање степена задовољења купаца;
- боља идентификација и следљивост производа и услуга;
- боље тржишне могућности;
- мањи губици и већи профит;
- континуирано обезбеђивање квалитета и ефикасности.

3.2. О Чачанској банци ад

Чачанска банка ад је основана и непрекидно послује од 1956. године. Органозована је као акционарско друштво и у банци је запослено 390 радника.

Поред тога што примењује савремени начин пословања, банка не одступа од основних банкарских принципа: сигурности, ликвидности и профитабилности.

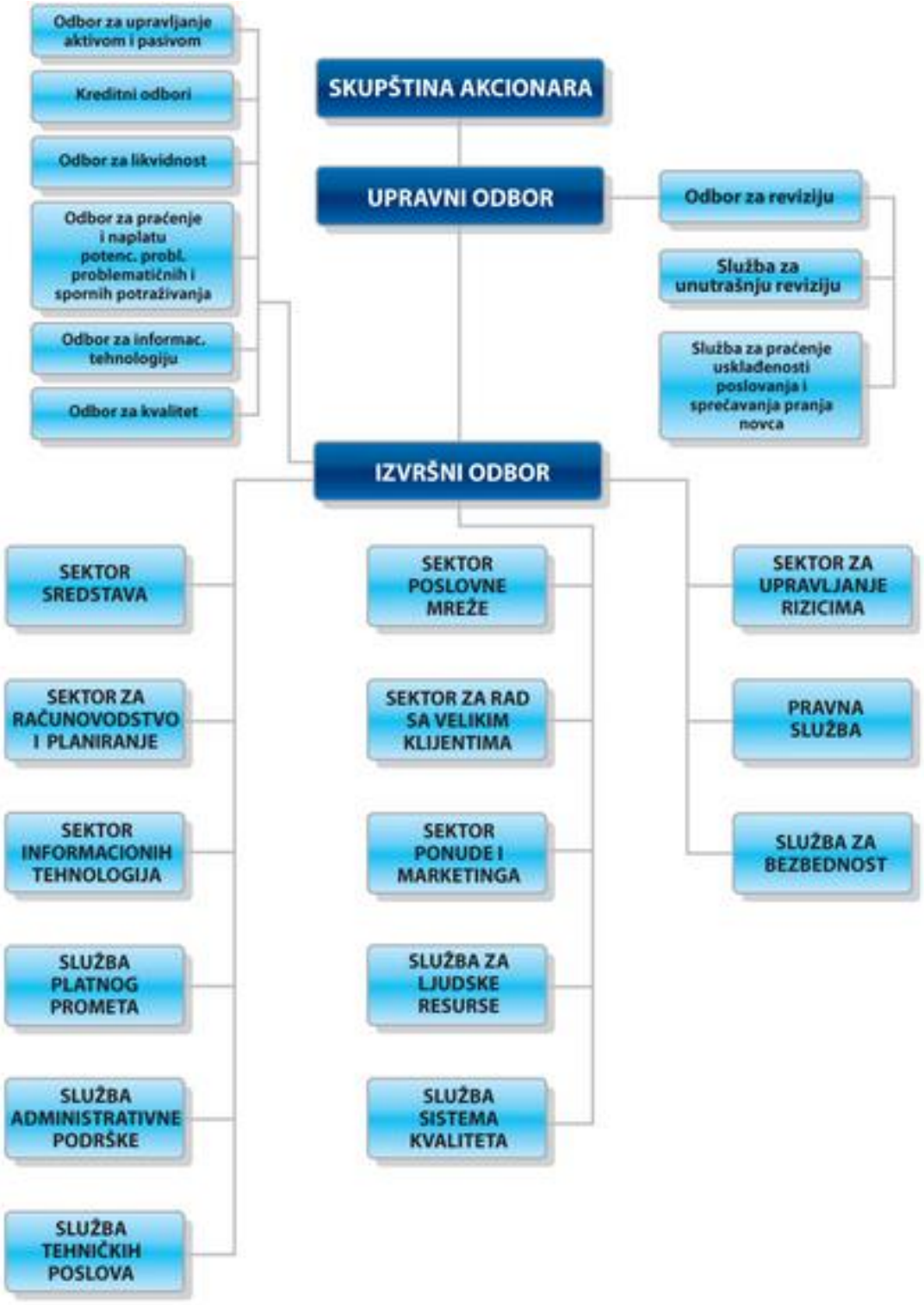
Чачанска банка ад је банка универзалног типа и пружа све врсте услуга становништву и привреди: прикупља новчане депозите, пружа услуге кредитирања, девизне, девизно-валутне и мењачке услуге, услуге платног промета у земљи и иностранству, брокерске услуге, услуге електронског банкарства, услуге издавања гаранција, платних картица (Visa, Dina) и сефова у закуп.

Чачанска банка ад је регионална банка и своју делатност обавља највише обавља на подручју западне и централне Србије. Веома је велики допринос Чачанске банке у финансирању развојних пројеката, технологије и реконструкције производних капацитета, школства, здравства, културе, информисања и спорта, индивидуалне и друштвене стамбене изградње.

Главни циљ Чачанке банке је да се позиционира као банка са значајним тржишним уделом и атрактивном позицијом у регионима западне и централне Србије. Банка се, пре свега, фокусира на сарадњу са клијентима малих и средњих предузећа, који има кључну улогу у привредном развоју Србије. Своје пословне циљеве Банка остварује на одговаран начин, уз трајну бригу о развоју друштвене заједнице и очувању животне средине.

У наредном периоду, Чачанска банка ће настојати да одговори на све изазове економске кризе, да повећа тржишно учешће и унапреди индивидуални приступ у пружању услуга малим и средњим предузећима и становништву. На овај начин створиће предуслове за експанзиван раст у посткризном периоду.

На слици 1 је приказана организациона структура Чачанске банке.



Слика 1. Организациона структура Чачанске банке

3.3. Интеграција система менаџмента квалитетом, базбедношћу информација и ризиком у процесу електронских плаћања у Чачанској банци ад

3.3.1. Мапа и метрика процеса и интеграција захтева стандарда

Опстанак и живот било које организације заснован је на потреби постојања система менаџмента, што произилази из природе и окружења у којем организација егзистира, а које је такво да нужно намеће потребу за ткз. интегрисаним системом менаџмента (IMS). Иако је сам процес увођења IMS-а у једну организацију веома осетљив, предности постојања једног таквог у банкарском систему омогућава вишеструке користи.[26]

Појам интегрисање значи комбиновање интерних система менаџмента у један систем.
Да би ови системи били интегрални део једне банке, треба да постоје компактне везе између компоненти и самих процеса, односно система.

Имајући то у виду, све компоненте треба да формирају једну целину за које постоје одређени разлози, а то су:[27]

- смањење понављања а уједно и трошкова,
- смањење ризика и повећање профитабилности,
- уравнотежење проблематичних циљева,
- елиминисање проблематичне одговорности и односа,
- померање оријентације на пословне циљеве,
- формализација неформалних система,
- хармонизација и оптимизација праксе,
- побољшање комуникације унутар организације и са околином,
- олакшавање обуке и развоја и
- повећање конкурентности.

Постојање система менаџмента квалитетом, безбедношћу информација и управљања ризиком се у финансијским институцијама и банкама посматрају као елементи интегрисаног система менаџмента и представљају универзално оруђе за решавање многобројних проблема и нежељених последица.Захтеви стандарда заинтеграцију система менаџмента квалитетомкоји су садржани у стандардима ISO 9001, ISO 27001 и ISO 31000 обезбеђују банци пословност и њену способност да испуни захтеве својих корисника и да тиме постане конкурентнија на тржишту.

Успостављање IMS-а у банци, уз помоћ којег ће се вршити ефикасно и ефективно управљање организацијом, подразумева да ће систем менаџмента бити постављен на бази процесног приступа. С тим у вези, кораци за успешно спровођење IMS-а у банци обухватају:

- идентификацију процеса рада и његово разлагање на активности,
- идентификацију претњи које се јављају у процесима,
- анализу утицаја претњи на перформансе банке,
- избор најпогоднијег алата за упоређивање утицаја више претњи и
- установљавање поступка праћења и вредновања ризика током дужег временског периода.

Усвајање процесног приступа у пословању јесте кључан аспекат иновирања процеса у банкама. Процесна оријентација у пословању задире у структуру, фокус организације, систем мерења, власничке и односе са корисницима. Једна од многобројних дефиниција процеса каже да је процес структурно уређен и мерном шемом опремљен сет активности, пројектован да произведе захтевани излаз намењен одређеном кориснику или тржишту. Сваки процес се разлаже на одређене подпроцесе.[28]

Сви процеси који се имплементирају у банци, морају да буду правилно мапирани јер мапирање пословних процеса даје јасан поглед на оно што се догађа у банци. Мапирање процеса представља поступак идентификације и успостављања релација између декомпоновања процеса. Пребацивање пословних процеса на папир даје добар поглед на целокупну слику пословања и отвараброjне могућности оптимизације, стварања нових модела рада и побољшања[29]. Једноставним приказом се сваки процес може довољно поједноставнити да би био јасан свакоме ко га посматра, а безда се изгуби основна идеја која је у темељима самог процеса.

Дакле, мапирањем пословних процеса се преноси пожељна пословна пракса из главе на папир. Резултат је мапа пословних процеса са приказаним редоследом одвијања процеса, а то је управо оно што банка жели као исход тако да свако ко погледа мапу може тачно да разуме шта треба да уради.

У Табели 2 приказана је шема процеса у Чачанској банци.

Група	***Процес***
Управљање	Планирање
	Организација и развој
	Управљање ризиком
	Маркетинг
	Управљање људским ресурсима
	Управљање капиталом
	Complience
Подршка	Набавка и продаја
	Рачуноводство
	Информационе технологије
	Правни и општи послови
Реализација	Доступност
	Штедња и депозити
	Пласмани и гаранције
	Платни системи
Мерење, праћење и унапређење	Праћење и мерење процеса и производа
	Интерна контрола иаудит
	Унапређење процеса и производа

Табела 2. Процеси у Чачанској банци

У раду ће бити приказано како се захтеви стандарда имплементирају на процес реализације услуге у Чачанској банци ад, односно конкретно како се захтеви стандарда ISO 9001, ISO 27001 и ISO 31000 имплементирају на процес електронских плаћања или E-banking-a у Чачанској банци ад.

Реализација услуге и процес реализације услуге се у Чачанској банци односи на управљање новчаним средствима и управљање активом и пасивом.

Управљање новчаним средствима представља управљање распоредом, односно диспонирањем свих новчаних средстава (у домаћој и страној валути) у складу са потребама унутрашњег и ино-платног промета, потребама за готовином у благајнама и трезорима банке, као и потребама за адекватним пласирањем средстава.

Управљање активом и пасивом Банке представља просец прилагођавања извора средстава потребама за кредитима, одржавања ликвидности и захтевима сигурности пословања уз минимизирање ризика за банку.

Процеси штедње и депозита се односе на депозитне послове (краткорочне и дугорочне) са правним и физичким лицима. Циљ процеса је прикупљање нових клијената, повећање извора-депозита, као и развој нових производа из области послова са становништвом и привредом и развој пословне мреже. Затим, иду процеси пласмана и гаранције. Циљ овог процеса ја да се ефикасном и свеобихвтаном применом процедура Банке обезбеди минимизирање кредитног ризика и оствари задовољавајући ниво профитабилности и ликвидности. Овим процесом се обезбеђује вишеструко плаћање кредитне функције Банке: по клијентима (привреда и становноштво), са рочног аспекта (краткорочног и дугорочног) и са валутног аспекта (у домаћој и страној валути), при чему се сваки кредит прати почев од одобравања до коначне наплате укључујући и управљање спорним кредитима.

Банка ову своју функцију обавља применом политике кредитирања која се односи на све ризичне елементне кредитирања, а то су: краткорочни и дугорочни кредити привреди и становништву, гаранције, скредитиви, менице, прекорачења (дозвољена и недозвољена) на рачунима дужника идр.

Улога процеса платни системи је да обезбеди поуздан, ефикасан и правовремени проток новца. Процес платни системи се састоји од следећих потпроцеса: ино платни систем, домаћи платни систем и платне картице.

Ино платни систем у Банци прихвата дневне налоге за плаћање од клијената и процесира их кроз систем међународног промета, чиме се налози ефективно и извршавају. Поред тога, врше се послови књиговодства који обухватају и евиденцију пословних промена на рачунима ино банака.

Домаћи платни промет подразумева прихватање налога од клијената и њихово просецирање кроз систем жиро клиринга или RTGS систем. Ово подразумева и њихово књиговодствено евидентирање и вођење пословних промена на рачунима клијената. Прихватање дневних налога омогућено је како на шалтерима Банке тако и путем E-banking-a.
Увођењем у неку од банкарских/картичних асоцијација Банка стиче право на издвавање платних картица, које се могу употребљавати само унутар државе или изван ње. Пословање овим картицама се обављњ у складу са стандардима одговарајуће асоцијације (Master Card Europe, VISA System и др).

Метрика процеса реализације услуга у Чачанској банци:

- Ефикасно управљање активом и пасивом,
- Ефективни депозитни послови,
- Кредитни ризик,
- Висок ниво профитабилности

Слика 2. Метрика реализације услуга у Чачанкој банци

У даљем раду ће бити приказано како се захтеви стандарда система менаџмента кавлитетом, безбедношћу информација и ризиком примењују на процес електронских плаћања у Банци, односно E-banking-a.

Свака банка па и Чачанска, у данашњем динамичном банкарском окружењу,настоји да на тржишту понуди што разноврсније производе и услуге и тако постане што конкурентнија на тржишту и придобије што више корисника. Једна од значајних конкуренстких предности је управо развој система електронских плаћања који данас постају потпуно нови модел успостављања односа између банке и клијента. Развој интернета, пре свега, довео је до тога да банке све више улажу у развој да се каналима електронских система плаћања омогући услуга клијенту с једне, али и олакшавање и поједностављење обављање те услуге, с друге стране.

Електронско банкарство подразумева да се на најсавременији начин, без папирног документа обављају и обрађују банкарске трансакције и шаљу даље у базу података. Под електронским банкарством се подразумева електронска размена информација између банке и њеног клијента. Овакав облик пословања омогућава да се трансакција обави на начин да омогућава и олакшава брзо повезивање клијената на великој удаљености.

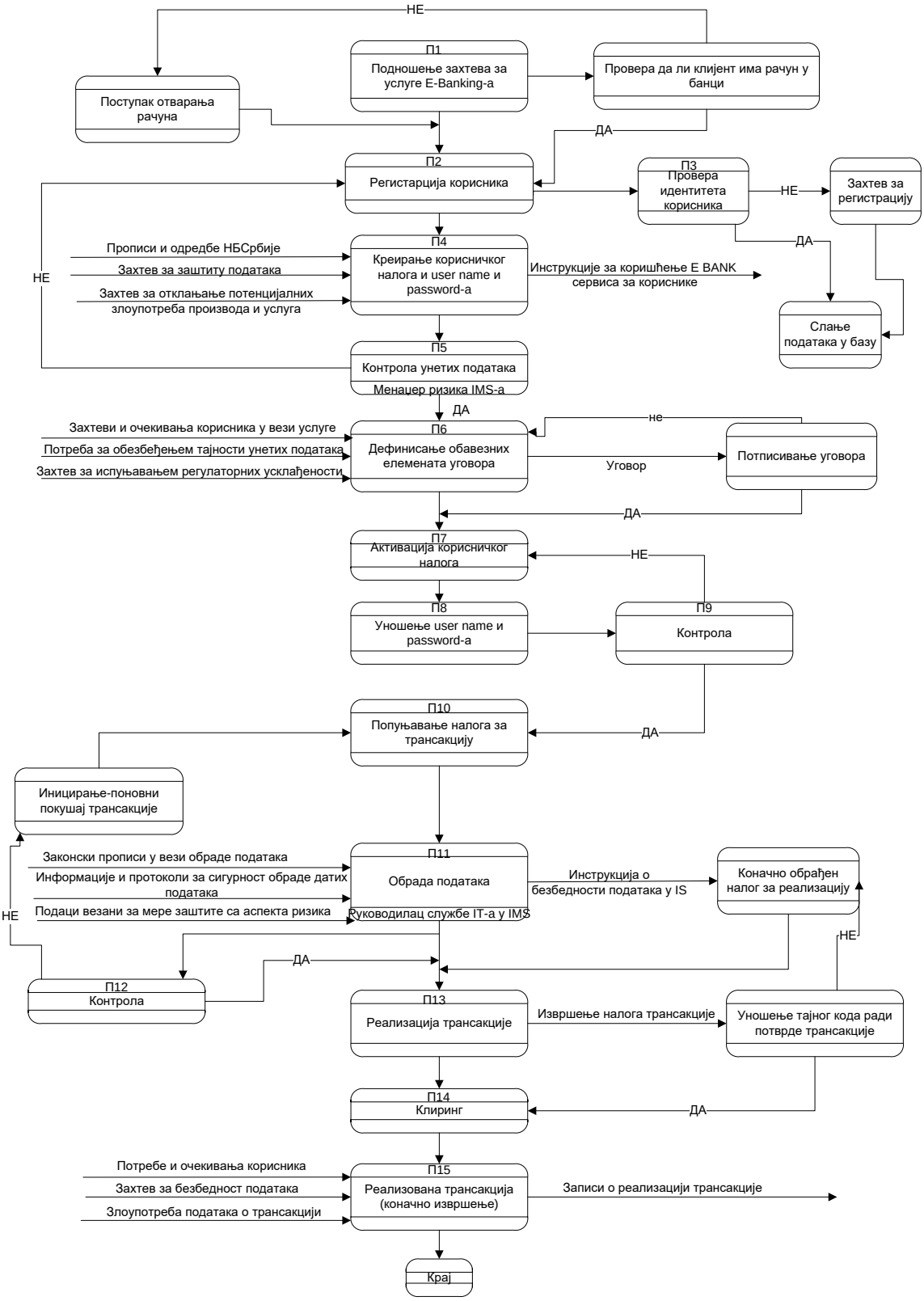
На развој електронског банкарства највише су утицала три битна фактора:

- Висок ниво развоја рачунарске технологије, погодне за примену у финансијским институцијама, што је за директну последицу имало концентрацију високо стручних и образовних кадрова у банкарским институцијама,
- Комплексна финансијска структура, карактеристична за велики број финансијских институција,
- Висок степен дерегулације на домаћем и међународном тржишту, која је појачала оштру конкуренцију између банака.

Бројне су предности развоја система електронског банкарства, а оне се пре свега огледају у смањењу папирне документације, затим нема обавезе да се физички долази у банку ради обављања трансакције, брзини преноса новца и тако даље.

Менаџмент Чачанске банке је донео одлуку да почне улагања у развој система електронских плаћања, јер је увидео да ће тиме моћи да:

- најпре задржи постојеће и придобије нове кориснике својих услуга,
- да омогући клијентима смањење трошкова,
- да адекватније управља ризиком у пословању и
- да коришћењем информационе технологије кроз развој електронских система плаћања стекне одговарајућу конкурентску предност.



Слика 3. Шема интеграције захтева стандарда на процесу електронског банкарства у Чачанској банци.

Процес покретања и коришћења електронског банкарства започиње подношењем захтева за услуге e-banking-a од стране корисника у експозитури Банке. Како би корисник могао да започне коришћење ове услуге потребно је да буде регистрован у Банци као власник текућег рачуна.Уколико корисник непоседује рачун у банци, започиње процедура отврања рачуна, након чега следи регистрација и провера идентитета корисника. Провером идентитета подаци се даље шаљу и евидентирају у базу података Банке.

Процес П4 на слици представља просец креирања корисничког налога и user name и password-a (корисничко име и лозинка) као основе за коришћење е банк услуге. У овом просецу Банка је интегрисала захтев стандарда система управљања квалитом (захтев 4.2 стандарда) који се односи на поштовање законских одредби, које прописује Народна банка Србије, везаних за поштовање начела која су прописана Законом о заштити корисника финансијских услуга, у којем се између осталог захтевају минимални стандарди упознавања корисника са свим значајним карактеристикама за коју се коришћењем е-банк услуге определио.

Други улаз у процес представља захтев стандарда система управљања безбедношћу информација као веома важан сегмент и односи се на све оно што је прописано Законом о безбедности података (захтев 4.3 стандарда), а суштински и практично се своди на то да банка информише клијента за које сврхе се његови лични подаци могу употребити, као и да он својим потписом пристаје и практично банци одобрава коришћење његових података.

Трећи улаз се односи на зехтев стандарда система управљања ризиком (захтев 5.6 стандарда) и односи се на предвиђање минималних карактеристика из којих се кориснички налог мора састојати како као такав не би био лак за потенцијалну хакерску или било какву другу злоупотребу.

Ова три значајна улазна захтева се међусобно интегришу у процес креирања корисничког налога из чега се након успешне регистрације кориснику даје сет упутстава и инструкција које практично описују начин на који ће он у будућности да користи ову услугу, као и услова које је прихватио, а који се заправо односе на горе поменуте улазне захтеве у процес.

Након завршетка овог процеса, менаџер ризика IMS-a врши проверу и контролу и тако даје одобрење за наставак поступка.

Уговор који произилазиис просеца П6 је један од најбитнијих ставки у окриву овог процеса. Њему предњачи потписивање уговора о коришћењу услуге. Како би се уговор између банке и корисника потписао, Банка мора да дефинише обавезне елементе уговора, што се заправо односи на дефинисаање уговорних обавеза између Банке и клијента. Суштина овог поступка је да клијент приказе банци каква су његова очекивања везана за

коришћење услуге (захтев 5.2 стандрда), затим да се кроз овај поступак као битна улазна компонента дефинишу заштите података (захтев 5.2 стандарда) које проистичу из услуге, али и да се са аспекта безбедности и ризика (захтев 5.5 стандарда) дефинише какве је активности потребно спровести на начин да се отклоне могуће злоупотребе.

Након што је уговор потписан, корисник може да покрене апликацију електронског банкараства на свом рачунару и то активирањем корисничког налога и уношењем user name и password-а. Провером и потврдом унетих података одобрава се коришћење, након чега корисник може да крене у поступак плаћања и то попуњавањем налога за трансакцију.

Када се сви неопходни и жељени подаци унесу, приступа се процесу обраде података П11. Процес обраде података се састоји од три улазна захтева. Захтев из система управљања квалитетом се односи пре свега на испуњење законских прописа у вези обраде података (захтев 5.1 стандарда). Ова улазна карактеристика прописана је Законом о минималним стандардима за управљање информационим системом при чему је посебан акценат стављен у том закону управо на дефинисане стандарде за обраду података, чијим ће се поштовањем обезбедити побољшан процес са аспекта квалитета.

Као друга значајна карактеристика тј.улаз у процес односи се на то да су захтеви стандарда који се односе на обраду података прописани одговарајућим протоколима који дефинишу поштовање сигурности обраде података (4.4 стандарда), док са треће стране постоје одређени захтеви које дефинишу и поступак минимизације ризика огледани кроз поштовање и спровођење мера заштите (6.2 стандарда). За надгледање поступка овог процеса задужен је руководилац службе IT-а у IMS-у. Сви захтеви и обрађени подаци у овом процесу се дефинишу у инструкцији која заправо даје основне мере о безбедности датих података у информационом систему.

Уколико се процес верификује као исправан, следи реализација и извршење дате трансакције.

Клиринг представља размену и обраду међубанкарских налога за плаћање и заправо он је потрвда да је извршено плаћање.

Поступак коначне реализације трансакције П15 пре свега као улазну карактеристику са аспекта квалитета има да покаже колико је заиста клијент задовољан услугом коју је одабрао да користи (8.2.1 стандрда). То практично треба да прикаже које су све значајне предности коришћења услуге, које се огледају у свим њеним једноставностима и ефикасностима. У савременом онлине пословању може се догодити и одређена крађа података, тако да остаје да се битна пажња посвети и отклањању таквих ризика, стога је захтев за безбедност података веома важан (9.1 стандарда).

Интеграцијом ова три улаза у процес завршетка транакције као резултат даје излазне варијанте које се односе на све идентификоване записи о реализацији трансакције, који ће имати, на пример, као последицу потенцијалну рекламацију клијента у случају да један о три улазна парамента није био у потпуности испоштован или мерење задовољења клијента производом или услугом и др.

Дакле, успешно имплементиран интегрисан систем управљања према захтевима стандарда ISO 9001, ISO 27001 и ISO 31000 даје уноси у пословање Банке један опште прихваћен начин рада којим се осигурава садашњим и будућим купцима или партнерима очекиван квалитет производа или услуга.

Када говоримо о пословању Чачанске банке са аспекта квалитета и стандарда ISO 9001, она је увођењем система електронских плаћања успела да знатно прошири лепезу својих услуга које се нуде клијентима, било да се ради о физичким или правним лицима.

Услуге које је Чачанска банка имплементирала, а које се односе на системе развоја елетронских плаћања за физичка лице и правна лица су:

- упит у стање на рачунима путем мобилног телефона,
- добијање обавештења о сваком приливу или одливу који настане на рачуну,
- могућност увида у стање рачуна путем ВЕБ сајта банке,
- могућност обављања плаћања свих рачуна преко е-налога,
- купопродаја девиза,
- преглед промета по свим рачунима у одређеном временском периоду,
- преглед стања курса по валути на жељени дан,
- преглед свих извршених плаћања,
- преглед извода по рачунима,
- могућност наручивања чекова,
- могућност подношења захтева за кредит,
- могућност обављања налога плаћања кроз платни промет,
- могућност најаве подизања готовине или најаве девизне трансакције итд.

Да би клијент банке могао да користи ове услуге, довољно је да се региструје у банци као корисник ових услуга. Регистрација је веома једноставна и може се спровести у свакој организационој целини Банке. Информације које су битне за сам поступак регистрације се у најкраћем могу свести на следеће:

- Име и презиме клијента или назив фирме,
- ЈМБГ или матични број фирме,
- Број пословног рачуна,
- Име и презиме овлашћених лица за заступање,
- Улица и број и место пребивачишта фирме/овлашћених лица,

- Емаил адреса,
- Број мобилног или другог телефона.

Све ове услуге које су имплементиране дају велику квалитативну и компаративну предност, а то је пре свега да корисник не мора да долази у банку ради обављања свих ових трансакција.Иницијални долазак у банку је потребан само ради прве регистрације и евентуално измене одређених података. То значи да би клијент банке могао да користи услуге електронског банкарства, потребно је да поседује рачун у банци, а да се након тога и региструје за корисника услуга система електронских плаћања.

Значајна предност је и та што клијент ове трансакције може обављати у било ком временском периоду, а то значи 24 сата дневно и 7 дана у недељи, чиме је значајно скраћено време које у супротном мора провести у банци ради ових трансакција, где је додатно ограничен радним временом.

Дакле, једноставност и ефикасност у обављању трансакције и уштеда у времену и новцу представља главне компаративне предности коришћења система електронских плаћања.

Савремени развој интернет услуга и заједно са тиме система електронских плаћања значајно је подигао свест о јачању безбедности информација.

Када говоримо о систему електронских плаћања, у савременом банкарском пословању бележи се значајан пораст оваквог вида трансакција у платном промету. То с друге стране доводи до повећавања ризика, имајући у виду да разни интерни и чешће екстерни фактори покушавају да изврше одређену злоупотребу.

Због тога се најчешће уводе одговарајуће додатне мере заштите које би онемогућиле да неко лако дође до података.

Чачанска банка је ради спречавања настанка ризика који настају од потенцијалног хакерисања података увела одређене мере заштите које се огледају у следећем:

- Шифровање података – овај вид заштите се користи код корисничких налога код којих је потребна посебна идентификација; данас се све више постављају одређени минимални нивои карактера из којих се шифра за идентификацију мора састојати. Такође, за одређене трансакције постоји и додатна заштита-аутентификација, која се односи на верификацију идентификације.
- Коришћење дигиталног потписа – овај вид се користи за аутентификацију интегритета поруке, у циљу контроле да ли је иста промењена од пошиљаоца до примаоца. Практично, када прималац неког податка добије дигитално потписану поруку, он уз помоћ алгоритма верификује потпис и на тај начин утврђује аутентичност корисника и поруке и на овај начин минимизира оперативни ризик.

- Коришћење дигиталног сертификата – овај вид заштите је такође заступљен у банци у циљу заштите оних који послују преко интернета. Банка има уговор са овлашћеном фирмом, која клијентима банке издаје ове сертификате. Овај систем заштите функционише тако што се на интернету утврђује аутентичност клијента банке који обавља трансакцију.

Паралелно са развојем интернета, који је омогућио развој електронских система плаћања, постоје и ризици који прате овај начин обављања банкарских услуга. Ови ризици прате сваку појединачну трансакцију и као такви могу значајно угрозити банкарско пословање.

У најкраћем ови ризици се могу посматрати са следећих аспеката и то:

- Оперативни ризици,
- Репутациони ризици,
- Системски ризици,
- Законски ризици,
- Ризици од напада криминогених активности и
- Ризици који настају из међународних трансакција.

У раду ће пажња бити посвећена оперативним ризицима који произилазе из трансакција које настају електронским путем.

Оперативни ризик је ризик могућности настанка негативних ефеката на финансијски резултат и капитал банке услед ненамерних и намерних пропуста у раду запослених, неодговарајућих унутрашњих процедура и процеса, неадекватног управљања информационим и другим системима у банци као и услед наступања других спољашњих непредвиђених догађаја.

У Чачанској банци постоји посебно одељење које се бави оперативним ризицима, односно њиховим евидентирањем, мерењем и проценом њиховог утицаја на капитал банке. Одељење се састоји од четири запослена на челу са руководиоцем. За адекватан рад, Банка је набавила одговарајући софтвер који се користи за унос оперативних ризика од стране свих запослених. Ова апликација је доступна на линку интерног сајта и служи као алат за укупно управљање овим ризицима. Начин рада са овом апликацијом је прописан одговарајућом инструкцијом за рад и њу су у обавези да користе сви запослени код којих је одређени оперативни ризик и настао. Одлукама органа банке, дефинисан је материјално значајан износ сваког догађаја који се по основу оперативног ризика евидентира. То практично значи да запослени кроз апликацију уносе сваки догађај који по основу оперативног ризика у бруто износу прелази 10.000 динара или је могао да у бруто износу пређе тај износ.

Када говоримо о системима електронских плаћања, процедуром је прописано и да банка идентификује изворе настанка оперативних ризика, а који могу бити следеће категорије догађаја:

- Прекиди у пословању,
- Грешке у системима банке,
- Извршење трансакција, испорука и управљање процесима у банци,
- Разне интерне преваре,
- Екстерне преваре упадом у информациони систем банке,
- Крађа података и информација.

Систем управљања квалитетом у Чачанској банци и процедурама и упутствима којима су документовани процеси рада, треба да се утврди обавеза испуњења одговарајућих процедура о квалитету као подлога за извођење активности које се јављају као резултат испуњења тих процедура.

Највише руководтсво у Чачанској банци, директор и руководиоци организационих целина своју опредељеност ка успостављању, примени и сталном унапређивању ефективности система управљања квалитетом манифестују путем:

- Јасно дефинисане организације процеса рада и пословања у оквиру које је утврђен значај и одговорност руководства и свих запослених,
- Утврђене основне – примарне политике функције упрваљања предузећем и политика свих организационих целина у подручју унапређења квалитета, процеса рада и пословања,
- Дефинисаних циљева квалитета и утврђене потребе за доношење и контролу планова њиховог остварења,
- Тимског рада руководства предузећа и руководства организационих целина, институционализованог у виду менаџерских тимова,
- Сталног преиспитивања система управљања квалитетом у виду редовних активности и активности које се изводе по потреби на осниву анализа проблема у процесима рада и
- Сталне бриге о ресурсима неопходним за извођење процеса рада.

Сви процеси рада и пословаља су у Банци усмерени ка:

- Задовољењу потреба, захтева и очекивања купаца/корисника,
- Остварењу партнерских односа са добављачима и другим пословним партнерима и
- Обезбеђивању високог нивоа квалитета услуга/проивода и прецеса рада и посливања који обезбеђују економске ефекте.

3.3.2.Процедуре за процесе које одговарају на све меродавне захтеве стандарда

Неке од процедура које одговарају на све меродавне захтеве стандарда приказане су у тексту који следи.

Процедура отварања рачуна у банци

Процедура за отварање рачуна у Чачанској бацни одређује услове под којима банка отвара и води рачуне клијената. Банка клијенту отвара вишевалутни рачун на основу његовог захтева и уговора, односно Уговора о отварању и вођењу рачуна који банка закључује са клијентима и општих пословања, као и на основу неопходне документације предвиђене важећом регулативом интерним правилима банке.

Банка отвара и води рачуне који могу бити текући или депозитни (неорочени, орочени, са посебном наменом или без намене), при чему се сваком рачуну у тренутку отварања додељује јединствени број. Клијент потписује стандардни захтев за отварање рачуна и доставља банци сву неопходну документацију утврђену позитивно правним прописима и интерним правилима банке. Клијент може путем *Onlinebanking*апликације или у писменој форми овластити једно или више лица да располажу средствима са рачуна, са тачно назначеним ограничењима, уколико таквих има.

У случају било које измене или подуне ове процедуре, банка обавештава клијента који је обавезан да без одлагања достави банци неопходну документацију којом се доказује наведена промена. Измене и допуне података ће бити правно обавезујуће за банку од момента достављања неоподне документације банци. По приспећу оваквог обавештења, раније дата овлашћења престају да важе.

Процедура издавања платних картица

Ова процедура дефинише да картица може бити издата физичком или правном лицу за које Чачанска банка утврди да испуњава услове кредитне способности. Издавање додатних картица условљено је потписивањем приступнице од извршног директора или овлашћеног лица фирме, за сваког појединачног корисника.

Подносилац захтева за издавање картице доставља попуњену и потписану приступницу банци. Потписом приступнице, подносилац захтева прихвата опште услове.

Кредитна способност утврђује се посебноим актима банке.Подносилац захтева је овом процедуром одговоран за тачност свих података наведених у захтеву за издавање, као и за тачност свих података датих у комуникацији са банком. Такође, картицу и пин преузима лично корисник.

Приликом преузимања, корисник је обавезан да потпише картицу. У супротном, он анеће бити важећа. Банка може од подносиоца захтева затражити и додатне податке и документацију и обавити проверу података. Одлуку о издавању и висини одобреног износа*charge* или *revolving*кредита доноси банка, без обавезе образложења одлуке подносиоцу захтева.

Процедура за заштиту података

Процедура за заштиту података је једна од најважнијих у Чачанској банци. Подношењем захтева за коришћење производа и услуге банке, клијент даје изричиту сагласност да банка има право да прикупља, обрађује, чува и користи његове личне податке у циљу релаизације пословног односа са банком, извршења обавеза банке у складу са прописима и за сврје које банка у обављању своје делатности сматра неопходним, као и да те податке и све друге податке који се сматрају банкарском тајном може учинити диступним Народној банци Србије, Кредитном бироу Удружења банака Србије, Националној корпорацији за осигурање стамбених кредита, Форуму за превеницју злоупотреба у кредитним пословима и са платним картицама при Провредној комори Србије, спољном ревизору банке, чланицама групе, као и свим осталим органима којима је банка по закону дужна да достави одоговарајуће податке или са којима је банка закључила уговор о заштити поверљивости таквих података.

Овом процедуром се клијент упознаје са правом да буде обавештен о личним подацима који се о њему воде, да има право на увид у исте, као и на исправку нетачних података. Такође, Чачанска банка на основу овлашћења прибавља извештаје од Кредитног бироа и других институција у којима су садржанио подаци о клијенти, односно подаци о клијентовој задужености.

Чачанска банка овом процедуром може тражити од других банака чије је услуге клијент користио, извештај са подацима о клијентовом дотадашњем начину коришћења услуга. Банка обрађује податке о клијенту (личне податке, податке за контакт са клијентом, финансијске податке, податке о пореклу средстава клијента и слично), само у сврху постизања легитимних циљева и само у оквиру потребном ради испуњавања обавеза предвиђених важећим прописима или уговорних обавеза, ради пружања услуга клијентима или посредовања и пружању услуга клијентима, за реализацију и

администрирање производа и услуга пружених клијенту, за реализацију наплате потраживања и ради заштите од повреда права банке.

Ова процедура одређује које личне податке клијента узима банка. Такође, које личне податке клијента користи у сврху спровођења статистичких истраживања и анализе тржишног удела групе клијената, производа и услуга и осталих финансијских показатеља, као и у циљу извештавања и управљања ризицима.

Процедура мониторинга реализације услуга

Извршиоци и руководиоци услугама реализују и прате процесе мониторинга услуге. Процес се одвија у складу са редоследом фаза и операција датих у оперативном плану и евиденцији извршених операција. Непосредни извршиоци спроводе мере прегледа пре и за време мониторинга услуга у банци.

Код сложенијих операција технолошки процес је дефинисан као под-процес просеца производње радним упутствима (референцирана у тачки 4.2 ове процедуре), која дефинише активности везане за одређена радна места или технологијама које дефинишу операције у изради производа.

Мониторингом карактеритика реализације услуга се врши попуњавање евиденције извршених операција у који се уносе подаци о реализованим операцијама. Извршиоци попуњавају евиденцију реализованих операција.

У процесу реализиације услуге дефинисани су следећи процесни параметри који се мере и прате у складу са дефинисаним индикаторима циљева квалитета:

- Временско оставрење планираних фаза процеса,
- Реализоване количине услуга,
- Степен искоришћености,
- Степен усаглашености,
- Трошкови квалитета,
- Степен искориошћености радног времена,
- Продуктивност.

Процедура контроле неусаглашености

Овом процедуром се прописује поступак контроле неусаглашености, дефинишу активности и начин њиховог спорвођења у случајевима појаве неусаглашености, од уочавања до њиховог решавања, како би се осигурало да се наусаглашена услуга која не

одговара захтевима идентификује и контролише ради спречавања њене ненамерне употребе или испоруке, односно како би се кориговала грешка уколико се она појави.

Сврха ове организације је дефинисање активности и одговорности за решавање идентификованих неусаглашених услуга. Ова процедура треба да одезбеди:

- Предузимање мера или акција за отклањање утврђених неусаглашености у реализацији услуга,
- Одобравање њиховог коришћења, примене или прохватања на основу накнадне дозволе за одступање,
- Предузимање мера или акција за спречавање његове планиране употребе или примене,
- Предузимање мера или акција које одговарају последицама или могућим последицама неусаглашености када се открије неусаглашена услуга после испоруке или пошро су употребљени, односно реализовани.

4. Закључак

У оквиру овог мастер рада дат је опис и преглед система менаџмента квалитетом, безбедношћу информација и ризиком у пружању финансијских услуга, затим процес мапирања као и интрегација поменутих стандарда на примеру Чачанске банке. Генерално, сама стандардизација подразумева примену осмишљеног система стандарда за унапређивање квалитета услуга. У примени стандарда или норми полази се од тога да стандард означава одређен квалитет. Сертификација интегрисаног система управљања квалитетом према поменутим стандардима осигурава и даје потврду усклађености пословања с међународно признатом нормом, доводи до већег поверења будућих корисника, даје бољу представу маркетиншке промоције производа и услуга као и бољу конкурентност на тржишту.

Стандарди у великој мери имају позитиван утицај на већину аспеката живота. Они обезбеђују жељене карактеристике производа и услуга као што су квалитет, позитивно деловање на животну средину, безбедност, поузданост, ефикасност и заменљивост.

ISO 9001 прецизира основне захтеве за систем управљања квалитетом, које организација мора да испуни како би показала своју способност да своје производе доследно производи, који укључују услуге, чиме се повећава задовољство корисника и испуњавају важеће законске регулативе.

Заштита и безбедност информација за данашњи свет бизниса је много важнији него икада раније. Данас, бизнис зависи од информационих технологија, комуникација путем мрежа, као и бежичних и мобилних комуникација. Стога, ISO/IEC 27001 је међународни стандард који својим захтевима дефинише систем менаџмента безбедношћу информација, чији је примарни циљ информационо-физичко-техничка заштита предузећа.

Систем менаџмента ризиком директно утиче на побољшање процеса доношења одлука, нарочито оних који носе велике ризике, омогућавајући руководиоцима да боље разумеју окружење и ризике, да заштите себе и своју организацију и на тај начин постигну постављене циљеве.

Дакле, сви ови системи менаџмента који се имплементирају у банкама, морају да буду правилно мапирани и управо у трећем делу рада јасно и види да мапирање пословних процеса даје јасан поглед на оно што се догађа у банци.

Интеграција менаџмент система представља природан пут, који формално задовољава различите стандарде, а истовремено подиже ниво способности организације и њено приближавање циљевима изврсности. Побољшање свих перформанси организације има за циљ остваривање најважнијег задатка сваког пословања, а то је опстати на тржишту.

Литература

[1] Андре, П. ISO 9000 Оцењивање система квалитета, Београд, 1996.

[2] Вујановић, Н. Стандард ISO9001:2000 Приказ, тумачење и примена, Београд, 2007.

[3] Awad, E. M., Ghaziri, H. M., Knowledge Managment ISO 9001 for Small Businesses — What to do, Pearson EducationInternational, 2004.

[4] Балабан Н., Ристић Ж., Дурковић Ј., Трнинић Ј., Информациони системи у менаџменту, Савремена администрација, Београд, 2002.

[5] Хелета М., Менаџмент квалитета, Универзитет Сингидунум, 2008.

[6] Beasley, J. S., Networking. Upper Saddle River, NJ: Prentice-Hall, 2004.

[7] Живковић,Н., Интегрисани системи менаџмента, Факултет организационих наука, Београд, 2012.

[8] Радојевић,Р., Инжењеринг квалитета, Београд, 1997.

[9]Системи менаџмента квалитетом, Захтеви–SRPS ISO 9001, Институт за стандардизацију Србије, 2008.

[10] Ђорђевић,Д., Ћоћкало Д., Управљање квалитетом, Технички факултет Михајло Пунин, Универзитет у Новом Саду, 2007.

[11] ISO/IEC 27001 — Information technology — Security techniques —Information security Management Systems — Requirements

[12] Daniels, C., Information Technology, The Management Challenge, Addison-Wesley, 1994.

[13] Cash, J. Jr, McFarlan, W., McKenney, J., Applegate, L., Corporate Information Systems Management 3rd ed., Harvard Business SchoolPublishing, Boston, 1992.

[14] Ђукановић,С., Управљање финансијским ризицима, Нови Сад, 2009.

[15] Симић,С., Управљање ризицима и континуитет пословања, ISO 31000.

[16] Вулановић,С., Развој општег модела за имплементацију интегрисаног система менаџмента на основу процене ризика у просецима организације, Докторска дисертација, Нови Сад, 2014.

[17] Вујановић, Н., Основни принципи и методологија интегрисања система менаџмента. Квалитет, 2009.

[18] Seuring, S., Miler, M., Standardization like support, Journal of Production, Volume 16 Issue 15, 2008.

[19] Бараћ С., Стакић Б., Хаџић М., Иваниш М., Практикум за банкарско пословање, Универзитет Сингидунум, Београд, 2007.

[20] Хаџић М., Банкарство, Факултет за финансијски менаџмент и осигурање, Београд 2010.

[21] Арсовски, З., Арсовски С., Савовић И., Систем менаџмента квалитетом у ITC огранизацијама, Квалитет, 2008.

[22] Claessens S., Glaessner T., Klingebiel D., Electronic finance, A new approach to Financial Sector Development, Word Bank, 2002.

[23] Ивковић, М., Милошевић С., Субић З., Добриловић Д., Електронско пословање, Технички факултет Михаило Пупин, Зрењанин, 2005.

[24] Новаковић, J., Електронско пословање, Мегатренд, Београд, 2005.

[25] Вуковић, Д., Принципи управљања ризиком за електронско банкарaство, Београд 2007.

[26] Черепналковска С., Модел унапређења интрегрисаног система менаџмента на основу ризика, Докторска дисертација, Нови Сад, 2016.

[27] Вулановић, С., Развој општег модела за имплементацију интегрисаног система менаџмента на основу процене ризика у просецима организације, Докторска дисертација, Нови Сад, 2014.

[28] Арсовски, С., Менаџмент процесима, Машински факултету Крагујевцу, 2007.

[29] Арсовски, С., Мапирање пословних процеса, Машински факултет у Крагујевцу, 2010.

[30]Новићевић,,Б.,Управљање пословним процесима као изазов управљачком рачуноводству. 41. симпозијум Савеза рачуновођа и ревизора Србије, 2010.

[31] Каровић, М., Комазец М., Управљање ризицима као предуслов за интегрисаног менаџмент система у организацји, Центар за обуку студената КоВ, Београд, 2009.

[32]Група аутора, Управљање информационим технологијама – Смернице за безбедност података и стандард ISO 17799, Београд, 2004.

[33] Каровић, М., Комазец М., Управљање ризицима као предуслов за интегрисаног менаџмент система у организацји, Центар за обуку студената КоВ, Београд, 2009.

[34] Павићевић С., Модели засновани на управљању ризиком применљиви уновој верзији стандарда ISO 9001:2015, ConsultADQMd.o.o., Београд,

[35] ISO 31000:2009 Менаџмент ризиком- Принципи и упутства

[36]Evgeny Avanesov, RISK MANAGEMENT IN ISO 9000 SERIES STANDARDS, International Conference for Risk Management and Management, Geneva, 2009.