UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

# ANALIZA INFORMACIJSKE REŠITVE ZA PREPREČEVANJE NEZAKONITIH BANČNIH TRANSAKCIJ V IZBRANI BANKI

Ljubljana, september 2016 ALEKSANDER KNEZ

# IZJAVA O AVTORSTVU

Podpisani Aleksander Knez, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza informacijske rešitve za preprečevanje nezakonitih bančnih transakcij v izbrani banki, pripravljenega v sodelovanju s svetovalcem prof. dr. Mirom Gradišarjem.

IZJAVLJAM

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študenta:_____

# KAZALO

## KAZALO SLIK

# UVOD

Pranje denarja je proces preoblikovanja kaznivih dejanj v domnevno zakoniti denar ali druga sredstva. Takšen denar prihaja iz nelegalnih poslov, kot so: trgovanje z mamili, orožjem, davčne utaje itd. Motiv pranja denarja je skriti denarna sredstva pred organi pregona, konkurenco, kreditorji, poslovnimi partnerji in drugimi (Šeme, 2007).

Banka je v splošnem dolžna opraviti običajni pregled stranke. Sicer pa mora zakonskim zahtevam ustrezati tudi banka. To področje ureja Zakon o preprečevanju pranja denarja in financiranja terorizma (v nadaljevanju ZPPDFT). ZPPDFT predvideva tudi dve posebni obliki pregleda strank, in sicer: poenostavljeni in poglobljeni pregled (Banka Slovenije, 2008).

Za stranke, ki predstavljajo povečano tveganje, se zahteva izvajanje poglobljenega pregleda. Banka s tem zagotavlja dodatne kontrole zaradi ustreznega obvladovanja večjih tveganj, ki jih predstavlja taka stranka. V ZPPDFT so tudi izrecno navedeni primeri, ko je banka dolžna opraviti poglobljeni pregled stranke. Banka mora opraviti poglobljeni pregled stranke tudi v primerih, ko na podlagi lastne analize tveganosti oceni, da gre za bolj tvegano stranko (Ur. l. RS, št. 60/2007).

V prizadevanju za odkritje potencialnega pranja denarja finančne institucije uporabljajo različne programe za preprečevanje pranja denarja. To so AML (angl. *anti-money laundering,* v nadaljevanju AML) programi za preprečevanje pranja denarja. Programi naj bi učinkovito pregledovali stranke (Cox, 2014).

AML programska oprema se uporablja v finančnih institucijah za izpolnjevanje zakonskih zahtev. Obstajajo štiri osnovne vrste programske opreme, ki omogočajo preprečevanje pranja denarja (Cox, 2014):

- spremljanje transakcij – to so nadzorni sistemi, ki se osredotočajo na identifikacijo vzorcev sumljivih transakcij, kar lahko vodi v prijavo sumljivih poročil, SAR sistemi (angl. *Suspicious Activity Reports*), ali sumljivih transakcij, STR sistemi (angl. *Suspicious Transaction Reports*),
- poročanje o valuti transakcij – CTR sistemi (angl. *Currency Transaction Reporting*), ki se ukvarjajo z velikimi denarnimi transakcijami,
- upravljanje identitete – preverijo različne negativne sezname, na primer OFAC (angl. *Office of Foreign Assets Control,* v nadaljevanju OFAC), in predstavljajo začetek spoznavanja strank,
- programi za zagotavljanje skladnosti – pomagajo podjetjem, da izpolnjujejo predpisane zahteve AML.

AML je prišel v ospredje po napadih 11. septembra 2001 v Združenih državah Amerike.

Vsaka programska oprema na ključ deluje nekoliko drugače. To so klasični moduli, ki so prisotni v AML programski opremi (AML, 2016):

- spoznavanje strank,
- spremljanje transakcij,
- poročanje o skladnosti,
- opozorilo glede upravljanja primerov,
- preiskovalna orodja,
- izvajanje usposabljanja AML,
- skrbni pregledi stranke, vključno z elektronskim preverjanjem,
- avtomatika standardnih operativnih postopkov,
- razširjanje AML pravila in postopki.

Kljub številnim prednostim AML programov pa imajo le-ti tudi pomanjkljivosti. Glavne izmed njih so:

- nezmožnost za odkrivanje majhnih zneskov, ki pridejo pod določeno mejo;
- število finančnih transakcij se povečuje, sistemi pa niso dovolj zmogljivi za
- preverjanje vsake transakcije na dosleden in celovit način;
- sistemi temeljijo na pravilih, zato kriminalci najdejo nove možnosti.

Zaradi tega je bistvenega pomena aplikacija, ki se prilagaja, tako da je sistem dinamičen in se odziva na spremembe (AML, 2016).

Pri načrtovanju in razvoju inteligentne aplikacije za preprečevanje pranja denarja je zato predvidena možnost, da se spremlja posamezne finančne transakcije, odkrije nenavadna vedenja in takšne transakcije izloči.

V magistrskem delu želim predstaviti vlogo informacijske rešitve pri preprečevanju pranja denarja v bančnem sektorju. Z analizo programskih podpor za preprečevanje pranja denarja želim ugotoviti ustreznost le-teh oziroma njihovo implementacijo v obstoječe sisteme. Prav tako želim analizirati produkt, razvit v banki, ter njegovo ustreznost v primerjavi z ostalimi produkti na ključ.

Z izvedenimi analizami želim potrditi oz. zavreči hipotezo, da je aplikacija, ki jo banka razvije sama in tudi sama implementira ter vzdržuje in nadgrajuje, ustreznejša, bolj prilagodljiva, popolnejša ter končno cenejša od aplikacij, kupljenih na ključ.
Cilj magistrskega dela je podrobna analiza informacijske rešitve za preprečevanje pranja denarja za potrebe izbrane banke.

Pri izdelavi magistrskega dela bom uporabil sledeče metode:

- študij literature (knjige, članki ipd.), uporabil bom domačo in tujo literaturo s svetovnega spleta,
- študij dokumentacije (zakonodaja, predpisi, obstoječe stanje),
- uporaba znanja, pridobljenega tekom študija na Ekonomski fakulteti ter z večletnim delom pri razvoju informacijskih sistemov za potrebe bank,
- primerjalna in kritična analiza.

V praktičnem delu bom naredil analizo informacijskega sistema izbrane banke za preprečevanje pranja denarja.

V prvem poglavju sem predstavil področje pranja denarja, spreminjanje »umazanega« v »čist« denar ter načine pranja denarja, ki jih pralci denarja najpogosteje uporabljajo. V drugem poglavju je opisana analiza tveganosti pranja denarja, preverjanje strank in nadzor nad poslovanjem strank. Tretje poglavje sem namenil je predstavljanju programska oprema za preprečevanje pranja denarja, njeni zgodovini, učinkovitost in doprinosu za podjetja. Četrto poglavje pa opisuje dejanski informacijski sistem za preprečevanje pranja denarja v izbrani banki.

# 1 PRANJE DENARJA

Pojem »pranja denarja« je bil skovan v znanem mafijskem obdobju ameriške zgodovine v letih 1920. Med kockanjem, prostitucijo in prepovedano prodajo alkohola je prihajalo do velikih vsot denarja, ki jih je bilo potrebno oprati. Povedano z drugimi besedam: potrebno je bilo razviti metode, ki vladnim organizacijam ne bi bile sumljive in bi prekrivale pravo naravo mafijskih finančnih sredstev. Glavna težava na katero so naleteli mafijci, je bila oblika pridobljenega denarja. Denar je bil namreč v obliki gotovine, pogosto so bili to bankovci majhnih vrednosti ali kovanci. Če bi ta finančna sredstva dali na banko, bi postali sumljivi tako bankam in v končni fazi tudi vladi. Poleg tega je shranjevanje denarja v takšni obliki fizično in logistično precej zahtevno in težko. Zaradi tega so si mafijci izmislili posle. Prvi takšen posel je vključeval igralne avtomate, torej zakonite igralnice, drugi pa javne pralnice perila. Kovanci so bili tako lahko uporabljeni za kockanje ali pa za pranje perila. Seveda pa je število dejansko uporabljenih kovancev močno presegalo pravo število kovancev, ki so bili pri tem poslu uporabljeni ter so tako prikazovali večje vsote, kot so bile dejansko namenjene kockanju oziroma pranju perila. Tako je se skoval izraz »pranje denarja« (Brigitte & Linde, 2013).

Izraz »pranje denarja« se je res pojavil v zgodnjih letih 20. stoletja, a sama ideja in ekonomija »pranja denarja« je bila prisotna že tisočletja. Pred 4000 leti so vladajoče kitajske in nekatere druge azijske oblasti izkoristile trgovce, da so prišle preko njih do večjih denarnih sredstev.

V zameno so trgovci postali usposobljeni za svobodno prenašanje denarja ne da bi bili identificirani ali prijeti (Brigitte & Linde, 2013).

## 1.1 Spreminjanje »umazanega« denarja v »čist« denar

Pranje denarja je vključevanje kriminalnih postopkov v prevladujoče legalne trende finančne skupnosti s prekrivanjem njegovega izvora. Enostavneje povedano je pranje denarja pretvarjanje umazanega denarja v legalnega. Zaradi tega je ta postopek poimenovan kot pranje oz. čiščenje. Pranje denarja lahko zveni za veliko ljudi kot nekakšna sofisticirana mednarodna igra spletk in skrivnosti, a potrebno se je zavedati, da za pranjem denarja stojijo nepošteni ljudje. Zelo pogosto je izid takšnih dejanj lahko usoden za tiste, ki so vanje vpleteni ali z njimi obkroženi. Pomislimo samo na mamilarske mafije in teroristične organizacije, ki imajo veliko denarja za oprati (Šeme, 2007).

Nepošteni ljudje, kriminalci, perejo denar iz različnih vzrokov. Legitimen finančni sistem je za kriminalca najverjetneje najbolj varen kraj za shranjevanje svojega premoženja. Premoženje, pridobljeno ne nelegalen način, mora tudi čim prej in čim hitreje obkrožiti svet. To pa najhitreje in legitimno naredijo ravno banke in podjetja, ki se ukvarjajo z denarnimi storitvami. Kriminalec, ki je ravno pridobil svoje premoženje, s katerim koli že nelegalnim dejanjem, se znajde v položaju, ko ne more svojega denarja porabiti nenačrtno in poljubno. V kolikor bi to počel na ta način, bi postal sumljiv tako sosedom, kot uradnim organom, finančnim institucijam in vladnim agentom (Šeme, 2007).

Palermska konvencija, ki je resolucija sprejeta s strani Združenih narodov leta 2000 v Palermu, podaja eno od definicij pranja denarja, katero se običajno pozablja. In sicer pravi, da je kazniva tudi pretvorba ali nakazovanje premoženja z namenom prikrivanja nezakonitega izvora, vedoč, da premoženje izvira iz kaznivega dejanja,. Nezakonito pa je tudi pomagati kateri koli osebi, ki je pooblaščena za izvajanje kaznivega dejanja z namenom izogibanja sodnim, torej zakonskim posledicam tega dejanja (Šeme, 2007).

## 1.2 Postopek pranja denarja

Kot sem že omenil, je pranje denarja postopek, pri katerem je velik znesek nezakonito pridobljenega denarja prikazan kot denar zakonitega izvora. Kriminalci tako ustvarijo podobo, da je nepošteno pridobljen dobiček njihov in ga lahko zapravijo. S tem kriminalci obdržijo nadzor nad svojim nelegalnim napredkom in končno zagotovijo zakonit izgled zgodbe o pridobitvi svojega prihodka. To pa jim zagotavlja uživanje sadov svojega kriminalnega dejanja. Pranje denarja običajno zajema zaporedje številnih transakcij, ki so uporabljene kot oblika dimne zavese za prekrivanje pravega izvora finančnega premoženja na način, da bi bil ta finančni dobiček uporabljen ne da bi izpostavljal kriminalca samega. Pranje denarja igra temeljno vlogo pri lajšanju ambicij prekupčevalcem drog, teroristom,

organiziranemu kriminalu, preprodajalcem, kot tudi vsem ostalim, ki se potrebujejo izogniti pozornosti avtoritetam zaradi nenadnega bogatenja, ki je plod nezakoniti dejanj (Sullivan, 2015).

Pranje denarja zajema tri osnovne faze (Šeme, 2006):

1. plasma, ki se začne, ko je pridobljen nezakonita vsota denarja. To fazo pranje denarja je najlažje odkriti. Običajno kriminalci tej fazi zberejo denar, ga razdelijo na manjše zneske ali ga zamenjajo za drugo valuto. Temu pa sledi poskus polaganja denarja v banko oz. banke ali druge finančne institucije.

2. ustvarjanje plasti, ki nastopu po uspešno opravljenem plasmaju denarja v finančno institucijo. V tej fazi kriminalec briše bančne in računovodske sledi nelegalnega izvora denarja, prenakazuje denar v tujino ali na druge račune. Pri teh postopkih se večinoma kriminalci poslužujejo elektronskih medbančnih transferjev, zlatih kreditnih kartic in podobno. Med izredno zapletene primere sodijo transakcije, ki jih opravljajo pralci iz borznoposredniških hiš. Težavno je tudi slediti pranju denarja, ko gre za mešanje umazanega in čistega denarja, ki ga pogosto uporabljajo podjetja, ki redno poslujejo z veliko gotovine. V tej fazi se velikokrat prekriva tudi dejanskega lastnika premoženja.

3. vključitev ali integracija, v kateri se zakrije sled za nelegalno pridobljenim denarjem, saj je med izvorom in opranim denarjem naloženih dovolj plasti. Nelegalen denar je potrebno prikazati kot legalno premoženje in ga uvesti v finančni sistem. Denar se vrne k storilcu in tako zaključi krog in vstopi v gospodarstvo.

## 1.3 Načini pranja denarja

V tem poglavju bom opisal nekaj načinov pranja denarja, ki jih je sicer v praksi ogromno in so tudi bistveno bolj obširni. Področje pranja denarja se konstantno razvija, nove metode in tehnike pranja denarja pa se iz dneva v dan povečujejo in širijo. Kriminalci ne poznajo meja in vedno iščejo nove načine kako oprati svoje umazano premoženje.

V osnovi lahko rečemo, da ostajajo samo trije načini pranja denarja in sicer (Sullivan, 2015):

- z uporabo legalnega finančnega sistema,
- fizični prenosi gotovine,
- fizični prenosi dobrin preko trgovskega sistema.

### 1.3.1 Delitev denarja na manjše zneske

Do sedaj je bila največkrat zaznana in prepoznana metoda pranja denarja delitev večjega zneska denarja na manjše. Oseba deli finančne transakcije, ko usmerja ali želi usmerjati več kot eno valutno transakcijo v enem ali več dnevih. Pri tem razdeli pologe na več manjših, ki so nižji od zakonsko določenega. Razlog, da pralci denarja delijo pologe umazanega denarja na manjše zneske je v zakonodaji, ki določa, da mora bančna institucija v primeru zneska večjega od zakonsko določenega preveriti transakcijo in o njej poročati. Z deljenjem zneskov pa se temu postopku izognejo (Sullivan, 2015)).

### 1.3.2 Tihotapljenje gotovine

Zakonsko poročanje bank in ostalih finančnih institucij o transakcijah, je prisililo pralce denarja, da poiščejo druge načine prenosa svoje nelegalno pridobljene gotovine. Tihotapljenje gotovine je uspešna in pogosto uporabljena metoda pranja denarja. Ko je denar enkrat zunaj meja, torej v državi z zakonsko striktnim bančnim varovanjem tajnosti, se postopek ustvarjanja plasti lahko prične (Sullivan, 2015).

Tihotapljenje gotovine predstavlja velike količine denarja, ki so skrite pri osebah, v prtljagi, v avtomobilih ali na ladjah, v različnih tovorih, privatnih letalih, če omenim samo nekaj možnosti. Poleg tega lahko gotovino spremenijo v vnovčljive listine kot so razna denarna nakazila, potovalni čeki ipd., ki so poslani v tujino. Najbolj pogosto se dogaja, da pralci denarja tihotapijo gotovino čim bliže državni meji. Vzrok za takšno početje je izogibanje možnosti, da denar najdejo organi kazenskega pregona. Gotovina v tem primeru ne potuje po avtocestah po državi, hkrati pa se privarčuje tudi na času. Od tu je potem denar fizično prenesen preko državne meje (Sullivan, 2015).

### 1.3.3 Zlato

Zlato se uporablja kot alternativa za premik dobička od prodaje drog iz države. Zlato kupujejo kriminalci z nezakonitimi sredstvi od rafinerije zlata ali od veletrgovcev. Kovino nato stalijo in odlijejo v različne majhne odlitke, kot so oblika oreščkov, vijakov, avtomobilskih delov, igrač ipd. Izdelki so kasneje prekriti z barvanjem na sivo ali srebrno, s čimer se zlato skrije. Prekrito zlato se potem prepelje preko kurirja ali letalskega tovornega prevoza v Kolumbijo, Venezuelo ali Ekvador. Zlato je lahko prodano kadar koli, a je običajno pod nadzorom organizacije dokler ni prodajna cena zadovoljiva (Sullivan, 2015).

### 1.3.4 Denarna storitev podjetja

Denarna storitev podjetij, kot je npr. pošta ali ostala podjetja, ki se ukvarjajo s prenašanjem denarja, so velikokrat uporabljeni s strani kriminalcev za prenos denarja od točke A do točke

B. Pri tem je potrebno povedati, da s takšnim poslom ni popolnoma nič narobe, saj so ta podjetja ravno tako kot banke, nevede izrabljena s strani kriminalcev, da izpolnijo svoje cilje.

Denarne storitve podjetij običajno ponujajo širok izbor storitev, ki so lahko uporabljene tudi za pranje denarja. Letalske vozovnice in menjava tujih valut so precej uporabljene metode. Storitev pošiljanja denarja v obliki telegrama, faksa, čeka ali kurirja obstajajo izključno z namenom, da omogočimo ljudem, ki so nezmožni uporabljati običajne finančne institucije, transfer denarja, a so žal tudi te izkoriščene s stani pralcev denarja. Zakonit posel predstavlja nakazovanje majhnih vsot denarja, ki jih tuji državljani želijo poslati svojim najbližjim v svoji domovini. Do sedaj je bila anonimnost strank glavna prednost teh storitev in ravno zaradi tega velikokrat izrabljena (Sullivan, 2015).

### 1.3.5 Poštna nakaznic

Poštne nakaznice, izdane s strani raznih finančnih podjetij, med katere sodijo pošta, Western Union, American Express, so najbolj pogoste oblike denarnih transferjev. Posluževanje storitev teh podjetij je bil običajno najbolj varen način tihotapljenja gotovine, saj ta podjetja veljajo za zanesljiva. Prednost poštnih nakaznic pred gotovino je, da so lahko kupljena v večjih vrednostih in vnaprej, tehtajo manj ter jih je lažje tihotapiti. Poleg tega se lahko nadomestijo v primeru, da so ukradena ali se izgubijo (Sullivan, 2015).

### 1.3.6 Nakazila denarja

Najbolj pogost sistem nakazovanja velikih vsot denarja po celem svetu so bančna nakazila denarja. Nakazilo denarja je del postopka ustvarjanja plasti. Ko je denar že položen v banki, sledi njegovo premeščanje in začetek cikla prevar z namenom pretentanja zakonskih določil. Nakazila denarja so bistveni del legitimne globalne poslovne skupnosti. Nakazila denarja, ki jih uporabljajo pralci denarja so večinoma uporabljena v povezavi z podjetji, ki služijo kot »lupina« in nimajo prave poslovne funkcije ampak njihov obstoj služi za pranje denarja. Banke, ki imajo račune teh podjetij, se običajno nahajajo v državah, ki imajo stroga bančna pravila zasebnosti. Tako je zelo težko slediti denarju, ki iz zakonsko urejenih držav na področju pranja denarja, pride na račune takšnih podjetij. Podjetja, ki služijo kot »lupina«, s fiktivno dokumentacijo vračajo denar v državo iz katere je prišel in na ta način operejo denar (Sullivan, 2015).

### 1.3.7 Igralnice

Pranje denarja preko igralnic je koristen način uporabe nezakonsko pridobljenega dobička, ki je v se uporablja že od nekdaj. Kot enega izmed najbolj značilnih načinov pranja denarja v igralništvu je, da igralec kupi veliko število plakov. Z njimi se odpravi igrati k mizam, a dejansko igra le navidezno. Po končanem igranju odnese plake na blagajno, kjer mu igralnica

izda ček, na katerem je navedeno, da gre za dobitek iz igralnice. Na takšen način pralec denarja pride do legalnega potrdila o izvoru svojega nezakonito pridobljenega denarja. A vse igralnice takšnih potrdil ne izdajajo in tako je pranje denarja preko njihove ustanove oteženo ali celo onemogočeno (Sullivan, 2015).

### 1.3.8 Pranje denarja na podlagi trgovanja

Pranja denarja na podlagi trgovanja je znano kot sistem izmeničnih nakazil. Takšen postopek pranja denarja prekriva izkupiček kriminalnega dejanja in pretok vrednosti preko trgovanja, s čemer poskuša oprati denar. V praksi se to lahko doseže s prekrivanjem oz. ponarejanjem prave cene, količine ali kvalitete uvoznih ali izvoznih produktov. Poleg tega pranje denarja preko trgovanja variira v svoji kompleksnosti in je pogosto uporabljeno v kombinaciji z ostalimi tehnikami pranja denarja. Velikokrat pralci denarja ustanovijo podjetja, ki so zgolj kulisa. Preko njih pa opravljajo navidezne uvozno izvozne posle. Precej pogosto se uporabljajo ponarejeni računi za določene izdelke ali storitve, ki imajo nerealne cene. Kriminalci pa se povezujejo tudi z različnimi uvoznimi podjetji, kjer odigrajo vlogo posrednika storitve ter plačujejo izvoznikom v tujino v tuji valuti. Podjetja, ki uvažajo blago, pa pralcem denarja povrnejo denar v domači valuti. Tečaj vrnjenega denarja je v tem primeru ugodnejši od veljavnega menjalnega tečaja (Šeme, 2006).

### 1.3.9 Elektronsko bančništvo

Elektronsko bančništvo je ena od novejših metod plačilnega sistema, ki zagotavlja elektronski prenos denarja. Spletno bančništvo ponuja pralcem denarja odlično priložnost prenosa velikih zneskov denarja, ki ne poteka fizično, kar je njihova največja skrb. Nič več tudi ni potrebna neposredna identifikacija stranke med izvajanjem transakcije. Stranka posluje s svojim računom preko računalnika. Do računa stranka dostopa z uporabo kode, ki generira ključ. Ključ je potreben za izmenjavo podatkov med uporabnikom in banko. Tako je omogočen dostop do računa, stanja na računu ter uporabi spletnih bančnih storitev. Ob tem se uporablja agent za certificiranje, ki je namenjen preverjanju strankinega digitalnega podpisa ali certifikata. Dandanes je dostop do spletne banke strankam omogočen tako rekoč povsod, nenazadnje tudi preko mobilnega telefona (Sullivan, 2015).

Poleg tega je to sistem, ki povezuje države, banke in finančne organizacije po celem svetu in je na voljo je 24 ur na dan. Nekatere države ne izvajajo dosledno določil o obveznem vključevanju podatkov o pošiljatelju in prejemniku, zaradi česar ostaja pošiljatelj mnogokrat neznan ali pa so podatki nepopolni (Sullivan, 2015).

Prenosi umazanega denarja se običajno zaključijo ali na internetu ali s predplačilnimi karticami (Sullivan, 2015).

### 1.3.10 Pametne kartice

Pametna kartica je kreditna kartica, ki vsebuje v plastičnem delu vgrajeno integrirano vezje - čip, ki je lahko programirano za sprejem, shranjevanje in pošiljanje podatkov. Pametna kartica je lahko uporabljena za »nalaganje« denarja nanjo iz komitentovega računa s pomočjo bančnega avtomata ali celo pametnega telefona. Kartica shrani vrednost, katere del lastnik lahko unovči v trgovini. Nato lahko lastnik kartico ponovno »napolni« in zopet uporabi. Pametna kartica lahko shrani približno osemdesetkratno količino podatkov v primerjavi z običajnimi magnetnimi kreditnimi karticami. V prihodnosti naj bi pametna kartica služila tudi za shranjevanje podatkov o zdravstvenih podatkih lastnika, vozniško dovoljenje ter ostale identifikacijske podatke (Sullivan, 2015).

### 1.3.11 Internet

Internetne banke, ki kar cvetijo na internetu, niso tipične banke v tipičnem tradicionalnem smislu besede, temveč ostaja velika možnost, da takšna banka nima svojega fizičnega sedeža. Dejansko obstaja samo na internetu ter na enem od računalnikov. Večina internetnih bank je nenadzorovanih in nezaščitenih. Pozitivna stran takšnih bank je za pralce denarja to, da ni potrebno nobenega poročanja in malo beleženja, virtualno pa ponujajo in zagotavljajo anonimnost. Slabost internetnih bank pa je, da ne ponujajo nikakršnega zavarovanja, ki ga npr. v Sloveniji nudi Banka Slovenije. V kolikor takšna banka propade, z njenim propadom izgine tudi ves denar. Pomembno je poudariti, da internetno bančništvo ni enako spletnemu bančništvu, ki ga uporabljajo prave banke. Spletno bančništvo običajno ponuja legalna finančna institucija (Sullivan, 2015).

### 1.3.12 Bankomati

Bankomati so razdeljeni na dva sektorja in sicer na bankomate v lasti bank in na bankomate v privatni lastnini. V Sloveniji velja, da so vsi bankomati v lasti bank, skrb in nadzor nad večino slovenskih bankomatov pa izvaja podjetje Bankart. Drugje po svetu pa so bankomati lahko tudi v privatni lastnini in ravno ti so kritični z vidika pranja denarja. Bančni avtomati v lasti bank so običajno pozicionirani pri banki ali na kakšni drugi lokaciji. V vsakem primeru te bankomate vzdržuje banka. Privatne bančne avtomate pa lahko kupujejo posamezniki ali poslovni subjekti ter jih postavljajo na lokacijo po lastni izbiri. Bankomati se potem tudi prodajajo in s tem se izgublja nadzor nad njimi. Sporno pri privatnih bančnih avtomatih za namene pranja denarja, je zmešnjava, ki nastane ob prodaji bankomatov. Ne ve se namreč točno kako sistem na teh bankomatih sploh deluje. V postopku so namreč vključene različne entitete, kot so razni sponzorji finančnih institucij, neodvisni operaterji, različna omrežja, gotovinski trezorji in podobno, kar naredi situacijo težko pregledno in kontrolirano (Sullivan, 2015).

Pralec denarja lahko kupi več bankomatov in jih postavi na različne lokacije. Nekatere od teh lokacij so lahko del poslovnih prostorov, ki lahko so ali pa tudi ne del zarote. Pranje denarja se začne, ko kriminalec naloži v bankomat denar, ki je bil pridobljen na ilegalen način ali pa ta denar vsaj pomeša med čisti denar. Temu sledi ponovno polnjenje bankomata z umazanim denarjem, ko je denar dvignjen. Denar dvignejo nesumljive osebe, ki popolnoma legitimno uporabljajo svojo bančno kartico na bankomatu. Lahko pa denar dvigujejo tudi poklicni pralci denarja, ki delajo za kriminalno združbo ter večkrat dvigujejo denar na tem bankomatu. Elektronska transakcija povzroči bremenitev bančnega računa. Konec meseca neodvisni operater bankomata prinese banki pristen bančni izpisek, ki prikazuje zneske dvigov njenih komitentov. Ta denar pa mu banka elektronsko nakaže na njegov račun. Na ta način se umazan denar spremeni v čistega (Sullivan, 2015).

Države, v katerih so v uporabi zasebni bankomati, se z zakonodajo že trudijo omejiti pranje denarja preko teh naprav.

### 1.3.13 Predplačniške kartice

Primarna nevarnost predplačniških kartic izhaja iz anonimnosti tovrstne kartice in poenostavljenega način razdeljevanje večjih vsot denarja na manjše ter s premeščanjem denarja. Osebi ni potrebno biti bančni komitent, da lahko pridobi predplačniško kartico. S tem je v večini primerov verifikacija identifikacije nezadostna. Ljudje, ki nimajo ali ne morejo imeti običajnega bančnega računa, lahko s pomočjo predplačniških kartic kupujejo in imajo dostop do bankomatov (Sullivan, 2015).

Predplačilne kartice so bile prvotno namenjene shranjevanju določene vsote denarja. Poznamo dve različici takšnih kartic. Prva različica je kartica zaprtega tipa. Te kartice se lahko uporabljajo samo za nakup blaga ali storitev pri točno določeni ustanovi in so popolnoma anonimne. Drugi tip kartic so predplačniške kartice odprtega tipa, ki se lahko uporabljajo v več različnih trgovinah ali pa se uporabljajo kot kartice z namenom plačila. Kartica ima lahko vir sredstev na bančnem računu, kar zagotavlja večjo varnost, saj banka z njo ravna skrbno v dobrobit lastnika. Lahko pa ima kartica izvir sredstev v gotovini, kar pa je anonimno in ne obstaja nobena možnost, da bi ji lahko sledili (Sullivan, 2015).

Ne glede na to ali je kartica odprtega ali zaprtega tipa, pa poznamo predplačniške kartice, ki se jih da ponovno napolniti ter druge, ki se jih ne da ponovno polniti in so uporabne samo enkrat za točno določen znesek na kartici (Sullivan, 2015).

Predplačniške kartice odprtega tipa omogočajo anonimne transakcije preko meja. Medtem ko kartice zaprtega tipa omogočajo preprodajo za gotovinsko plačilo. Predplačniške kartice so postale ena izmed priljubljenih metod plačevanja prodajalcem drog s strani organiziranih skupin prekupčevalcev drog (Sullivan, 2015).

Riziko predplačniških kartic je v anonimnosti in prenosljivosti. Vsakdo namreč lahko kupi toliko kartic kot želi ne da bi ga pri tem kdor koli prosil za identifikacijo. Zaradi tega lahko kriminalec pošlje svojo ekipo nakupovati predplačniške kartice pri čemer uporabi svoj nelegalno zaslužen denar brez kakršnega koli incidenta. Še več, takšna kartica ni obravnavana kot denarna vrednota in zaradi tega ni predmet nobenega od zahtevanih poročil, ko zapusti državo. Poleg tega je ugotavljanje vrednosti na teh karticah s strani carinikov skoraj nemogoče. Zaradi tega so predplačniške kartice eden od uspešno delujočih načinov pranja denarja, ki sicer ne omogoča hiter prenos velikih zneskov denarja, je pa metoda, ki jo kriminalci lahko uporabljajo (Sullivan, 2015).

### 1.3.14 Avtomobili

V mnogih primerih so avtomobili uporabljeni kot tržno blago v postopku pranja denarja. Kupujejo pa jih tudi kriminalne združbe kot transportno sredstvo. Uporabljajo ga kot luksuzni avto ali kot sredstvo za prevažanje drog, gotovine, čekov in bančnih menic. Zaradi možnosti zaplembe premoženja, se kriminalci namesto lastništva večkrat poslužujejo lizinga. Avtomobili so lahko uporabljeni ekskluzivno samo za pranje denarja. Vozila so kupljena z nepošteno pridobljeno gotovino oz. premoženjem, kasneje pa so prodana v tujini za dvojno vrednost (Sullivan , 2015).

### 1.3.15 Korespondenčno bančništvo

Korespondenčno bančništvo je dogovor med bankami, pri katerem ena banka vrši in prejema plačila v imenu druge banke. Banka, ki izvršuje ali prejema plačila je domača banka in se imenuje poravnalna banka ter je ponudnica storitev. Druga banka pa je banka stranke v tujini in jo imenujemo korespondenčna banka. Do finančnih in operativnih tveganj lahko pripeljejo primeri, kjer so tovrstni plačilni tokovi koncentrirani samo pri nekaj bankah (Sullivan, 2015).

Največja nevarnost korespondenčnega bančništva je tveganje, da korespondenčna banka ne pozna osebe ali subjekta, ki je vršilec transakcije.

### 1.3.16 Kreditne kartice

Kreditne kartice se uporabljajo v fazi plastenja in vključevanja ali integracije pranja denarja. Dobra stran je, da transakcijam lahko sledimo. Poleg tega obstajajo tudi omejitve pri plačilu (Sullivan, 2015).

V preteklosti je bilo izrab kreditnih kartic zelo malo. To sicer ne pomeni, da jih ni bilo, vendar kreditne kartice med pralci denarja ne veljajo za enega izmed priljubljenih načinov pranja denarja, čemer najverjetneje botruje omejenost zneskov (Sullivan, 2015).

### 1.3.17 Nepremičnine

Pranje denarja preko nepremičnin je v zadnjem času postalo precej popularno. K njegovi popularnosti je pripomoglo dejstvo, da je pranje denarja precej enostavno zaključiti in to mimo nadzora uradnih inštitucij. V večini primerov pralci denarja kupijo nepremičnino. Pred nakupom podplačajo cenilca nepremičnin, ki oceni nepremičnino precej pod vrednostjo. Za ocenjeno vrednost pralci denarja vzamejo kredit, ki ga odplačujejo z uporabo umazanega denarja. Nekateri pralci denarja nepremičnino po nakupu tudi prodajo za višji znesek (Sullivan, 2015).

### 1.3.18 Intenzivno gotovinsko poslovanje

Gotovinsko intenzivno poslovanje je poslovanje, kjer se posluje večinoma z gotovino. To so razni bari, picerije, hoteli, restavracije, dostave hrane, avtopralnice itd. in so dobre krinke za pranje denarja. Takšna podjetja so lahko zavita v oblake in je njihovo uradno lastništvo napisano na nekoga, ki ima čisto zgodovino in ni sumljiv ter s tem ne povzroča sumljivosti. Pranje denarja preko intenzivno gotovinskega posla pomeni mešanje umazanega denarja s čistim. Zaradi narave tovrstnega posla, je zelo težko ugotoviti kakšen je bil dejanski zaslužek podjetja na določen dan. Dnevni izkupiček bara lahko pride s prodajo pijač. Ko je umazan denar pomešan med dobiček, je za bar enostavno prikazati večji prihodek. Brez natančne revizije poslovanja je težko določiti kateri del prihodka je čist in kateri umazan. Lastniki barov, ki preko svojega posla perejo denar lahko uporabijo veliko izgovorov zakaj je prihodka več, od tega, da se je pijača podražila, da je potrebno plačati zaradi glasbene skupine ipd. Vse skupaj pa precej zaplete situacijo (Sullivan, 2015).

Tako kot pri vseh oblikah pranja denarja, je tudi pri gotovinsko intenzivnem poslovanju, dobro poznavanje zakonodaje in njenih pomanjkljivosti največja prednost pralcev denarja.

### 1.3.19 Zavarovanje

Nekatero do zavarovalnih produktov so lahko uporabljeni za namene pranje denarja. Najbolj izpostavljeno je življenjsko zavarovanje. Pralci denarja izrabijo takšno zavarovanje zato, da ga plačujejo z umazanim denarjem v obliki čekov, denarnimi nakazili ali elektronskih prenosov denarja z namenom nakupa življenjske police. Kasneje zahtevajo predčasno izplačilo teh sredstev. Drugi način izrabe zavarovalnice pa je, da pralec denarja zavaruje drage predmete, kasneje pa naredi lažno prijavo izginotja na policiji. V obeh primerih kriminalec dobi ček za uradno podlago pologa svojega umazanega denarja (Sullivan, 2015).

### 1.3.20 Digitalna valuta

Govori se, da bodo digitalne valute ali virtualne valute oz. kripto valute, kot jim tudi pravijo, v prihodnosti kompenzirale trenutne finance. Gre za digitalno predstavitev vrednosti, ki je lahko shranjena ali poslana v elektronski obliki. V preteklosti je bilo kar nekaj poskusov različnih podjetij, ki se ukvarjajo z digitalizacijo, ki so želela posodobiti finančni sistem z digitalno valuto (Sullivan, 2015).

Najbolj znana digitalna valuta je »bitcoin«. Nastajanje in prenos »bitcoinov« temelji na odprtokodnem protokolu, ki ni odvisen od centralne banke ali drugega regulatornega organa. Tržna kapitalizacija valute konec leta 2013 presegala 9 milijard dolarjev. Danes kot plačilno sredstvo sprejema valuto »bitcoin« vedno več spletnih in fizičnih trgovin z izdelki in storitvami (Sullivan, 2015).

Digitalno valuto se hrani v t.i. elektronski denarnici. Digitalna denarnica je v bistvu datoteka, ki vsebuje zbirko ključev za naslove lastnika denarnice. Programska denarnica je nameščena na osebnem računalniku, spletna denarnica ima funkcijo storitev v internetu, mobilna denarnica pa je nameščena na mobilni napravi. Elektronsko denarnico je potrebno varovati pred krajo ali razkritjem, pri čemer mora lastnik izpolnit določene ukrepe za varovanje (Sullivan, 2015).

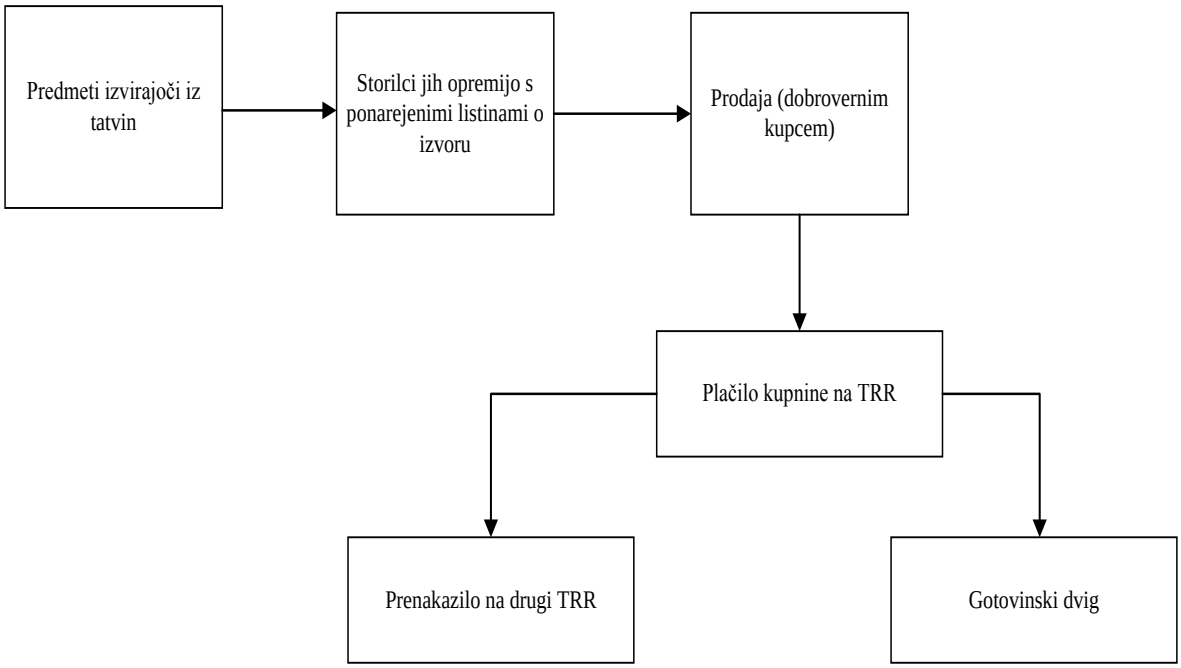
Poleg tega je z »bitcoinom« možno trgovati tudi na spletnih borzah. Uporaba tovrstnih borz ni varna, saj je velika izpostavljenost uporabnikov pred tveganju valutnih nihanj in računalniškimi vdori. Ravno tako pa te uporabnike ne ščiti zakonodaja. V Sloveniji valuta »bitcoin« uradno še ni priznana (Coindesk, 2016).

Kljub temu, da se elektronska valuta sliši kot zelo zanimiva zadeva, je potrebno vedno pomisliti tudi na to, da nekje tičijo kriminalci, ki bodo poskušali najti način za manipuliranje in izrabo tovrstnega sistema. Skrb vzbujajoče dejstvo je anonimnost lastnikov računov. Računi se namreč lahko odprejo preko interneta, za kar pa ni potreben noben dokument.

Pralci denarja združujejo različne načine pranja denarja ter uporabljajo še mnogo drugih načinov, ki jih nisem omenil. Zgoraj je omenjenih zgolj nekaj najbolj poznanih. Pralec denarja se že ob nameri izvedbe kaznivega dejanja, lahko odloči za različne možnosti prekrivanja umazanega denarja. Vedno bolj je mogoče sklepati, da pralec denarja postaja »specializiran poklic«, pranje denarja pa postopek, ki je vse bolj premišljen, dodelan, sofisticiran, odkrivanje in sledenje takšnim dejanjem pa je vedno težje in bolj zapleteno (Šeme, 2006).

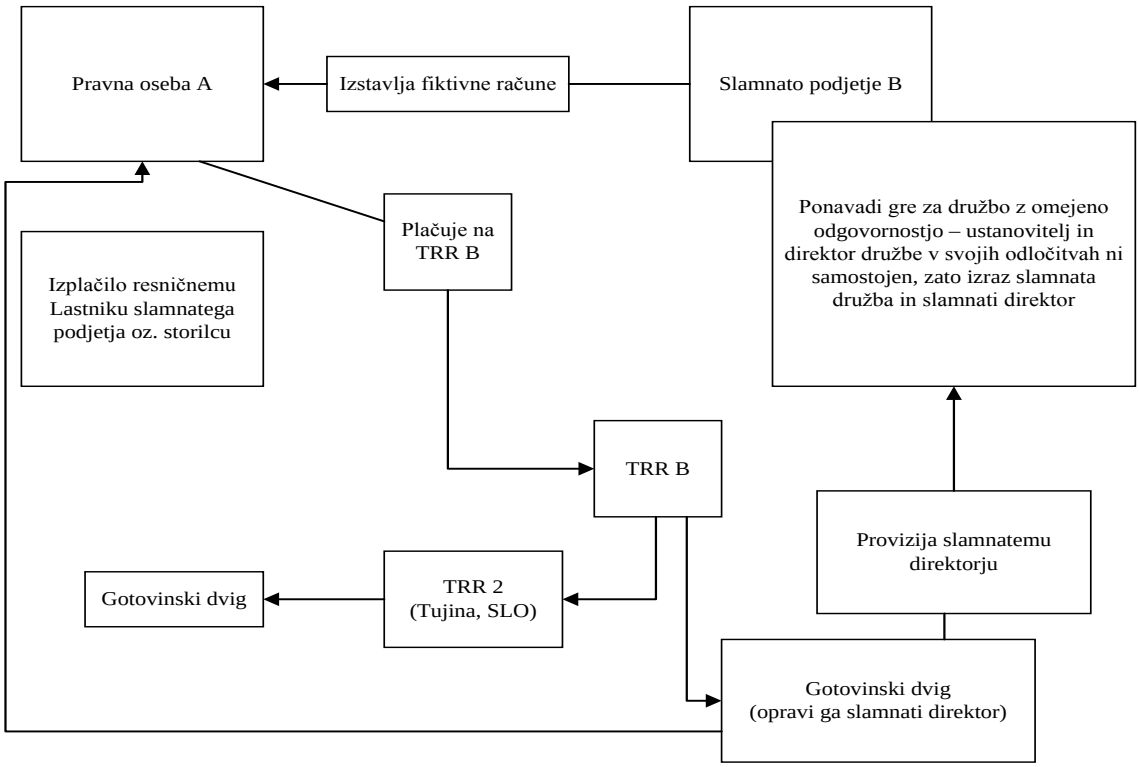
Na Slikah 1, 2 in 3 so prikazani trije med seboj različni načini pranja denarja.

*Slika 1: Prvi primer pranja denarja*



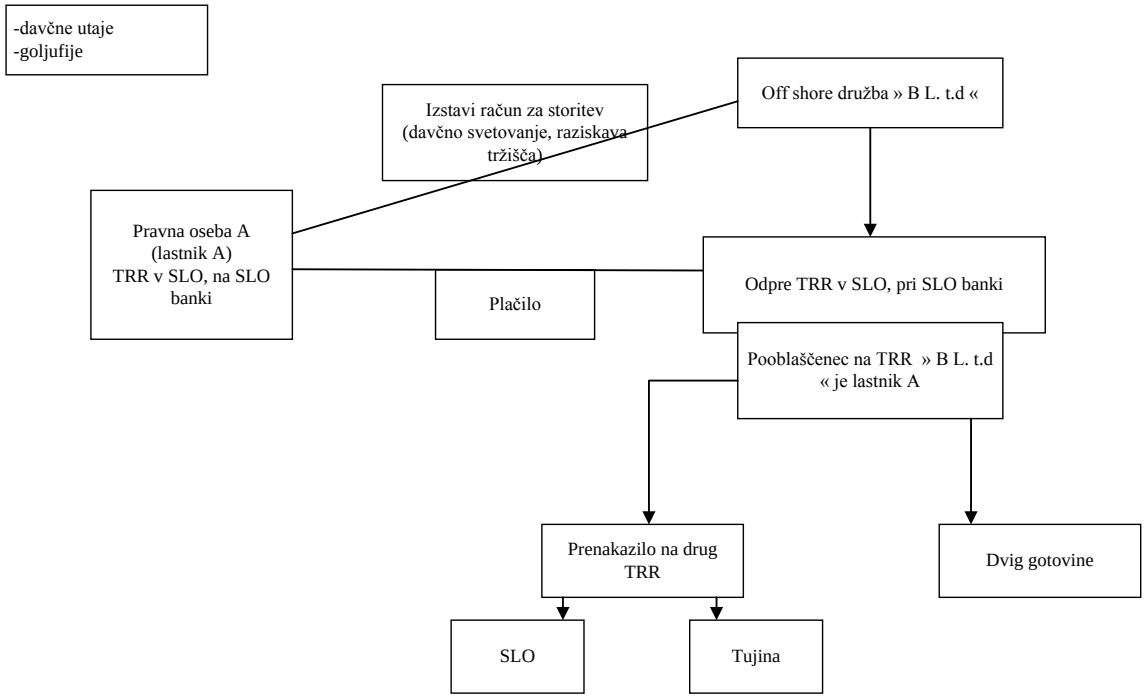

*Povzeto in prirejeno po M. Slapnik, Strategija preprečevanja pranja denarja, 2010, str. 12.*

*Slika 2: Drugi primer pranja denarja*




*Povzeto in prirejeno po M. Slapnik, Strategija preprečevanja pranja denarja, 2010, str. 12.*

*Slika 3: Tretji primer pranja denarja*




*Povzeto in prirejeno po M. Slapnik, Strategija preprečevanja pranja denarja, 2010, str. 13.*

# 2 PREPOZNAVANJE KRITIČNIH STRANK

Pranje denarja je nevarnost, da bi neka fizična ali pravna oseba izkoristila finančno organizacijo preko katere bi umazan denar spremenila v čistega. Vsaka finančna organizacija mora glede na zakonske določbe narediti analizo tveganosti. Analizirati je potrebno tveganost poslovnega razmerja, ki ga sklepa banka s stranko. Z analizo banka pripravi pogoje za čim bolj uspešna preverjanja strank (Banka Slovenije, 2008).

Pred analizo tveganosti mora banka pripraviti in potrditi svoje interne pravilnike, v katerih določi načine obvladovanja nevarnosti pranja denarja. S takšnimi pravilniki banka določi katera področja njenega poslovanja so izpostavljena in v kakšni meri ter načine postopanja v primeru težav s pranjem denarja (Banka Slovenije, 2008).

Zakonodaja daje bankam nekaj napotkov o tem kako naj pripravi analizo tveganosti. Predlagano jim je, da naredijo popis svojih poslovnih procesov in določijo tveganje vsakega posebej ter načine kako bodo tveganje zmanjšali, hkrati pa določijo vloge vodstva ob tem ter opredelijo namene in cilje nadzora nad pranjem denarja (Ur. l. RS, št. 63/94, 23/99, 40/04).

## 2.1 Preverjanje strank

Finančne organizacije morajo upoštevati določila zakonodaje, ki se nanaša na preprečevanje pranja denarja. Prvi postopek pri ugotavljanju morebitnih kaznivih dejanj, je prepoznavanje stranke oz. komitenta. Namen preverjanja stranke je preverjanje istovetnosti stranke, torej resničnosti strankine identitete. Preverjanje stranke mora potekati na verodostojen način. V kolikor gre za poslovni subjekt, je potrebno preveriti lastništvo, pridobiti je potrebno podatke o namenu poslovanja in o predvideni naravi posla (Banka Slovenije, 2008).

Določene stranke predstavljajo večje tveganje za pranje denarja od drugih. Zaradi tega poteka preverjanje strank na različne načine. Stranke, ki veljajo za sumljivejše z vidika pranja denarja, doleti bolj poglobljeno, celovito preverjanje, katerega postopki so strožji od preverjanja strank, za katere je sum na pranje denarja manjši ali zgolj znaten in je postopek preverjanja enostavnejši. Natančnejši postopek preverjanja strank je določen v ZPPDFT (Banka Slovenije, 2008).

Za ugotavljanje prave identitete stranke finančna organizacija uporablja verodostojne in objektivne vire, ki so hkrati tudi neodvisni. Stranko se preveri z vpogledom v dokument, s katerim se identificira. To je lahko osebni dokument, izpisi iz javnega registra, preverjanje strankine identitete se lahko izvede, ko je stranka osebno prisotna ali je prisoten njen zakoniti zastopnik oz. pooblaščenec. Zakoniti zastopnik ali pooblaščenec zadostuje, ko gre za pravni subjekt. V primeru fizičnih oseb mora biti stranka tudi osebno prisotna. Lahko pa se stranko preverja tudi preko tretje osebe ali z uporabo digitalnega potrdila, ki pa mora biti kvalificirano (Banka Slovenije, 2008).

Banka oz. vsaka finančna organizacija mora preveriti stranko, ko z njo stopa v poslovno razmerje, kar pomeni, da identificira stranko ob sklenitvi pogodbe, ki se nanaša na eno izmed dejavnosti finančne organizacije (Banka Slovenije, 2008).

Preverjanje stranke poteka tudi pri vsaki transakciji, ki je višja od 15.000 evrov (v nadaljevanju EUR). Transakcija v višini 15.000 EUR ali več pa ni nujno narejena z eno samo transakcijo ampak je lahko ta znesek razdeljen na več transakcij, ki pa so med seboj nekako logično povezane. Lahko jih ena stranka izvrši v več transakcijah na račun tretje osebe ali pa jih vrši več oseb ravno tako v korist tretje osebe (Banka Slovenije, 2008).

Stranko preverja finančna institucija tudi v primeru, da se ji že pridobljeni podatki o identifikaciji stranke zdijo sumljivi ter vsakokrat, ko obstaja sum na kaznivo dejanje pranja denarja ne glede na znesek transakcije (Banka Slovenije, 2008).

Sklepanje poslovnega razmerja in izvajanje transakcij je zakonsko prepovedano finančnim ustanovam v primeru, da se finančna organizacija ne more dokopati do prave identitete

stranke, ko podvomi v verodostojnost predloženih strankinih dokumentov o identifikaciji, ko stranka ne želi pomagati organizaciji pri zagotavljanju pravih podatkov in zavrača sodelovanje pri pridobivanju dodatnih pojasnil. V takšnih primerih je finančnih organizacijam priporočeno, da takšno nenavadno obnašanja strank sporoči regulatorjem po presoji in preučitvi primera z vidika možnosti kriminalnega dejanja pranja denarja. Primer seveda ustrezno preučijo organizacije v okviru svojih sposobnosti (Banka Slovenije, 2008).

Zgoraj opisan postopek velja za novo stranko. Za že obstoječo stranko pa se bistveno ne razlikuje. V kolikor se že obstoječa stranka obnaša na takšen način, finančna ustanova s stranko lahko zamrzne obstoječe poslovno razmerje ali pa ga prekine, kar pa je poslovna odločitev same organizacije na podlagi narave posla, ki ga ima s stranko sklenjenega. Sumljivo obnašanje stranke tudi v tem primeru finančna ustanova sporoči regulatorjem. Vseeno pa je priporočeno, da se v takšnih primerih stranko obravnava kot sumljivo oz. bolj tvegano in se bolj natančno spremlja njene finančne dejavnosti (Banka Slovenije, 2008).

Ko je podano povečano tveganje za nastanek kriminalnega dejanja pranja denarja, morajo finančne ustanove opraviti natančnejše preverjanje stranke. Takšna preverjanja je glede na določila ZPPDFT potrebno opraviti pri vseh bančnih razmerjih, ki so sklenjena s tujo politično izpostavljeno osebo in pri strankah, ki niso fizično prisotna pri ugotavljanju in preverjanju identitete ter pri drugih strankah, kjer obstaja visoko tveganje (Banka Slovenije, 2008).

### 2.1.1 Preverjanje politično izpostavljene tuje osebe

Politično izpostavljena tuja oseba že sama po sebi velja za stranko z visokim tveganjem pranja denarja. Zaradi tega mora organizacija vedno opraviti temeljit pregled takšne osebe pred sklenitvijo poslovnega razmera ali izvrševanjem transakcij. Tako kot za tujo politično izpostavljeno osebo veljajo enaka pravila za njene ožje družinske člane ter ožje sodelavce. Osebi je potrebno preveriti morebitno stalno prebivališče v drugih državah in njeno delovanje v vlogi javne osebe. Vse te podatke organizacija pridobi pred sklenitvijo posla na podlagi posebne pisne izjave, ki mora biti lastnoročno podpisana ter sestavljena v slovenskem in angleškem jeziku (Banka Slovenije, 2008).

Natančnejši pregled stranke zajema poleg osnovnih korakov pregleda stranke, ki velja za vse, še nekaj dodatnih aktivnosti. Banka mora pridobiti podatke o izvoru sredstev ali premoženja, namenjenega transakciji. Preden se transakcija izvede, jo mora pisno odobriti nadrejena odgovorna oseba še preden je sklenjeno poslovno razmerje. Po izvedbi transakcije pa je potrebno le-to in vse aktivnosti, ki povezane s tovrstno stranko, natančno spremljati (Banka Slovenije, 2008).

Ko kljub vsem pridobljenim podatkom na podlagi izjave obstaja dvom v njihovo resničnost, banka naredi dodatno preverjanje podatkov z pregledom raznih javnih ali drugače dostopnih evidenc, katerih obseg sama presodi. Ima pa seveda tudi možnost stopiti kontakt s pristojnimi organi drugih držav, konzulati in veleposlaništvi, zunanjim ministrstvom (Banka Slovenije, 2008).

### 2.1.2 Preverjanje stranke, ki ni navzoča

ZPPDFT določa, da mora finančna organizacija opraviti bolj detajlni pregled v primeru, da stranka ali njen pooblaščenec ni osebno prisoten ob sklepanju posla. Poleg obveznih točk pregleda, zahteva takšen pregled še nekaj dodatnih poizvedb. Banka mora pridobiti dokumente ali podatke oz. informacije, ki dodatno potrjujejo identiteto stranke. Podatke o stranki se v takšnem primeru preverijo tudi v javno ali kako drugače dostopnih evidencah. Takšno stranko banke preverjajo še pri ostalih bankah, pri katerih ima stranka morebiti že odrt račun ali kako drugače sklenjen posel. Pogoj za preverjanje podatkov pri drugih bankah ali finančnih inštitucijah je, da delujejo v skladu državno zakonodajo o preprečevanju pranja denarja. Poleg preverjanja stranke pri drugih bankah v državi, se o stranki pridobivajo podatki tudi pri državnih organih in drugih organizacijah, kjer ima stranka svoj sedež ali prebivališče. Nenazadnje pa banka pred sklenitvijo poslovnega razmerja stopi neposredno v stik s stranko preko telefona ali pa jo obišče s stani banke pooblaščena oseba na domu ali njenem sedežu (Banka Slovenije, 2008).

Slovenska zakonodaja omogoča preverjanje identitete fizične osebe, samostojnega podjetnika ali posameznika, ki opravlja dejavnost, na podlagi kvalificiranega digitalnega potrdila. Pri takšne načinu preverjanje je potrebna velika pazljivost, saj lahko kaj hitro pride do zlorabe. Zaradi tega je še pred sklenitvijo kakršnega koli poslovnega razmerja preveriti ali ima morebiti kvalificirano digitalno potrdilo kakšne omejitve, veljavnost potrdila, veljavnost zasebnega ključa, ali je potrdilo morda preklicano ter verodostojnost izdajatelja potrdila. Banka lahko zahteva od overitelja, ki je potrdilo izdal, podatke o načinu ugotavljanja in preverjanja istovetnosti stranke (Banka Slovenije, 2008)..

Banka sklene poslovno razmerje s stranko, ko je prepričana o istovetnosti stranke, ki je lastnik digitalnega potrdila in ne obstaja nobenega suma kaznivega dejanja (Banka Slovenije, 2008).

### 2.1.3 Ostale stranke z visokim tveganjem

V kolikor ima banka opravka s stranko, pri kateri meni, da bi lahko prišlo do pranja denarja, to stranko preveri na enak ali podoben način, kot preverja politični izpostavljene osebe in stranke, ki niso navzoče. To pomeni, da za preverjanje uporabi še ostale razpoložljive

metode, preko katerih pride do dodatnih podatkov o stranki pri drugih bankah, državnih institucijah, v različnih evidencah (Banka Slovenije, 2008).

### 2.1.4 Enostavno preverjanje stranke

Banka lahko opravi poenostavljen pregled stranke pred sklenitvijo poslovnega razmerja, ko je stranka pravna oseba ali njen lastnik ter so podatki o stranki pregledni ali javno dostopni ali pa ima država ustrezen nadzor na poslovanjem te stranke ter ob vsem tem obstaja neznatno tveganje za pranje denarja. Spisek potrebnih podatkov je v tem primeru manjši, saj ni potrebno ugotavljanje lastnika stranke, ravno tako pa ni potrebna prisotnost zakonitega zastopnika ali pooblaščenca pravne osebe (Banka Slovenije, 2008).

Enostavno preverjanje stranke lahko banka naredi sami v primeru, ko je ocena tveganja za pranje denarja te stranke neznatna. Oceno tveganja banka naredi na podlagi prejetih podatkov o stranki. Preden banka ne opravi pregleda vseh dejstev, ki so potrebna za dopustnost enostavnega preverjanja stranke, ne sme skleniti poslovnega razmerja ali narediti transakcije. V kolikor pa v povezavi s stranko obstaja sum pranja denarja ali financiranja terorizma pa enostaven pregled stranke nikakor ni mogoč (Banka Slovenije, 2008).

## 2.2 Nadzorovanje poslovanja strank

Nadzor nad denarnim poslovanjem strank je zelo pomembno za to, da se učinkovito izvajajo predpisane zahteve za preprečevanje pranja denarja. Poslovanje strank se nadzira z namenom odkrivanja neskladnosti s predvideno naravo poslovanja. Poslovanje stranke naj bi se ujemalo z njegovo običajno količino posla. Pri nadziranju poslovanja stranke se preverja tudi veljavnost dokumentov in ažurnosti podatkov o stranki (Banka Slovenije, 2008).

Način in naravo poslovanja strank se  nadzoruje na različne načine. Banka preverja vse transakcije stranke in okoliščine, v katerih so nastale z namenom preprečevanja pranja denarja. Zakonodaja določa sezname indikatorjev, ki so osnova za preverjanje in nadzorovanje. Stranko se preverja vsakokrat, ko se pripravlja nova ocena tveganosti ter v primeru obnovitve že obstoječe ocene (Banka Slovenije, 2008).

Bank sama določi višino zneska, nad katerim bo preverjala naravo transakcij. Lahko ga določi za vsako stranko posebej in sicer na podlagi ocene, ki jo je sama naredila. Velikokrat se za uspešno preverjanje uporablja informacijska podpora. (Banka Slovenije, 2008).

Banka preverja tudi veljavnost pridobljene dokumentacije, ki se nanašajo na stranko. Preverjajo se podatki o podjetju, naslovu, sedežu podjetja, lastniku podjetja, imenu lastnika, njegovem stalnem in začasnem prebivališču ter njeni morebitni politični izpostavljenosti. V

kolikor ima podjetje izpostave, mora banka preveriti tudi vse prej naštete podatke tudi za vsako izpostavo. Banka ponovi preverjanje podatkov, v kolikor obstaja dvom v resničnost že pridobljenih podatkov. Preverjajo se podatki o stranki v javnih registrih, neposredno pri stranki ali morebitnem zastopniku oziroma pooblaščencu. Preverjajo se tudi razne liste sumljivih oseb (Banka Slovenije, 2008).

Finančna ustanova sama določi kako pogosto in v kakšnem obsegu bo preverjala poslovanje strank glede na oceno o tveganju, ki jo je pripravila sama pred sklenitvijo poslovnega razmerja s stranko. V vsakem primeru pa zakonodaja nalaga banki, da mora stranko preveriti vsakih pet let, v kolikor stranka izvaja transakcije. Če stranka transakcij ne izvaja, pa mora banka preveriti stranko, ko le-ta izvede prvi nakup ali prodajo oz. kakršno koli drugo transakcijo. Finančna ustanova mora pri spremljanju transakcij strank nameniti veliko pozornost v kolikor imajo transakcije nenavadno sestavo, če so transakcije zapletene, neobičajno visoke, brez jasnega ekonomskega ali pravnega namena ter transakcijam, ki se ne skladajo s pričakovano naravo poslovanja stranke. V takšnih primerih transakcij, ki nakazujejo na sum kaznivega dejanja pranja denarja, mora banka preveriti tudi ozadje transakcij in njihov namen v taki meri, kot ji okoliščine dopuščajo. Vse ugotovitve pa mora zapisati in shraniti (Banka Slovenije, 2008)**.**

Posebno pozornost morajo finančne ustanove nameniti strankam in transakcijam, ki so v povezavi z državami, kjer zakonodaja ni dovolj stroga do morebitnih pralcev denarja.

### 2.2.1 Potencialno sumljive aktivnosti , ki nakazujejo na pranje denarja

Obstaja veliko potencialno sumljivih aktivnosti ali sklopov aktivnosti, ki lahko namigujejo na poskus pranja denarja. Spodaj navajam le nekaj izmed mnogih. Obstajajo seznami potencialno sumljivih akcij, kateri se uporabljajo tudi pri snovanju računalniških programov za preprečevanje pranja denarja.
Eno izmed mnogih skupin, predstavlja skupina sumljivih aktivnosti stranke, ki zagotovijo nezadostno število podatkov ali pa so ti podatki sumljivi (Sullivan, 2015):

- stranka uporablja nenavaden ali sumljiv identifikacijski dokument, ki ga ni mogoče takoj preveriti;
- stranka uporablja različne davčne številke z variacijami svojega imena;
- ob odprtju poslovnega računa stranka ni pripravljena podati popolnih podatkov o naravi in namenu posla, predvidene dejavnosti na računu, pretekle bančne odnose, imena uradnikov ali direktorja ter informacije o lokaciji podjetja;
- domača ali poslovna telefonska številka ne obstaja oz. je izklopljena;
- strankino ozadje se razlikuje od pričakovanih aktivnostih na podlagi njegovih poslovnih aktivnosti;

- stranka izvaja pogoste in visoke transakcije ter nima nobenih podatkov o preteklih ali sedanjih poslovnih izkušnjah;
- stranka je lahko sklad, navidezno podjetja ali privatna investicijska družba, ki ni pripravljena zagotoviti informacij o vodstvu podjetja. Vodstvo namreč lahko najame nekoga, ki ustanovi navidezno podjetje in mu odpre bančni račun, pri tem pa ščiti identiteto lastnika.

Drugo skupino predstavljajo stranke, ki si prizadevajo, da bi se izognile poročanju ali evidentiranju (Sullivan, 2015):

- stranka ali skupina prisili bančnega uslužbenca, da ne ohranja in ne arhivira zahtevanih poročil,
- stranka je nejevoljna, ko mora zagotoviti informacije potrebna za obvezna poročila, je proti arhiviranju poročil ali pa noče več nadaljevati s transakcijami po tem, ko je bila obveščena o nujnosti poročil,
- stranka je nejevoljna, ko mora podati podatke o identifikaciji, ko kupuje prenosljive listine v zneskih, ki se beležijo,
- stranka zahteva, da se jo izvzame iz poročil in evidenc,
- oseba uporablja bankomat, da naredi več pogostih manjših depozitov,
- stranka deponira manjša sredstva na več različnih računov, ki jih kasneje združi na glavni račun in jih prenese v tujino,
- stranka dostopa do sefa po tem, ko je naredila večjo transakcijo, s katero je umaknila denar.

Prerazporeditev sredstev je tudi eno od potencialno sumljivih dejanj. Običajno se prerazporeditve sredstev dogajajo v velikih zneskih, ki so zaokroženi na stotine ali tisočine. Prerazporeditve se izvajajo iz ali v območja, kjer veljajo zakoni diskretnosti strank. Lahko so brez očitnega poslovnega razloga ali pa se razlog ne sklada s preteklimi poslovnimi dejanji istega subjekta.

Prenos sredstev se lahko zgodi tudi v ali iz finančne ustanove, ki se nahaja na zelo oddaljenem območju glede na lokacijo stranke, kjer velja strožja zakonodaja (Sullivan, 2015).

Sumljivo je tudi večje število majhnih nakazil ali depozitov, ki so narejeni preko čekov ali denarnih nakaznic. Skoraj takoj po tem pa se ves denar nakaže v tujino ali v drugo mesto, pri čemer na način, ki se ne sklada s preteklimi dejanji tega podjetja (Lilley, 2001).

Sumljivi so večji zneski, ki jih stranka prejme v imenu tuje stranke, pri tem pa je namen nakazila zapisan zelo skopo ali ga celo ni. Ravno tako so na listi sumljivih aktivnosti, ki nakazujejo na pranje denarja tista nakazila, ki so nepojasnjena, ponavljajoča ali nakazujejo

na nenavadne vzorce ter nakazila ali prejemki brez povezave z zakonskimi pogodbami, dobrinami ali storitvami. Nenavadni so transferji, ki so poslani ali prejeti s strani iste osebe z ali na druge račun (Lilley, 2001).

Spiski takšnih in drugačnih sumljivih dejanj so precej obsežni in nesmiselno bi bilo navajati vse. Tu je naštetih le nekaj, na podlagi katerih lahko dobimo občutek na kaj vse morajo biti finančne ustanove pozorne in kaj vse mora programska oprema zajemati ter podpirati (Sullivan, 2015).

# 3 AML MODELI

Na globalnem trgu pranje denarja predstavlja enega izmed najbolj perečih vprašanj, s katerimi se soočajo regulativni organi. Regulativni organi pričakujejo od finančnih institucij po vsem svetu, da poslujejo s svojimi strankami odgovorno in pri tem poskrbijo za zaščito nacionalne varnosti pred pranjem denarja in rizikom financiranja terorizma. Zaradi tega regulativni organi spodbujajo podjetja, da izkoristijo tehnologijo za upravljanje različnih pomembnih tveganj. Istočasno pa zahtevajo, da finančne institucije upravljajo s tveganji, ki so povezana z uporabo novih tehnologij in prevzamejo nadzor nad rezultati avtomatiziranih sistemov, kot je program za preprečevanje pranja denarja. Zaradi prevelikih pričakovanj regulativnih organov veliko podjetij ne opravi potrebnih rednih pregledov (AML modeli, 2016).

Ostra konkurenca finančnih institucij v izdelkih in storitvah, ki zagotavljajo najhitrejše, najlažje in najbolj prilagojene izdelke in storitve za potrebe kupcev na potrošniškem trgu, je otežila sledenje pretoku sredstev v celotnem svetovnem finančnem sistemu. Skrajšan čas izvršitve finančne transakcije pa je otežil pravočasno prepoznavanje tveganj za pranje denarja in riziko financiranja terorizma. Tehnološki razvoj, kot je bila npr. uvedba mobilnega bančništva, pa je reševanje problematike še podaljšal. Finančne institucije iz dneva v dan ugotavljajo, da je upravljanje in blažitev AML tveganj težavna (AML modeli, 2016).

## 3.1 Kaj je AML

AML ali programska oprema za preprečevanje pranja denarja (angl. *AML software*) je programska oprema, ki se uporablja v financah in pravnih panogah za preprečevanje pranja denarja ali poročanje o tovrstnih aktivnostih.

Obstajajo štiri osnovne vrste AML programske opreme, ki podpirajo poslovne zahteve (AML, 2016):

- sistem za spremljanje transakcij, ki se osredotoča na prepoznavanje sumljivih vzorcev transakcij. Rezultat delovanja takšnega sistema so razna poročila,

- valutna transakcijska poročanja, ki se ukvarjajo z večjimi zneski transakcij,
- sistem za identifikacijo stranke, ki preverja različne negativne sezname (npr. OFAC), lahko pa preverja tudi druge baze podatkov (npr.: telefonske sezname, sezname dobavitelja električne energije, poštno bazo pošiljk ipd.), da pridobi identiteto.
- programska oprema za skladnost, ki pomaga podjetjem ugotavljati skladnost z AML kontrolnimi zahtevami, ob tem shranjuje potrebne evidence skladnosti.

## 3.2 Zgodovina AML-ja

Smernice za preprečevanje pranja denarja so prišle globalno v ospredje po napadih 11. septembra 2001 in poznejših uzakonitvah »USA PATRIOT ACT-a« v Združenih državah Amerike ter z vzpostavitvijo posebne enote finančnih ukrepov za preprečevanje pranja denarja (angl. *Financial Action Task Force on Money Laundering*). Od leta 2010 veliko število sodnih oblasti zahteva od finančnih institucij, da nadzorujejo, raziskujejo in poročajo o sumljivih primerih finančnim institucijam v lastni državi (Federal Financial Institutions Examination Council, 2016).

Celotna industrija je razvila programsko opremo za analiziranje transakcij z namenom identificiranja transakcij ali vzorcev transakcij, imenovanih tudi strukturiranje. V kolikor finančne institucije ne upoštevajo določenih pravil, so sankcionirane, kar vključuje visoke finančne kazni in stalen nadzor celo do točke preklica ustanovne listine (AML, 2016).

## 3.3 Učinkovitost AML-ja

Učinkovitost AML-ja je velikokrat pod vprašajem. Vsi AML programski produkti temeljijo in so odvisni od vhodnih podatkov. Nato ovrednotijo transakcije ali račune glede na opažen nivo sumljivosti in pregledajo anomalije sumljivih podatkov, ki temeljijo na statističnih podatkih ali scenarijih. Sumljiva transakcija bo izbrana glede na visok dvig ali polog na račun. Vsekakor je zanesljivost takšnih sistemov odvisna od znanja, ki je vgrajeno v program in razpoložljivosti podatkov za takšen sistem. Prednost takšnih sistemov je neprestana sposobnost analiziranja velike količine podatkov (Cox, 2009).

V kolikor takšne programske opreme ne bi imeli na voljo, bi lahko imeli veliko težav. Če predpostavljamo, da ima banka veliko število komitentov, ki so razdrobljeni po raznih lokacijah, bi bilo preverjanje tolikšnega števila podatkov brez ustrezne programske opreme zelo počasno. Ročni proces zbiranja podatkov temelji na posredovanju podatkov strank, pri čemer je malo kontrol, ki bi ovrgle nepravega komitenta. Popravljanje takšnih list bi pomenilo vnovičen pogovor s stranko. Banke morajo zagotoviti izvajanje finančnih predpisov, prav tako pa jim tudi ni v interesu, da bi poslovale s pralci denarja in finančnimi teroristi. Uporaba programa ima posledično dva namena (Cox, 2009):

- zagotavlja kontrolo, da so sumljive transakcije zabeležene in pregledane,
- prav tako zagotavlja obrambo podjetja pred obtožbami, da bi moralo biti več postopkov pregledovanja.

V primeru velike količine podatkov na različnih lokacijah je težko delovati brez takšnih programov in osebno tveganje bi bilo preveliko.

Za učinkovit sistem spremljanja transakcij bi podjetja morala, kot navaja (Cox , 2014):

- imeti analizirano zmogljivost sistema delovanja do zadovoljivega nivoja podrobnosti, pravilo za pravilo, ki bi omogočalo razumevanje pravih razlogov za pridobljene rezultate,
- postaviti sistem, ki ne naredi premalo poizvedb samo z namenom izboljšanja zmogljivosti, obstaja namreč riziko umetno dvignjenih deležev zaznav sumljivih transakcij, ki so na koncu dobljeni kot sumljivi brez generiranja kvantitetnih in kvalitetnih izboljšav,
- narediti analitična orodja za identificiranje sumljivih dejavnosti, ki do tedaj še niso označena kot sumljiva;
- dodeliti ustrezna sredstva za analizo in oceno delovanja sistema, zlasti za merjenje uspešnost, in zagotoviti trdno bazo podatkov za uspešno analizo,
- dosledno spremljanje namesto zgolj občasnega, da se zagotovi, da podatki o uspešnosti niso izkrivljeni zaradi npr. ad-hoc odločitev, da naj tečejo določena pravila ob različnem času,
- koliko se le da meriti učinkovitost s primerljivimi družbami.

Program naj bi nadziral različne stvari. V nekaterih primerih podjetje lahko doda posebnosti, ki jih želi imeti poleg tistih, ki jih rutinsko izdelajo programi. Pri tem je potrebno biti pozoren na (Cox, 2009):

- spremljanje transakcij s proizvodi, strankami, vrednostjo ali katerim koli dejavnikom, ki ga podjetje določi,
- mirujoče račune, ki postanejo aktivni,
- spremembe obsega transakcij strank, ki so nad določenim odstotkom,
- podatke svoje stranke, ki jih mora podjetje poznati, in ugotovljena neskladja s pomočjo nekaterih oblik statističnih tehnik,
- račune, ki so predmet izboljšav zaradi pretirane skrbnosti lastnika, in vzroke za takšno početje,
- stranke, ki imajo pomanjkljive podatke v verificiranju identifikacije,
- države ali sumljive posle, ki so osnovani na zunanjih podatkih,
- politično izpostavljeni osebe (angl. *PEPs*, v nadaljevanju PEP), katerih podatki so običajno uvoženi v obstoječi sistem iz zunanjih podatkovnih baz,

- nadzorovane finančne sankcije, pri čemer se ravno tako uporabljajo zunanje podatkovne baze,
- prepoznavo izločenih posameznikov ali direktorjev, če je regulator sprejel ukrepe s pomočjo zunanjih virov informacij,
- strankina dejanja, ki se spreminjajo po zgodovinsko znanih primerih pranja denarja.

To so samo nekatere stvari, ki bodo v praksi pregledane. Vsak program ima namreč različne pristope pregledovanja.

## 3.4 Doprinos AML programov za podjetje

Uporaba AML programov pa lahko doprinese finančni ustanovi veliko koristnega. AML program omogoča podjetjem, da enostavno dokumentirajo, da so izpolnili predpisane zahteve, ki so jih dolžni izvajati glede na različne zakonske podlage za preprečevanje pranja denarja. AML programi lahko pomagajo pri stalnem spremljanju in vodenju evidenc ter odkrivanju nenavadnih transakcij (Mitchell, 2005).

Uporaba tovrstne programske opreme lahko podjetju zagotovi tudi obrambo pred globami in ohranitev ugleda v primeru, ko pride do tega, da je podjetje imelo opravka z nekom, ki je pral denar (Mitchell, 2005).

AML programi bi morali povečati število primerov, ki bi bili predani preiskovalnim organom, saj bolj natančne preiskave omogočajo analizo informacij, ki je temeljita, natančna in hitra. To povečuje možnost, da bodo poročila o sumljivih dejanjih nemudoma predložena. Njihova uporaba zmanjšuje tudi stroške poslovanja, saj programska oprema racionalizira preiskovalni proces, da je potrebno manj človeškega vložka. Podjetja pa lahko ta sredstva in zaposlene uporabijo na drugih področjih delovanja podjetja (Mitchell, 2005).

Uporaba programske opreme lahko izboljša učinkovitost in poslovno upravljanje, zaposleni pa dobijo popoln pregled nad tveganjem, ki vpliva na poslovanje (Mitchell, 2005).

## 3.5 AML programi na tržišču

Programska oprema za spremljanje transakcij se osredotoča na spremljanje posameznih transakcij z namenom preprečevanja in odkrivanja pranja denarja. To je zlasti koristno pri veliki količini kompleksnih podatkov v finančnih institucijah, vključujoč male in korespondenčne banke (Cox, 2014).

Programska oprema na trgu na splošno uporablja celovite analitične rešitve, da preveri vse račune in transakcije ter s tem najde primere pranja denarja. Primere program najde z analiziranjem ocen tveganja tipa komitenta, izdelka, storitve in geografskega območja.

Ujemanje primera zazna tudi z iskanjem po listah, kot so PEP in OFAC, odkriva pa tudi skrite odnose med družinskimi člani, prejemniki in političnimi strankami. Program išče tudi ujemanje dogajanja na računu po znanih scenarijih za pranje denarja. Poleg tega pa analizira podatke o transakcijah glede na vrsto, kombinacije z drugimi transakcijami in višino zneskov, da lahko prepoznava potencialno sumljive dejavnosti.
Na ta način dobimo dva tipa programskega produkta. Prvi tip produkta temelji na scenarijih, drugi tip pa ugotavlja potencialno sumljive dejavnosti (Cox, 2014).

### 3.5.1 Programi za elektronsko identifikacijo

Programska oprema AML, ki identificira ID stranke elektronsko, je dragocena, saj omogoča preveritev ključnih dokumentov, ki jih stranka prinese fizično. A pri tem obstaja težava, da so dokumenti lahko ponarejeni. V tem primeru uporabi napredno programsko opremo, da na različne načine poskrbi za elektronsko overitev identitete stranke. To lahko vključuje tudi uporabo neodvisnih virov podatkov, da se preveri vire informacij. Nekateri programi na trgu lahko zagotovijo rezultat ali vrednost indeksa, ki označuje stopnjo zaupanja, da sta identiteta posameznika ter naslov pravilna (Cox, 2014).

### 3.5.2 Programi za sankcijske in politično izpostavljene liste

Podjetje mora vedeti, ali ima opravka z znanimi goljufi, teroristi ali pralci denarja. Posledica tega, da nimamo zadostnega sistema za ugotavljanje, ni samo grožnja s kaznimi s strani regulativnih organov ali grožnja nacionalni varnosti, temveč to škodi tudi ugledu podjetja (Cox, 2014).

OFAC in PEP programska oprema pogosto in skrbno pregleda seznam strank v podjetju, da bi zaznala posameznike, ki so navedeni na nacionalnem in mednarodnem sankcijskem seznamu. S tem pa zagotavlja tudi, da podjetje ne bi nevede pomagalo pri financiranju terorističnih dejanj (Cox, 2014).

Večina OFAC in PEP rešitev minimizira napačno izbrane (potencialno izbrani morajo biti dodatno še ročno preverjeni), ki se lahko običajno pojavijo pri avtomatiziranih rešitvah. Večina sistemov bo omogočila tudi popolno revizijsko sled in pregled sankcij ter poročanje o skladnosti (Cox, 2014).

## 3.6 Izbira AML-ja

V mnogih primerih so neuspešne programske implementacije posledica pomanjkljive presoje različnih tipov programskih produktov. Razlike niso vedno očitne na spletnih straneh družb, tako da so potrebna srečanja z različnimi prodajalci in razprave z uspešnimi uporabniki.

Ena od ključnih faz izbirnega postopka je izgradnja seznama podjetij, ki bodo obravnavana v postopku izbire, ne glede na izbrano metodo za končno odločitev. V mnogih primerih napačen izbor izvira iz nepopolnega seznama potencialnih dobaviteljev, s čimer se prezre ključne prodajalce proizvoda. Sposobnosti podjetij, ki so pomembne pri izbiri dobavitelja, so (Cox, 2014):

- nadzor transakcij: odkrivanje in opisovanje strank in transakcijskih aktivnosti vseh izdelkov in kanalov;
- avtomatizirana ocena tveganja: ocena lokacije, izdelka in vrste posla skupaj z oceno transakcij, vedenja in stalnih podatkov;
- poznati svoje stranke: vodeno uvajanje za stranke skozi določeno zaporedje korakov v procesu dela;
- analiza povezav: odkriva skrite odnose med transakcijami, strankami, računi, opozorili, primeri, izdelki in kanali;
- integracije z vgrajenimi sistemi in bazami podatkov: vgrajeni dodatki za integracijo na obstoječe sisteme in baze podatkov.

## 3.7 Ponudniki AML-jev

Kot napovedujejo nekateri analitiki, je obetavna tržna niša analitična programska oprema, ki zna predvidevati in s tem zmanjšuje možnosti napak ter tako s skladnostjo zmanjšuje stroške. Globalni AML trg kaže na ogromen potencial glede na to, da ponudniki takšne programske opreme ponujajo veliko različnih produktov in rešitev ter jih prilagajajo na razne načine svojim kupcem (Wood, 2016).

Na trgu je veliko ponudnikov različnih vrst AML-jev. To je pa seznam vodilnih ponudnikov tovrstne opreme (Wood, 2016):

- ACI Worldwide,
- AML360,
- AML Partners,
- AML RightSource,
- BAE,
- EastNets,
- Experian,
- Fiserv,
- Nice Actimize,
- Oracle,
- Reed Elsevier,
- Safe Banking Systems,

- SAS,
- SunGard,
- Thomson Reuters,
- Tonbeller,
- Truth Technologies in
- Verafin.

Drugi vidnejši ponudniki na trgu so:

- Aquilan,
- Ascent Technology Consulting,
- Banker's Toolbox,
- Cellent Finance Solutions,
- CGI group,
- IBM,
- KPMG,
- Jack Henry,
- TCS in
- Temenos.

## 3.8 Prihodnost AML-jev

AML programi omogočajo, da finančne ustanove in druga podjetja odkrivajo sumljive transakcije in analizirajo podatke strank. Tržne raziskave napovedujejo rast AML programov do leta 2020 za 11 %. Pomembno gonilo rasti na trgu je vse večja zahtevana skladnost s predpisi, ki sili finančne institucije, da uporabljajo AML programe (Wood, 2016).

Za največje uporabnike AML programov so analitiki ocenili Združene države Amerike, saj je tam največji trg za tovrstno programsko opremo. Naraščajoče sprejemanje strogih predpisov, ki sili finančne institucije v uporabo na eni strani ter pospešuje razvoj AML programov, ki podpirajo tovrstne zakonske zahteve, na drugi strani, pa kaže na to, da se bodo tovrstne programske rešitve razširile tudi na druge trge razvijajočih se gospodarstev, kot so Avstralija, Kitajska in Indija (Wood, 2016).

# 4 INFORMACIJSKI SISTEM ZA PREPREČEVANJE PRANJA DENARJA V IZBRANI BANKI

Četrta EU direktiva s področja preprečevanja pranja denarja in financiranja terorizma uvaja novo zahtevo za prepoznavanje domače politično izpostavljene osebe, na podlagi katere bo spremenjen tudi ZPPDFT.

Poleg zakonodajne zahteve je izbrana banka vpeta v mednarodna poslovna razmerja z večjimi evropskimi in ameriškimi bankami, ki pričakujejo od banke, da ima uveden ustrezen nadzor pri obravnavi svojih strank.

S to zahtevo želi zagotoviti enoten nadzor in ustreznost izvajanja posameznih korakov v procesu kontrole list omejevalnih ukrepov in enoten način obravnave strank, ki so v banki identificirane kot stranke ali zgolj naključni izvajalci transakcij. Cilj izbrane banke je poenotenje internih virov informacij in izključitev večkratnih oziroma nepotrebnih kontrol.

Kontrola liste omejevalnih ukrepov v izbrani banki se izvaja različno, in sicer z uporabo različnih sistemov, saj je kontrola nastajala vzporedno z razvojem posameznih sistemov v banki. Ker je aplikacij in različnih sistemov v banki zaradi takšnega razvoja v preteklosti veliko, se povečuje tveganje, da je v nekem delu procesa sklepanja poslovnega razmerja oziroma izvajanja transakcije rešitev postavljena neustrezno. Rešitev je neustrezna, v kolikor ne omogoča nadzora in upravljanja tega kompleksnega področja z enotne točke. To pomeni, da ne obstaja centralna shema rešitve na enem mestu, ni enotnega skrbništva, ni uporabniškega vmesnika za nadzor in upravljanje sistema kontrol na liste omejevalnih ukrepov; to je omejitev na finančne transakcije do posameznih oseb oziroma blaga v določene države.

Za kontrolo sumljivosti komitentov oziroma njihovih transakcij služijo eksterni in interni podatkovni viri. Ti podatkovni viri so osnova, na kateri tečejo trenutni sistemi.

Prvi podatkovni vir je črna lista, ki jo ažurira Združenje evropskih bank (angl. *European Banking Federation,* v nadaljevanju FBE). V skladu z Zakonom o omejevalnih ukrepih, ki jih je Slovenija uvedla ali jih izvaja skladno s pravnimi akti in odločitvami, sprejetimi v okviru mednarodnih organizacij, je banka dolžna pri svojem poslovanju upoštevati in izvajati omejevalne ukrepe, ki jih določajo pravni akti Evropske unije (v nadaljevanju EU) oziroma Organizacija OZN.

FBE pripravlja konsolidirano bazo oseb, ki zajema seznam vseh oseb (fizičnih, pravnih in drugih oseb), zoper katere so uvedeni mednarodni omejevalni ukrepi prepovedi opravljanja finančnih storitev. Za vsako osebo, navedeno na tem seznamu, je priložen tudi pravni akt, s katerim je bila sankcija uvedena.

Bančni delavci so dolžni pred sklenitvijo poslovnega razmerja, v vseh primerih, ko se poslovno razmerje ne sklepa preko avtomatičnega sistema, obvezno opraviti ročni vpogled v črno listo FBE, in sicer:

- pri vseh fizičnih osebah, ki imajo stalno ali začasno bivališče v tujini oziroma imajo tuje državljanstvo, in
- pri vseh tujih pravnih osebah.

V primeru, da pri pregledu liste bančni delavec ugotovi, da se stranka, ki želi skleniti poslovno razmerje, nahaja na črni listi FBE, mora le-ta o tem takoj obvestiti pooblaščenko za preprečevanje pranja denarja. Banka je namreč dolžna v skladu z zakonodajo o poskusu sklenitve poslovnega razmerja ali izvedbe transakcije obvestiti Ministrstvo za zunanje zadeve RS, in sicer najkasneje v roku 48 ur. Sporočilo bančni delavec posreduje bančni pooblaščenki in brez njenega soglasja se poslovno razmerje ne sme skleniti. Črna lista FBE je javna listina, zato v tem primeru ni obveze varovanja tajnosti podatkov (Slapnik, 2010).

Druga tovrstna lista s podatki je lista OFAC (angl. *Office for Foreign Assets Control*, v nadaljevanju OFAC). Je lista ameriškega Urada za nadzor tujih naložb. Zaradi preprečevanja pranja denarja in financiranja terorizma Združenih držav Amerike izvaja programe, v katerih objavlja listine fizičnih in pravnih oseb ter držav, s katerimi je prepovedano poslovno poslovanje. Tudi bančno poslovanje z navedenimi osebami s sedežem ali naslovom v državah, ki so navedene na listah, ni dovoljeno.

Kontrolo politične izpostavljenosti izvajamo ob preverjanju istovetnosti stranke. Pri strankah s stalnim bivališčem v Republiki Sloveniji po trenutnem zakonu ne ugotavljamo PEP, stranke s stalnim bivališčem v tujini pa se morajo pisno opredeliti z Izjavo stranke o politični izpostavljenosti. Z novo evropsko direktivo je potrebno informacije o politični izpostavljenosti pridobivati za vse komitente banke, zato je potrebno proces avtomatizirati, saj ročno zbiranje izjav ne bo izvedljivo.

Poleg že navedenih mednarodnih evidenc je ob sklenitvi poslovnega razmerja ali izvedbi plačilne transakcije potrebno izvajati kontrole tudi na interne evidence sumljivih subjektov, in sicer na osnovi internih zaznav ali na podlagi zahteve zunanjih institucij, kot sta
lista Urada za preprečevanje pranja denarja (v nadaljevanju UPPD) – seznam oseb, zoper katere je UPPD uvedel spremljanje transakcij, ki jo ažurira pooblaščenec za preprečevanje pranja denarja, in seznam računov, katerih nosilci so prejemniki sredstev iz naslova zlorab elektronske banke (v nadaljevanju MULE), ki jo ažurira upravljavec varovanja informacijskih sistemov (v nadaljevanju IS).

IS je sistem, ki uporablja informacijsko tehnologijo za zajemanje, shranjevanje, prenašanje, pregledovanje, obdelovanje ter izpisovanje podatkov in informacij, ki jih potrebuje organizacija za tekmovanje z organizacijami iz okolja (Gradišar & Resinovič, 1998).

Mednarodni listi sumljivih oseb FBE in OFAC izvirata iz različnih virov, in sicer iz dveh brezplačnih spletnih povezav in dodatno s plačljivo podporo zunanjega dobavitelja.

Način kontrol, ki se trenutno uporablja, ima kar nekaj pomanjkljivosti, ki jih je potrebno z izgradnjo in uvedbo nove aplikacije odpraviti. Kot prva pomanjkljivost se kaže nezadostno ažuriranje informacij o tveganih osebah v registru komitentov. V registru je namreč omogočen ročni vnos oznake za FBE, predvidena je tudi dopolnitev za označevanje politično izpostavljenih oseb, ne izvaja pa se označevanje preostalih vrst sumljivosti komitenta . Zaradi sprotnega preverjanja in sprejemanja ukrepov s področja preprečevanja pranja denarja in financiranja terorizma (v nadaljevanju PPDFT) bi bilo smiselno in primerneje, da bi celovito informacijo vključeval že register komitentov, kar bi omogočilo pomembno poenostavitev programskih kontrol in performančno razbremenitev sistemov.

Druga pomanjkljivost, ki jo vidim pri sedanjem načinu kontroliranja, je nezadostno ažuriranje informacij o tveganih osebah v registru komitentov, v katerem je omogočen ročni vnos za oznake FBE. Neenotni in nezadostni so tudi avtomatizirani postopki za poročanje Uradu za preprečevanje pranja denarja.

Zaradi neenotnega koncepta kontrol list omejevalnih ukrepov in internih list se izvajajo enake in nepotrebne večkratne programske kontrole. Ker ni vzpostavljen enoten koncept kontrol list omejevalnih ukrepov in internih list, se postopki kontrol v procesu izvršitve transakcije po nepotrebnem ponavljajo. Zaradi nezadostnih informacij o prisotnosti strank na listah omejevalnih ukrepov in internih listah v registru izbrane banke se tudi za masovno izvajanje transakcij izvajajo zahtevne kontrole iskanja in primerjav v mednarodnih evidencah.

Z arhitekturnega vidika pa velja za izbrano banko izpostaviti naslednja pomembna dejstva. Izbrana banka enake podatkovne vire črpa iz različnih naslovov. Mednarodni listi sumljivih oseb FBE in OFAC prevzemamo v dveh brezplačnih spletnih inačicah in dodatno s plačljivo podporo zunanjega dobavitelja. Ti podatki se sicer uporabljajo tudi v različnih drugih informacijskih podporah v izbrani banki.

Druga pomembna arhitekturna pomanjkljivost je razpršenost internih podatkovnih virov. Poleg že navedenih mednarodnih evidenc je ob sklenitvi poslovnega razmerja ali izvedbi plačilne transakcije potrebno izvajati kontrole tudi po internih evidencah sumljivih subjektov, ki jih na osnovi internih zaznav ali na podlagi zahteve zunanjih institucij, vsebinsko upravlja pooblaščenec za PPDFT in varovanje informacijskih sistemov (v nadaljevanju VIZ). Ti podatki

se posredujejo v različnih oblikah in po različnih poteh. Vpišejo se preko vmesnika, pošiljajo po elektronski pošti, različni šifranti se ažurirajo celo ročno. Posledično so izdelani tudi različni programski postopki za izvajanje ustreznih kontrol.

Posledica vsega je tudi nezadostno ažuriranje informacij o tveganih osebah v registru izbrane banke. V Registru komitentov je omogočen ročni vnos oznake za FBE, ne izvaja pa se označevanje preostalih vrst sumljivosti komitenta. Zaradi sprotnega preverjanja in sprejemanja ukrepov s področja PPDFT bi bilo smiselno in primerneje, da bi celovito informacijo vključeval že Register komitentov, kar bi omogočalo pomembno poenostavitev programskih kontrol in performančno razbremenitev sistemov.

Dodaten razlog za centralizacijo informacij v Registru komitentov je najnovejša poslovna odločitev o širitvi kriterijev za izvajanje kontrol na FBE in OFAC. Zahteva izhaja iz dejstva, da je skupina izbrane banke vpeta v mednarodno poslovno okolje medbančnega poslovanja, ki zahteva zelo strog nadzor, saj je v primeru neustreznih kontrol v kateri koli članici skupine izbrane banke izpostavljena visokemu tveganju, da bi ameriške banke in večje evropske banke z izbrano banko prekinile izvajanje mednarodnega plačilnega prometa, kar bi imelo znatne negativne poslovne posledice za celotno skupino izbrane banke.

Neenotni in nezadostni so tudi avtomatizirani postopki za poročanje Uradu za preprečevanje pranja denarja (v nadaljevanju UPPD). Podatki za poročanje o gotovinskih transakcijah se nalagajo na aplikaciji, namenjeni poslovanju na bančnih okencih, od koder se prevzemajo v staro aplikacijo za preprečevanje pranje denarja, ki omogoča pregled pooblaščencu za PPDFT in posredovanje na UPPD. Negotovinske transakcije pa se izvršujejo v aplikacijah plačilnega prometa. Programsko izdelane sezname uporabniki ročno verificirajo z registrom in jih preko elektronske pošte posredujejo pooblaščencu za PPDFT, kjer se izvede dodatni pregled, prevedba UPPD strukture in posredovanje na UPPD.

V izbrani banki poteka tudi večkratno programsko izvajanje enakih zahtevnih kontrol, kar je posledica nevzpostavljenega enotnega koncepta kontrol za liste omejevalnih ukrepov in interne liste. Postopki kontrol se v procesu izvršitve transakcije po nepotrebnem ponavljajo. Zaradi nezadostnih informacij o prisotnosti strank na listah omejevalnih ukrepov in internih listah v registru izbrane banke se tudi za masovno izvajanje transakcij izvajajo zahtevne kontrole iskanja in primerjav v mednarodnih evidencah.

Na splošno bi lahko rekli, da je trenutni način dela aplikativne podpore področja preprečevanja pranja denarja in financiranja terorizma v izbrani banki heterogen.

Vzpostaviti je potrebno učinkovitejše obravnave sumljivih transakcij, kar pa je pogojeno z jasno definiranimi poslovnimi zahtevami in celovito funkcionalno analizo najprimernejših tehničnih rešitev.

## 4.1 Želeno stanje informacijske podpore za izvajanje omejevalnih ukrepov

Izbrana banka se je za uvedbo nove aplikacije za preprečevanje pranja denarja odločila iz več razlogov. Prvi razlog so gotovo stroge zakonodajne zahteve v povezavi s sankcijskimi listami in spremembami ugotavljanja PEP na osnovi četrte direktive na področju PPDFT, ki jih mora izpolniti. Nova aplikacija bi te zahteve upoštevala in tako bi tudi v prihodnje izbrana banka lažje sledila novim zahtevam in jih aplicirala v aplikacije. Poleg tega je izbrana banka pod močnimi pritiski finančnih institucij, še posebej s strani Združenih držav Amerike. Ob neupoštevanju mednarodnih pravil se ji lahko zgodi, da zaprejo račune in tako izbrana banka posledično ne more poslovati več s tujino. S prehodom na novo aplikacijo bi izbrana banka znižala tudi tveganja neustreznega izvajanja zahtev zaradi razpršenosti in različnosti trenutno implementiranih rešitev tako na ravni banke kot na ravni celotne bančne skupine izbrane banke. Z enotnim pristopom na ravni bančne skupine bi zmanjšali stroške vzdrževanja in licenčnin pri nabavi list ter zmanjšali tveganje.

Nova aplikacija bi ji prinesla tudi dolgoročno optimizacijo stroškov, saj bi z njo poenotila listo in bazo vseh zahtevanih listin, imela bi enotno informacijsko rešitev, ki bi potrebovala za delovanje tudi enotno podporo. Poleg tega pa bi bili poenoteni tudi procesi dela in s tem optimizirani postopki.

Takšna aplikacija bi zagotovila konsistenten nadzor in upravljanje sistema kontrol. Posledično bi se zmanjšalo tveganje, saj bi v banki imeli enotna pravila za izvajanje kontrol, ki bi omogočala upravljanje, vnos in pregled na enem mestu. S tem pa bi imeli več kakovostnih kontrol in hkrati bi izločili nepomembne.

### 4.1.1 Razvoj nove aplikacije

Razvoj informacijske podpore plačilnemu prometu je zasledoval sprotno aktualne poslovne zahteve in organizacijo tovrstnih storitev. Pomembne spremembe zunanjega in notranjega okolja, ki smo jim priča v zadnjem času, narekujejo poenotenje in centralizacijo sicer zelo razvejane palete aplikativnih rešitev. Z vzporednim procesiranjem posameznih vrst plačil so se namreč multiplicirale tudi splošne programske funkcije, značilne za vse vrste plačil. Ena takšnih je tudi vse bolj izpostavljeno izvajanje kontrol nad izvajanjem transakcij v povezavi z omejevalnimi ukrepi.

Ker je izvajanje tovrstnih kontrol v podpori plačilnemu prometu tesno povezno s splošnimi programskimi in podatkovnimi elementi, je analiza obstoječih rešitev terjala širši pregled obstoječe podpore. Ob tem so bile ugotovljene nekonsistentnosti in neučinkoviti pristopi, ki onemogočajo racionalno definiranje novih zahtev. Predlog zato povzema kar najširši funkcionalni okvir in podaja izhodišča možne racionalizacije.

Zaradi nove zakonodajne zahteve po kontroli politično izpostavljenih oseb tudi za rezidente Slovenije, je bil izbran nov dobavitelj list, Dow Jones.

Takšen pristop, poleg neupravičenih stroškov, terja tudi nepotreben razvoj več vzporednih postopkov za prevzem in osveževanje podatkov in onemogoča uporabo enovitih servisnih funkcij za izvajanje kontrolnih funkcij.
Poleg že navedenih mednarodnih evidenc je ob sklenitvi poslovnega razmerja ali izvedbi plačilne transakcije potrebno izvajati kontrole tudi za interne evidence sumljivih subjektov, ki so nastale na osnovi internih zaznav ali na podlagi zahteve zunanjih institucij.

Izhodišči za takšno rešitev sta poenotenje eksternih in internih virov informacij in zagotavljanje vseh potrebnih informacij o sumljivosti subjekta ali komitenta v registru izbrane banke. Potrebno je tudi centralizirati nadzor plačil v breme ali v dobro vseh komitentov, ki niso slovenski državljani.

Zagotovitev modula oz. servisa za celovito in fleksibilno kontrolo je tudi eno od pomembnih izhodišč za nadgradnjo sistema. Poleg tega je izključitev vseh nepotrebnih in večkratnih kontrol ključna za izogib ponavljajočim se delovnim procesom. Celoten sistem pa mora biti nadgrajen tudi z integracijo in avtomatizacijo poročanja odgovornim organizacijam.

Izbrana banka si je za polnjenje list podatkov izbrala ponudnika Dow Jones. Pri Dow Jones-u si prizadevajo za odpravo pranja denarja in financiranja terorizma ter korupcije. Zaradi tega poskušajo olajšat delo organizacijam po svetu in povečati skladnost med njimi ter učinkovito obvladovati tveganja. Dow Jones lista uporablja oseb globalno največjih finančnih institucij. Njegove liste so statistično dokazano najbolj natančne, točne, popolne in ažurne, saj vključujejo seznam visoko politično izpostavljenih oseb, njihovih družinskih članov in bližnjih sodelavcev. Dow Jones nudi celovite sezname profilov oseb, ki so povezani z visokim tveganjem za kriminalna dejanja, kar omogoča organizaciji, ki te liste uporablja, veliko manjše tveganje za izgubo ugleda. Njihova baza podatkov je prilagojena PEP pristopu.

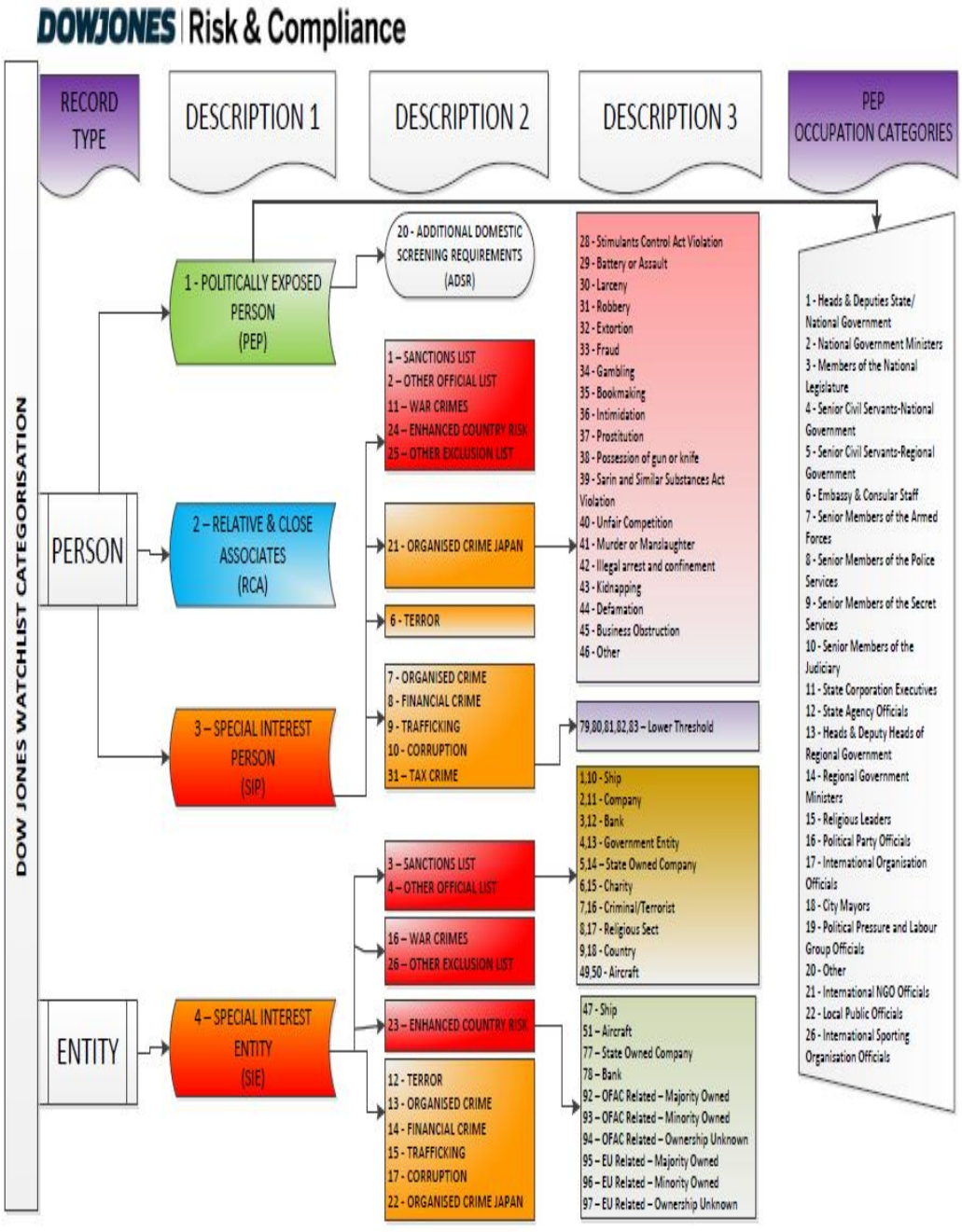
Na Sliki 4 je prikazana lista, ki jo uporablja izbrana banka za podporo v svojih programih.

### 4.1.2 Proces razvoja

Celoten proces razvoja aplikacije je nazorno prikazan z V-modelom. V-model razvoja programske opreme temelji na slapovnem modelu, vendar je učinkovitejši pri pravočasnem zagotavljanju kakovosti. Glavna prednost V-modela je, da se proces testiranja premakne v zgodnejše faze razvoja. Faza testiranja je razširjena in se jo izvaja med fazami: analiza zahtev in priprava specifikacij, načrtovanje arhitekture, podrobno načrtovanje in faza izvedbe. Kot prikazuje organigram na Sliki 5, se za vsako od omenjenih faz pripravi plan, kako se jo bo

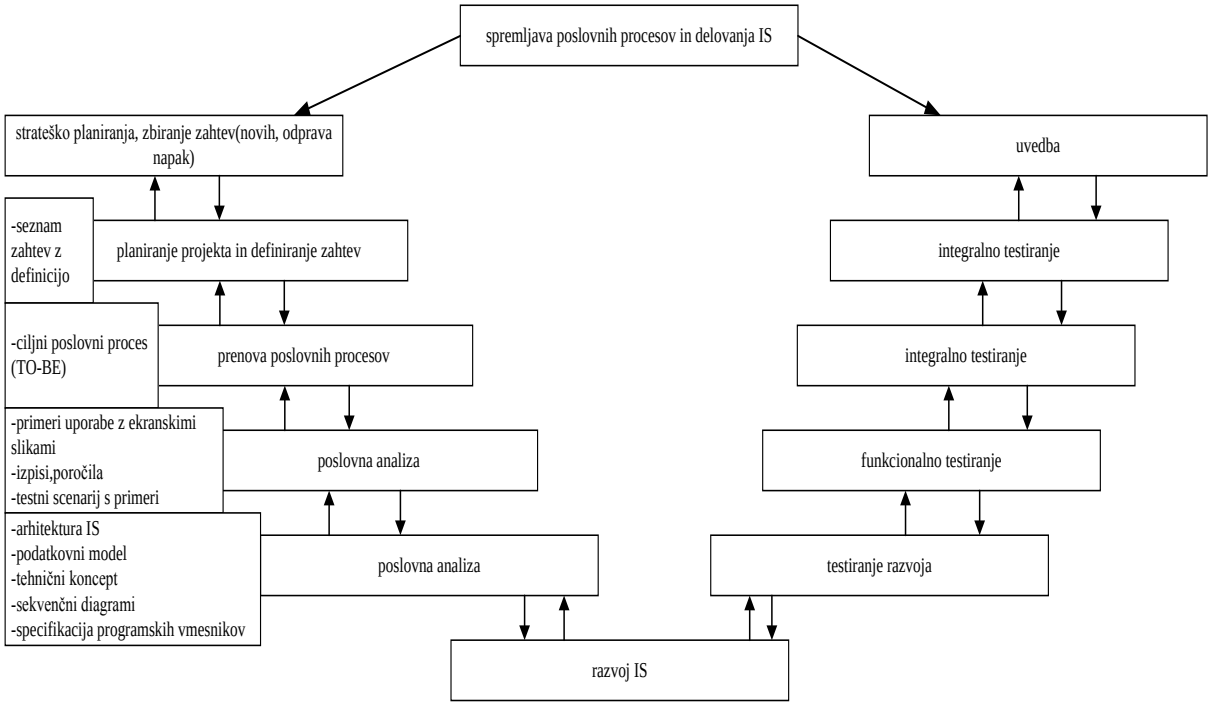
testiralo. Sam proces testiranja še zmeraj poteka po implementaciji, vendar so testni plani in včasih tudi avtomatski testi že napisani, zato poteka veliko hitreje (Gruden, 2014).

*Slika 4: Dow Jones lista*




*Vir: Izbrana banka, Dow Jones analiza, 2015a.*

*Slika 5: Življenjski cikel razvoja (V-model, Waterfall model)*




*Vir: Izbrana banka, Izvajanje procesa razvoja z IT komponento, 2016.*

Skozi razvoj se vloge prisotnih spreminjajo in prilagajajo evoluciji razvoja sistema.
Ključne vloge so: uporabnik, poslovni analitik, načrtovalec, razvijalec, tester.

Sam proces razvoja aplikacije je razdeljen na več različnih faz. Prva faza obsega zbiranje naročnikovih zahtev in njihovo podrobno proučitev. Nekatere zahteve bi lahko bile nerealne ali nesmiselne, saj si lahko med seboj celo nasprotujejo. Ko so zahteve jasno definirane in zapisane, jih naročnik potrdi, da se glede na zahteve napiše specifikacije, namenjene tako naročniku kot razvijalcem. Takšna dokumentacija mora biti jasna in razumljiva tako naročniku kot izvajalcem, saj je osnova za izvajanje zahtev in za kasnejši izogib nesporazumom.
Glavna značilnost tradicionalnih metodologij razvoja programske opreme se pokaže v tej fazi s t. i. »Big Design Up Front«, kar pomeni, da še pred začetkom izvedbe naredijo natančen načrt izdelka.

Ta faza ima nekaj izrazitih prednosti in slabosti. Včasih se izkaže, da prvotni načrt ni izvedljiv. V takšnem primeru je sprememba načrta veliko cenejša v tej, tj. začetni fazi, kakor če bi ta problem odkrili šele med implementacijo (kodiranjem) posameznih delov produkta. Po drugi strani takšen proces dela onemogoča oziroma zelo oteži kakršno koli spremembo naročnikovih želja po zaključku te faze. Velikokrat se med implementacijo tudi izkaže, da je bila kljub podrobnemu načrtovanju v začetku projekta kakšna pomembna podrobnost

spregledana, in se je iz faze izvedbe treba vrniti nazaj v fazo načrtovanja, kar lahko zelo podaljša čas izvedbe produkta.

Kadar govorimo o poslovnih procesih v organizacijah, se velikokrat pokaže, da jih le redko kdo pozna v celoti, saj gre za kompleksne sisteme, ki nastajajo v organizacijah vrsto let. Od njihovega delovanja je odvisen uspeh podjetja, javnih služb oziroma organov državne uprave. Formalno opisati in opredeliti poslovne procese je težavno, kar posledično povzroča težave pri razumevanju in težnji po izboljšanju poslovnih procesov. Upravljanje poslovnih procesov tako ponuja eno možno rešitev, in sicer da podjetje začne z izboljševanjem poslovnih procesov.

### 4.1.3 Proces razvoja v izbrani banki

Metodologija razvoja informacijskih sistemov in njegovih sprememb je v izbrani banki interni akt, po katerem se ravna projektna in linijska organizacija. V aktu je opredeljeno izvajanje razvojnega postopka ter sistematično vodenje zapisov o opravljenih postopkih razvoja. Akt se deli na dva dela, in sicer na proces razvoja informacijskih sistemov in na proces nadgradnje informacijskih sistemov. Dokument je namenjen temu, da vodi izvajalce do čim bolj uspešnega zaključka razvoja ne glede na organizacijski vidik, ki je lahko projektno ali linijsko organiziran, ali vrsto razvoja, ki je lahko lastni ali v sodelovanju z zunanjimi izvajalci. Tehnološka navodila urejajo odnose med uporabniki in izvajalci, definirajo in poenotijo postopke in delo v procesih razvoja ali nadgradnje, izboljšajo kakovost izdelkov, omogočajo sprotno pripravo dokumentacije, izboljšajo spremljanje dela, nadzor nad potekom dela in porabo virov ter definirajo odgovornost udeležencev procesa razvoja ali nadgradnje informacijskih sistemov.

Metodologija, ki jo izbrana banka uporablja, določa tudi dokumentacijo, ki omogoča pregledno izvajanje razvojnih faz v življenjskem ciklu. Evidenčni list je prvi in osnovni dokument, ki je del dokumentacije projektne mape. Ta dokument se začne izpolnjevati takoj po začetku projekta. Temu listu se tekoče prilagaja dokumentacija, ki vsebuje sklope dokumentov za procese specificiranja zahtev, načrtovanja, izdelave, testiranja in uvedbe.

Sklop dokumentacije, preko katere se vodi postopek specificiranja zahtev, vsebuje dokumente, ki obsegajo predlog projekta, zagonsko koncepcijo projekta, poslovni proces, plan projekta ter plan kakovosti.

Sklop dokumentacije za načrtovanje obsega sledeče dokumente: plan konfiguracije, načrt informacijske rešitve, plan testiranja, analiza informacijskih tveganj, verifikacija in validacija.

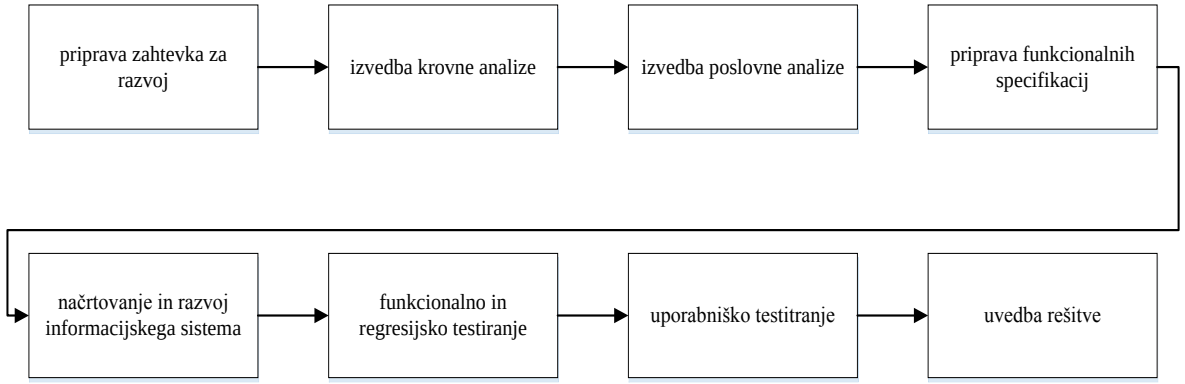
Dokumentacija, ki je namenjena podpori procesa izdelave informacijske rešitve, vsebuje dokument za izdelavo in testiranje podatkovne baze, programiranje in testiranje modulov in programov, pripravo distribucijskega paketa, določitev verzije, tehnično navodilo, uporabniško navodilo ter interno testiranje.

Paket dokumentov, ki so del procesa testiranja informacijske rešitve, vsebuje dokumente za dokumentiranje plana testiranja, testnih primerov in uporabniško sprejemnih testov, poročila o uporabniško sprejemnem testu ter analizo tveganj informacijske tehnologije.

Kot zadnji del postopka razvoja oz. nadgradnje informacijske rešitve nastopi faza uvajanja. Ta faza je podprta z dokumenti za šolanje uporabnikov in vzdrževalcev sistema, uvedbo sistemain aktiviranje sistema v produkcijskem okolju ter poročilom o uvedbi.

Proces razvoja informacijskega sistema je v osnovi viden že iz zgoraj opisane dokumentacije. Za uspešen razvojni cikel je potrebno, da tradicionalne faze razvoja potekajo vzporedno. Na začetku razvoja celotna ekipa analizira uporabniško zahtevo, ki jo bodo v tem ciklu razvijali. Ko celotna ekipa zahtevo enako razume, se preide na naslednji korak, ko poslovni analitik izvede podrobno poslovno analizo in pripravi primer uporabe, načrtovalec pripravi načrt rešitve z vsemi specifikacijami in razvijalci začnejo programirati. Vsa vprašanja in nejasnosti se rešuje sproti (Proces razvoja, 2016).

*Slika 6: Izvajanje procesa razvoja*




*Vir: Izbrana banka, Izvajanje procesa razvoja z IT komponento, 2016.*

### 4.1.4 Specifikacija zahtev

Poslovno idejo za razvojne potrebe, operativne potrebe ali identifikacijo napake lahko poda vsak zaposleni, pri čemer je treba jasno identificirati tudi lastnika zahtevka, ki bo imel interes izvedbe in bo odgovoren za vsebinski del izvedbe.
Podlaga za poslovno idejo je lahko:

- zakonsko ali drugače regulatorno pogojena,
- usmerjena v rast ali racionalizacijo poslovanja ali
- uresničevanje strategije banke.

Poslovna ideja mora vsebovati zlasti: podlago za poslovno idejo, opis sedanjega stanja, ciljno stanje, koristi ter prednosti, pridobljene z implementacijo predloga, in morebitna tveganja. Predpisane karakteristike poslovne ideje zapišemo v predpisan obrazec v izbrani aplikaciji (podrobnosti navajamo v navodilih za izpolnjevanje poslovnega zahtevka, ki so priloga temu dokumentu). Kakovost opisa in argumentacija ideje sta ključni za jasno informiranje vseh deležnikov glede pričakovanj lastnika zahtevka, kar bo v kasnejših fazah procesa omogočilo boljšo izvedbo z manj napakami.

Lastnik zahtevka mora ob pričakovanih spremembah procesa skladno z metodologijo obvladovanja poslovnih procesov sodelovati s procesnikom iz oddelka za razvoj organizacije, za kakovostnejšo opredelitev elementov zahtevka pa lahko k sodelovanju povabi tudi poslovnega analitika iz oddelka za poslovno analizo. Prav tako je zaželeno, da lastnik zahtevka poslovno zahtevo uskladi s strokovnimi službami banke, ko je to potrebno. V primeru, da takega soglasja pri usklajevanju ni mogoče doseči niti v kasnejši fazi izvajanja poslovne analize, lahko o izvedbi odloča razvojni svet.

Ko je poslovna ideja dovolj dobro opredeljena ter usklajena s ključnimi deležniki, jo direktor sektorja lastnika zahtevka po skrbnem pregledu v aplikaciji tudi formalno potrdi.
S tem dobi ideja status poslovne zahteve in jo aplikacija posreduje v oddelek poslovnih analiz. Rezultat je izpolnjen in potrjen obrazec o poslovni zahtevi.

Vodje skupin oddelka za poslovno analizo pregledajo poslovno zahtevo. Poslovno zahtevo pregledajo zlasti z naslednjih vidikov:

- ali je dovolj razumljiva in vsebuje vse v točki 1.1 predpisane zahteve, zlasti pa ali vsebuje dovolj informacij in podatkov za izvedbo poslovne analize,
- ali so opredeljene koristi in prednosti,
- ali so opredeljena morebitna tveganja neizvedbe,
- ali so dodani dokumenti, ki so potrebni za izvedbo poslovne analize,
- ali vsebuje ostale ključne elemente zahtevka.

Če so podatki pomanjkljivi, bodo poslovno zahtevo z ustrezno razlago vrnili lastniku zahtevka v dopolnitev, v nasprotnem primeru pa bodo določili poslovnega analitika, ki bo zahtevek sprejel v analizo. Rezultat je posredovan zahtevek imenovanemu krovnemu analitiku.

Naslednji korak je izvabljanje uporabniških zahtev. Pomeni pa izvajanje različnih aktivnosti, ki poslovnemu analitiku omogočijo definiranje dejanskih poslovnih potreb. Pri izvabljanju

se uporabljajo različne tehnike poslovne analize, kot so intervjuji in ciljne skupine. Najpomembnejše je postavljanje t. i. »zaprtih vprašanj« in sprotno potrjevanje enakega razumevanja. Po zaključku te faze morajo biti znani odgovori na vprašanji, kaj je potrebno razviti in zakaj je razvoj potreben. Identificirani in vključeni v usklajevanje morajo biti vsi deležniki razvoja. V izvabljanju zahtev sodelujeta lastnik zahtevka in procesnik, če gre za spremembo procesa.

Poslovni analitik popiše obstoječe stanje »kot je« (angl. *AS-IS*, v nadaljevanju AS-IS) in pripravi različne izvedljive alternative razvoja z izdelanim stanjem »kot bo« (angl. *TO BE*, v nadaljevanju TO-BE) in kontekstnimi diagrami toka podatkov. Predlaga cenovno in arhitekturno optimalno alternativo in pripravi argumente izbire. Pri izdelavah alternativ razvoja sodelujejo procesnik in IT načrtovalec.

Poslovni analitik nato pripravi več možnih alternativ in jih razvršča glede na izvedljivost, cenovni vidik in arhitekturno sprejemljivost na:

- priporočljive,
- izvedljive in
- nepriporočljive.

Za vsako od navedenih priporočljivih in izvedljivih alternativ poslovni analitik pripravi oceno dela za celoten razvoj, in sicer podrobno za vsako vlogo v razvojnem procesu. Na podlagi teh podatkov in s strani lastnika zahtevka navedenih koristi izvede analizo stroškov in koristi (v nadaljevanju CBA) posameznih izvedljivih alternativ. Poslovni analitik mora pri presoji alternativ upoštevati strateške, poslovne in objektne cilje banke. Pripravi predlog priporočljive alternative in izbiro utemelji. Oceni trajanje izvedbe priporočljive alternative (angl. *duration*) in možen pričetek razvoja glede na ostale prioritete in naloge v delu. Po potrebi te ocene pripravi tudi za druge izvedljive alternative.

V poslovni analizi najprej opišemo obstoječe stanje AS-IS. V tej fazi sodeluje več akterjev: od procesnikov, tehnologov, načrtovalcev do občasno tudi razvijalcev.
Ko je obstoječe stanje opisano, se naredi predlog izboljšave TO-BE, ta se dopolni še s primeri uporabe (angl. *USE-CASE*).

Uporabniki opišejo poslovne procese v primeru uporabe, kar imenujemo diagram primerov uporabe, ki prikazuje primere uporabe in akterje, ki so z njimi povezani. Izraža uporabniški pogled na sistem. Primeri uporabe predstavljajo potek dogodkov, ki prinašajo želene rezultate akterju, ki jih izzove. Akter je oseba ali drug sistem izven obravnavanega, ki vstopa v interakcijo s sistemom. Akter ni konkretna oseba, ampak predstavlja določeno vlogo, ki jo le-ta predstavlja (npr. prodajni predstavnik). Primer uporabe predstavlja opis določenega dogajanja, ki nastane v interakciji akterja in sistema (Sturm, 1999, str. 60).

Dokument poimenujemo po internih določilih, prvi dve črki sta PU (primer uporabe), nato sledi šifra aplikacije (00XX), zaporedna številka (0001) in ime PU-ja (npr.: PU00XX_0001_Prijava uporabnika). Spodaj podajam primer dokumenta za opis primera uporabe. Na ta način se opišejo vsi primeri uporabe. Diagram primerov uporabe služi prikazovanju povezav med različnimi primeri uporabe in akterji, zato na enem diagramu prikažemo več povezanih primerov uporabe.

*Slika 7: Obrazec za popis primera uporabe*

**1. Opis**

Aplikacija Liste omejevalnih ukrepov in PEP omogoča:
- Iskanje oseb na sankcijskih listah OFAC, EU, FINCEN in UN ter politično izpostavljenih oseb (PEP)
- Urejanje seznama ujemanja podatkov oseb iz Registra komitentov in entitet na sankcijskih listah in listi politično izpostavljenih oseb.
- Definiranje list omejevalnih ukrepov, na katerih izvajamo kontrolo prisotnosti osebe.

**2. Akterji**

**2.1. Primarni akterji**
- Bančni delavci v poslovalnicah in drugih organizacijskih enotah,
- Pooblaščeni delavci Centra za skladnost poslovanja in krepitev integritete.

**2.2. Sekundarni akterji**

**2.3. Drugi akterji**

**3. Začetni pogoji**

Aplikacija Liste omejevalnih ukrepov in PEP mora biti dosegljiva. Vstop v aplikacijo in vpogled v liste je omogočen vsem uporabnikom, dostop do »Administracije« pa samo pooblaščenim osebam.

**4. Končni pogoji**

Uspešen vstop v okolje aplikacije Liste omejevalnih ukrepov in PEP.

**5. Scenarij**

**5.1. Startni dogodek**

V program vstopamo preko seznama WEB aplikacij, kjer v koloni »Liste omejevalnih ukrepov in PEP« izberemo ».
Domenska prijava v aplikacijo zazna uporabnika, ki je prijavljen na računalnik in njegova pooblastila.

**5.2. Osnovni tok**

Aplikacijo uporabljata poslovna sistema izbrane banke.

Na osnovnem ekranu s klikom izberemo »Liste omejevalnih ukrepov in PEP«. Po vstopu v program se odpre začetni ekran s pripadajočim menijem.

Domenska prijava v aplikacijo zazna uporabnika, ki je prijavljen na računalnik in preveri njegova pooblastila.

**Pooblastila**:
- Za iskanje oseb na listah omejevalnih ukrepov in PEP listi ne potrebujemo pooblastila.
- Za dostop do ekrana Iskanje entitete za BŠ preko linka v bančno okence ne potrebujemo pooblastila.
- Pooblaščenec banke za PPDFT in njegov namestnik imata pooblastilo za dostop do Administracije za pregled Liste ujemanja registra – LOU/PEP in urejanje list omejevalnih ukrepov.

*Vir: Izbrana banka, Primeri uporabe, 2015b.*

### 4.1.5 Načrtovanje in arhitektura

Načrtovanje obsega analizo specifikacij, identifikacijo in načrtovanje podsistemov, arhitekturo, logično in fizično podatkovno modeliranje, identifikacijo specifikacij transakcij, dnevnih, mesečnih in letnih poročil.

V koraku načrtovanja opredelimo fizični model sistema, ki bo osnova za uresničevanje. Opredelimo model načrta in model porazdelitve. V modelu načrta podrobno opredelimo razrede, povezave med njimi in dinamično obnašanje sistema. Dokončno opredelimo atribute razreda, opredelimo vidljivost in opišemo metode. Metode lahko opišemo v naravnem jeziku ali psevdo kodi ter programiramo v naslednjemu koraku, lahko pa jih tudi takoj programiramo v izbranem. programskem jeziku. Povezave med objekti dokončno opredelimo glede na številnost, smer navigacije in imenovanje vlog, te pa glede na predvideno okolje uresničitve. Prav tako je treba upoštevati predvideno tehnologijo shranjevanja podatkov, ko načrtujemo razrede, ki izvajajo zapisovanje podatkov v okviru transakcije. Pakete preoblikujemo v podsisteme. Treba je zagotoviti čim manjšo odvisnost med podsistemi, opredeliti ustrezne vmesnike in zagotoviti, da podsistem ponuja pravilno realizacijo operacij, ki so opredeljene z njegovimi vmesniki (Debelak, 2002).

Dinamično obnašanje sistema podrobno opišemo z diagrami zaporedja, diagrami prehodov stanj in diagrami aktivnosti. Tako je model načrta podrobna predstavitev sistema z upoštevanimi lastnostmi okolja, v katerem bo uresničen.

Model porazdelitve vključuje vozlišča, njihove lastnosti in povezave ter začetno razporejanje razredov in podsistemov v vozlišča. Za opisovanje uporabimo diagram porazdelitve.

Načrtovanje razdelimo na več korakov:

- izdelava plana konfiguracije,
- izdelava načrta IT rešitve,
- plan testiranja,
- analiza IT tveganj in
- pregled načrtovanja.

V planu konfiguracije se opredeli posamezne elemente konfiguracije:

- specifikacije uporabniških zahtev,
- entitetni diagram,
- podatkovni slovar,
- dekompozicijski diagram procesov,
- diagram pretoka podatkov,

- opisi poslovne logike,
- specifikacije za implementacijo podatkovne baze,
- specifikacije za implementacijo modulov in programov,
- specifikacije povezav sistema z drugimi sistemi,
- specifikacije procedur za izvajanje paketnih obdelav,
- specifikacije uporabniških vmesnikov,
- izvorna koda,
- objektna koda,
- uporabniška navodila za uporabo sistema in
- tehnična navodila za uporabo sistema.

Vrste razvoja:

- lastni (notranji) razvoj (npr. logično in fizično modeliranje sistema),
- nakup že izdelanih rešitev (»black box« oziroma »of the shelf«),
- razvoj infrastrukture (npr. računalniška omrežja, HW, sistemski SW …) in
- razvoj po naročilu (»outsourceing« – sodelovanje z zunanjim dobaviteljem).

Načrt IT rešitve:

- skladen s tehnološkim standardom,
- vsebuje vse potrebne elemente za integracijo nove rešitve v obstoječi sistem,
- vsebuje procedure za evidentiranje transakcij,
- vsebuje opis strojne računalniške opreme,
- vsebuje opis komunikacijske opreme (računalniško omrežje),
- vsebuje opis programske opreme (sistemska, aplikativna) in
- vsebuje opis kadrovskih in organizacijskih potreb informatike (znanja).

Faza načrtovanja in faza poslovne analize morata biti med seboj povezani. Faze se med seboj prekrivajo, zato je v teh fazah zelo pomembno delo načrtovalca. Kot profil so se izkazali za zelo dobre bivši informatiki s širokim spektrom znanja in izkušnjami s poslovnega področja.

V izbrani banki poteka proces načrtovanja tako, da se najprej opredeli in pripravi postavljanje arhitekture IS, podatkovno modeliranje, sistemske specifikacije za razvijalce – specifikacije vmesnikov, transakcij, funkcij in storitev ter sekvenčni diagrami.

Načrtovalec IS v sodelovanju s sodelavci (arhitektom, BE razvijalcem, FE razvijalcem, DBA, sistemskim inženirjem) in analitikom v oddelku za poslovno analizo izvede fazo načrtovanja informacijskega sistema. Za načrtovanje informacijskega sistema načrtovalec IS uporabi pripravljene funkcionalne specifikacije za načrtovalce in razvijalce:

- primeri uporabe so  skladni s standardi za definiranje funkcionalnosti IS,
- primeri uporabe in predloga za pisanje navodil za izdelavo specifikacij,
- primeri uporabe oz. specifikacije za razvoj,
- primeri ekranskih slik,
- poslovna pravila,
- primeri izpisov in poročil,
- testni scenariji za izvedbo funkcionalnega testa in
- enolično definirana prioriteta v okviru seznama vseh zahtev.

Rezultat so sistemske specifikacije, ki vsebujejo:

- definirano arhitekturno shemo na več nivojih,
- fizični podatkovni model, ki je pripravljen skladno z metodologijo podatkovnega modeliranja,
- sekvenčne diagrame, pripravljene skladno s standardi za opis poteka delovanja informacijskega sistema s tehniko UML, in
- specifikacije posameznih enot sistema (funkcije, transakcije, storitve, obdelave …), skladne s standardi za definiranje programskih vmesnikov.

### 4.1.6 Značilnosti dobrega in slabega IT načrtovanja

Dobro načrtovan sistem je zasnovan tako, da programerji »ne potrebujejo« dodatne razlage oziroma pojasnil. Dokumentacija je vzdrževana, urejena in lahko dostopna, za vodenje verzij dokumentacije se uporabljajo sistemi za verzioniranje. S tem pripomoremo tudi k enostavnejšemu prehajanju kadrov.

Iz zgodovine računalništva so znani številni poskusi določitve kriterijev, ki bi omogočali ocenjevanje kakovosti načrta – za objektno načrtovanje sta nabor takih kriterijev določila Coad in Yourdon. Z leti pa je postajalo jasno, da je kakovost načrta pravzaprav odvisna od konteksta oziroma ciljev, ki jih želimo z načrtovanjem doseči. Ne da bi se spuščali v podrobnosti kakovosti načrtovanja, lahko intuitivno sklepamo, da je dober načrt tisti načrt, ki izvajalcu daje dobro podlago za izvedbo. Podobno kot gradbeni načrt omogoča izvajalcu, da se osredotoči na izvedbo posameznih delov in se ne ukvarja z ugotavljanjem, kako naj posamezni deli stojijo skupaj, kakšnih dimenzij in oblik naj bodo, kakšna naj bo izbira materiala ipd. Podobno je v računalništvu. Programer implementira posamezne dele programske opreme, kako naj bodo ti povezani, v kakšnem vrstnem redu jih je potrebno razviti, kakšne vzorce naj uporabi ipd., pa je določeno z načrtom. Vendar obstaja med načrtovanjem v računalništvu in načrtovanjem v gradbeništvu pomembna razlika. Ko pripravljamo načrt za gradnjo nekega objekta, se namreč ne oziramo na možnost, da se bo objekt morda v prihodnje spremenil, ker se to tudi v praksi redko dogaja. V računalništvu pa je ravno nestabilnost zahtev največji problem. To še posebej velja za poslovne rešitve, ki so

zaradi dinamičnega okolja, v katerem delujejo, neprestano izpostavljene spremembam. V računalništvu je zato ena temeljnih lastnosti dobrega načrta prav odprtost za spremembe in prilagoditve (Bajec & Krisper, 2003).

Kako torej zagotoviti, da bo načrt informacijske rešitve ustrezal trenutnih zahtevam, obenem pa bo odprt za morebitne spremembe in razširitve? Kako ugotovimo, da je načrt slab, kako se to vidi? Načrtovalske napake, ki se pogosto omenjajo kot simptomi slabega načrtovanja, so (Bajec & Krisper, 2003):

- togost (angl. *Rigidity*): da je načrt tog, pravimo takrat, ko ne omogoča sprememb in razširitev oziroma le-te zahtevajo veliko truda;
- krhkost (angl. *Fragility*): krhkost načrta se pokaže, kadar spremembe omejenega dela načrta vplivajo na spremembe drugih delov. Krhkost se močno poveča z odvisnostjo med moduli sistema. Večja kot je odvisnost, večja je krhkost sistema;
- neprenosljivost (angl. *Immobility*): načrt je neprenosljiv, kadar ga je težko ponovno uporabiti;
- viskoznost (angl. *Viscosity*): ko se pojavi potreba po spremembi, imamo navadno več možnosti za njeno implementacijo. Način, ki ohranja načrt, je optimalen, način, ki načrt spreminja in s tem vpliva na številne module, pa je nezaželen. Da je načrt viskozen, pravimo takrat, ko želeno spremembo veliko lažje uveljavimo na neustrezen način (s spremembo načrta) kot na ustrezen način;
- nepotrebna kompleksnost (angl. *Needless complexity*): nepotrebna kompleksnost je pogosta napaka pri načrtovanju. Da bi sestavili čim bolj splošen in uporaben sistem, načrtovalci nemalokrat načrtujejo funkcionalnosti na zalogo;
- nepotrebno kopiranje (angl. *Needless repetition*): ena od posledic hitrega razvoja je kopiranje posameznih delov načrta (t. i. mouse abuse). Takšna praksa privede do težav in napak pri vzdrževanju sistema;
- nejasnost, nerazumljivost (angl. *Opacity*): poleg kopiranja je posledica hitrega razvoja tudi nerazumljivost ali nejasnost načrtov. Z nerazumljivim načrtom zgubimo praktično vse koristne lastnosti načrtovanja.

### 4.1.7 Podatkovno modeliranje

Podatkovno modeliranje je ena od osnovnih dejavnosti načrtovanja vseh sistemov in aplikacij, ki se razvijajo v okviru lastnega razvoja v banki ali »po naročilu« pri zunanjih ponudnikih. Izjema so kupljeni programski paketi, kjer podatkovni model navadno ni na voljo, saj se v njem skriva del proizvajalčevega know-howa. Tak podatkovni model obravnavamo kot črno škatlo (angl. *black-box*) in ga proučujemo zgolj preko podatkov, ki jih produkt izmenjuje z okolico s pomočjo vhodnih in izhodnih vmesnikov.

V izbrani banki veljajo pravila podatkovnega modeliranja za sistem DB2 Z/OS.

Splošna pravila za podatkovno modeliranje za ta sistem so:

- poimenovanje elementov (entitet, atributov, relacij) v podatkovnem modelu,
- veljavni podatkovni tipi in standardizirana polja,
- definiranje baznih objektov (tabela, view, indeks, trigger, funkcija …) in
- razlikovanje med aktivnimi in arhivskimi podatki (poimenovanje arhivskih tabel).

Velja, da pri poimenovanju elementov v podatkovnih modelih ne uporabljamo šumnikov. Splošna pravila opredeljujejo poimenovanje podatkovnih objektov za DB2 Z/OS podatkovni sistem.

Logični podatkovni model se praviloma definira na osnovi podatkovnih potreb poslovnega sistema, opredeljenih v konceptualnem modelu podatkov in/ali v modelu poslovnih procesov, kjer se podatkovne potrebe definirajo kot parcialni pogled na podatkovne potrebe z vidika posameznih poslovnih procesov.

Logični podatkovni model predstavlja bolj podrobno raven opredelitve podatkovnih zahtev poslovnega sistema, zato je faza logičnega podatkovnega modeliranja tudi verifikacija in dopolnitev podatkovnih zahtev, opredeljenih na predhodnih ravneh.
Logični podatkovni model se od konceptualnega podatkovnega modela razlikuje po tem, da je strukturiran na način, ki je prevedljiv v fizični podatkovni model, seveda pa je le kakovosten logični podatkovni model lahko osnova za kakovosten dizajn baze podatkov.

V splošnem logični podatkovni model:

- predstavlja sliko podatkov, ki jih želi poslovni sistem spremljati v informacijskem sistemu in zato o njih hraniti zapise v bazi podatkov,
- je neodvisen od ciljne implementacijske tehnologije in njenih omejitev,
- je neredundanten (ali z minimalno kontrolirano redundanco, v logični model vgrajeno v obliki t. i. »izvedenih« atributov, »izvedenih« entitet in dodatnih relacij),
- je v vsaj 3. normalni formi in
- nima relacij s kardinalnostjo M:M.

Entiteta je »nekaj« za poslovni sistem tako pomembnega, da želi to enoznačno identificirati ter o tem zbirati in spremljati podatke (kot na primer KOMITENT) ali da želi po tem podatke klasificirati, razvrščati, diferencirati, grupirati ipd. (kot na primer VRSTA PRISPEVKA, TIP IZPLAČILA, DRŽAVA).

Če v realnem svetu med dvema entitetama obstaja neposreden odnos, ki izhaja iz povezanosti poslovnih podatkov v takih dveh entitetah, med njima vzpostavimo povezavo (angl. *relationship*). Ta izraža:

- ali identifikacijsko odvisnost
- ali neidentifikacijsko odvisnost, ki je lahko bodisi obvezna bodisi opcijska eksistenčna odvisnost entitete, h kateri »vlečemo« povezavo, in sicer od entitete, od katere »vlečemo« povezavo.

Ob vzpostavitvi identifikacijske odvisnosti se primarni ključ »nadrejene« entitete kot tuji ključ avtomatsko prenese v odvisno entiteto in postane del primarnega ključa odvisne entitete (in nato naprej v vse entitete, ki so od nje odvisne).

Ob vzpostavitvi neidentifikacijske odvisnosti se primarni ključ »nadrejene« entitete kot tuji ključ avtomatsko prenese v odvisno entiteto (ne pa naprej v vse entitete, ki so od nje odvisne).

Ime relacije se zapisuje z malimi črkami. Šumnikov pri poimenovanju ne uporabljamo. Relacija ima definicijo v primeru dvoumnosti (npr. dve relaciji med istima entitetama).
Iz definicije entitete v logičnem podatkovnem modelu izhaja, da mora imeti vsaka entiteta primarni ključ (PK), ki služi za enoznačno identifikacijo pojavljanj entitete (oziroma zapisov v podatkovni bazi) in se avtomatsko prenaša v fizični podatkovni model.

- Primarni ključ neodvisne entitete

Entitete, ki so »na vrhu« hierarhije odvisnosti (so torej neodvisne), morajo praviloma imeti atomaren (nedeljiv) primarni ključ. Le-ta se, če je to mogoče, izbere izmed enega od poslovnih atributov entitete, ki so »kandidati za primarni ključ entitete«. Kandidat za primarni ključ je lahko atribut, ki enoznačno identificira entiteto, ima izpolnjeno vrednost za vsa pojavljanja entitete, njegova vrednost se skozi življenjski ciklus entitete ne spreminja. Tako izbrani ključ je t. i. »naravni ključ« entitete.

Če noben od poslovnih atributov ne odgovarja kriterijem za primarni ključ entitete, definiramo t. i. »surogat« ključ z imenom npr: »ID_STORITEV«.

- Primarni ključi odvisne entitete

Ključi za identifikacijsko odvisno entiteto se sestavijo s ključi njenih staršev in (če je to za enoznačno identifikacijo pojavljanj entitete potrebno) z dodatnim lastnim ključem odvisne entitete, ki je izbran izmed obstoječih naravnih atributov (ki odgovarjajo kriterijem za določanje dela primarnega ključa entitete). Če to ni možno, se kreira dodatni lastni »umetni ključ« v okviru ključa nadrejene entitete. (Npr. pri entiteti POSTAVKA NAROCILA KUPCA se za ključ, ki enoznačno identificira posamezno pojavljanje entitete, določi sestavljeni ključ, ki vsebuje ključe entitet staršev – npr. »Stevilka naročila kupca« – in

dodatni lastni ključ – npr. »Stevilka postavke narocila kupca«, numerirana v okviru NAROCILA KUPCA).

Za entitete, ki so od vseh svojih staršev odvisne zgolj eksistencialno (in ne nujno tudi identifikacijsko), se za primarni ključ lahko definira tudi identifikacijski »surogat« ključ, vendar je potrebno za takšen način določanja primarnega ključa odvisnih entitet od primera do primera skrbno pretehtati, drugače lahko s tem po nepotrebnem znižujemo nivo podatkovne integritete.

- Alternativni ključ entitete

Razen primarnega ključa lahko entiteti določimo tudi alternativni ključ, ki je lahko izbran izmed preostalih »kandidatov za primarni ključ entitete«. Za alternativni ključ se lahko izbere enega ali več poslovnih atributov. To nam daje večjo fleksibilnost pri izbiri, katere vrste ključ naj se prenese (»migrira«) v odvisne entitete.

Transformacija logičnega podatkovnega modela v izhodiščni oziroma inicialni fizični podatkovni model poteka avtomatsko, saj inicialni fizični model nastaja istočasno z logičnim modelom. Zato je vpogled v inicialni fizični model pravzaprav ves čas dostopen. Ko je zaključen razvoj logičnega modela, je istočasno zaključen tudi inicialni fizični model.

Fizični podatkovni model je:

- slika vseh podatkov, ki bodo (oziroma so) shranjeni v bazi podatkov,
- odvisen od tehnologije in tehnoloških standardov in od vseh s tem povezanih omejitev (tj. od konkretnih sistemov za upravljanje baz podatkov ter od standardov informacijske arhitekture) za razliko od logičnega podatkovnega modela.

Od logičnega podatkovnega modela se razlikuje tudi po tem, da je vanj vgrajena t. i. kontrolirana redundanca, ki je potrebna za doseganje ustrezne odzivnosti sistema. Le-ta se v izhodiščni fizični podatkovni model, generiran iz logičnega podatkovnega modela, vgradi pri postopku t. i. transformacije inicialnega fizičnega podatkovnega modela.

Z avtomatsko transformacijo iz elementov logičnega modela nastanejo naslednji glavni elementi fizičnega podatkovnega modela:

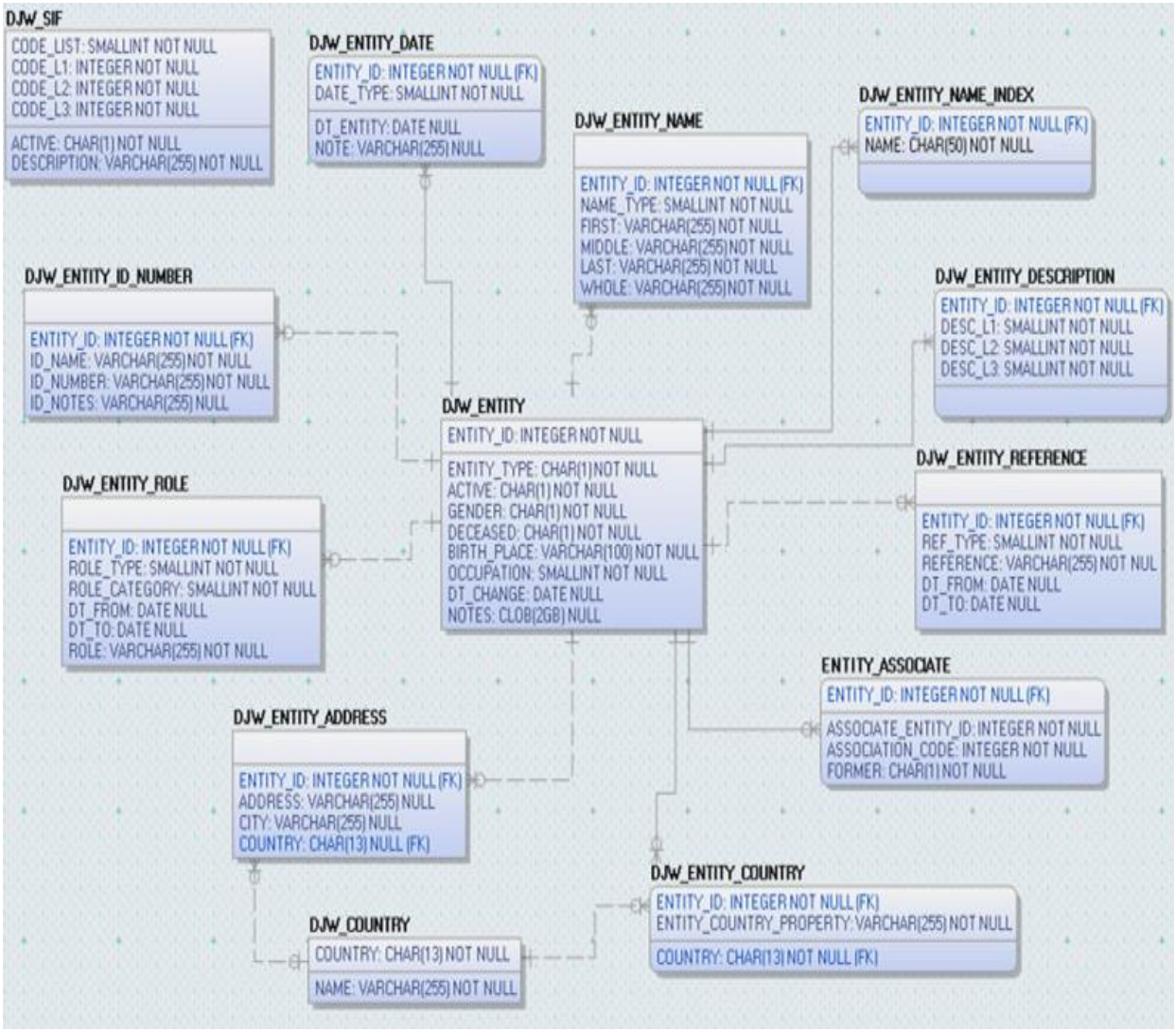
- tabele,
- kolone,
- relacije,
- indeksi,
- pravila za validacijo in

- privzete vrednosti kolon.

Predpogoj za njihovo avtomatsko transformacijo so določeni standardi za avtomatsko mapiranje logičnih imen v fizična.

Tabela je zbirka, v kateri so fizično shranjeni vsi podatki, s katerimi se v aplikaciji razpolaga. Vse tabele skupaj predstavljajo bazo podatkov. Tabele so lahko uporabnikom prikrite (nepoznane), do podatkov iz tabel pa lahko dostopajo preko drugih objektov (procedure, obrazci). Podatki v tabeli so shranjeni v zapisih. Zapis je zaporedje podatkovnih lastnosti elementov ali polj s podatki, ki vsi skupaj opisujejo kakšno stvar, osebo ali dogodek (Gradišar, 226).

*Slika 8: Fizični podatkovni model za razvoj aplikacije preprečevanja pranja denarja*




*Vir: Izbrana banka, Podatkovni model, 2015c.*

### 4.1.8 Poslovno - informacijska in IT arhitektura

IT arhitektura je del poslovno - informacijske arhitekture (angl. *Enterprise Architecture*, v nadaljevanju PIA.

PIA je formalen opis sistema ali podroben plan sistema na nivoju komponent, ki usmerja njegovo implementacijo. Zajema strukturo komponent, njihovo medsebojnih povezav in načel ter smernic, ki vodijo njihovo načrtovanje in evolucijo skozi čas:

Pojem poslovno - informacijska arhitektura se je pojavil več kot 20 let nazaj in poskuša rešiti dve stvari (Izbrana Banka, 2016):

- zniževanje cene vzdrževanja in poenostavitev kompleksnosti (organizacije zaradi kompleksnosti in formacijskih sistemov zapravijo veliko denarja za njihovo vzdrževanje),
- povečanje dodane poslovne vrednosti, učinkovitosti in izboljšanje poslovnega odločanja. V IT-ju je veliko vlaganj, ker se vloženi denar velikokrat ne povrne.

PIA podjetju zagotavlja medsebojno usklajenost, ki je vidna v (Izbrana Banka, 2016):

- tehničnih ciljih, ki opisujejo platformo, katera je sestavljena iz strojnega, operacijskega in mrežnega sistema ter hrambe. Na platformi se razvijajo aplikacije in na njej tudi tečejo,
- informacijskih ciljih, kjer gre za usklajenost podatkov, struktur, podatkovnih tokov, metod dostopa do podatkov in aplikacij in
- poslovnih ciljih, ki so zapisani v strategiji, načrtih in poslanstvu.

PIA je načrt podjetja, v katerem je opis organizacijske strukture in model poslovanja. Sestavljena je iz poslovne, tehnične in aplikacijske arhitekture. Tehnična in aplikacijska arhitektura skupaj predstavljata IT arhitekturo. IT arhitektura zajema podatkovne, programske in infrastrukturne elemente, njihove lastnosti in medsebojne relacije.

Za PIA je pomembno, da jo imamo, saj je s tem IT podpora enotnejša, učinkovitejša, bolj obvladljiva, infrastruktura pa načrtovana in bolj pregledna.

PIA je proces prevajanja poslovne vizije in strategije v učinkovito prenovo poslovnih sistemov, in sicer s pomočjo ustvarjanja, komuniciranja in izboljšanja ključnih načel in modelov, ki opisujejo bodoče stanje poslovnega sistema in omogoča njegov razvoj (Gartner, 2016).

Posel je predstavljen kot množica med seboj povezljivih komponent, ki podpirajo poslovne aktivnosti v različnih delih organizacije, kar pripomore k večji fleksibilnosti in učinkovitosti njenega delovanja. Te poslovne komponente skupaj s poslovnimi procesi predstavljajo neko storitev. Poslovni model vsebuje tudi definicijo podatkov, ki so potrebni za ta posel. Na ta način so predstavljene osnovne poslovne entitete in relacije med njimi. To je poslovna arhitektura.

Aplikacijska arhitektura izdela aplikacije za implementacijo poslovnega modela in procesov. Lahko so to dopolnjene obstoječe »legacy« aplikacije, remote aplikacije ali nove aplikacije. Zajema tudi načine kako uporabniki dostopajo do poslovnih storitev, lahko je to preko web vmesnikov, portala, mobilnih naprav itd.

Zadnji nivo predstavlja implementacija aplikacijske arhitekture z uporabo infrastrukturne arhitekture. Ta opisuje, kako so procesi, storitve in aplikacije razporejene na obstoječ middleware in strojne platforme ter poskrbi za optimizacijo, virtualizirane resurse, ter definira politiko predpisov teh virov za posamezne aplikacije itd.
Na Sliki 9 je prikazana usklajenost med poslovno in IT arhitekturo, in sicer prikazuje različne dimenzije postavitve nove rešitve od zgornjega nivoja – poslovne strategije, procesov, skozi aplikacije do implementacije na določeni platformi.

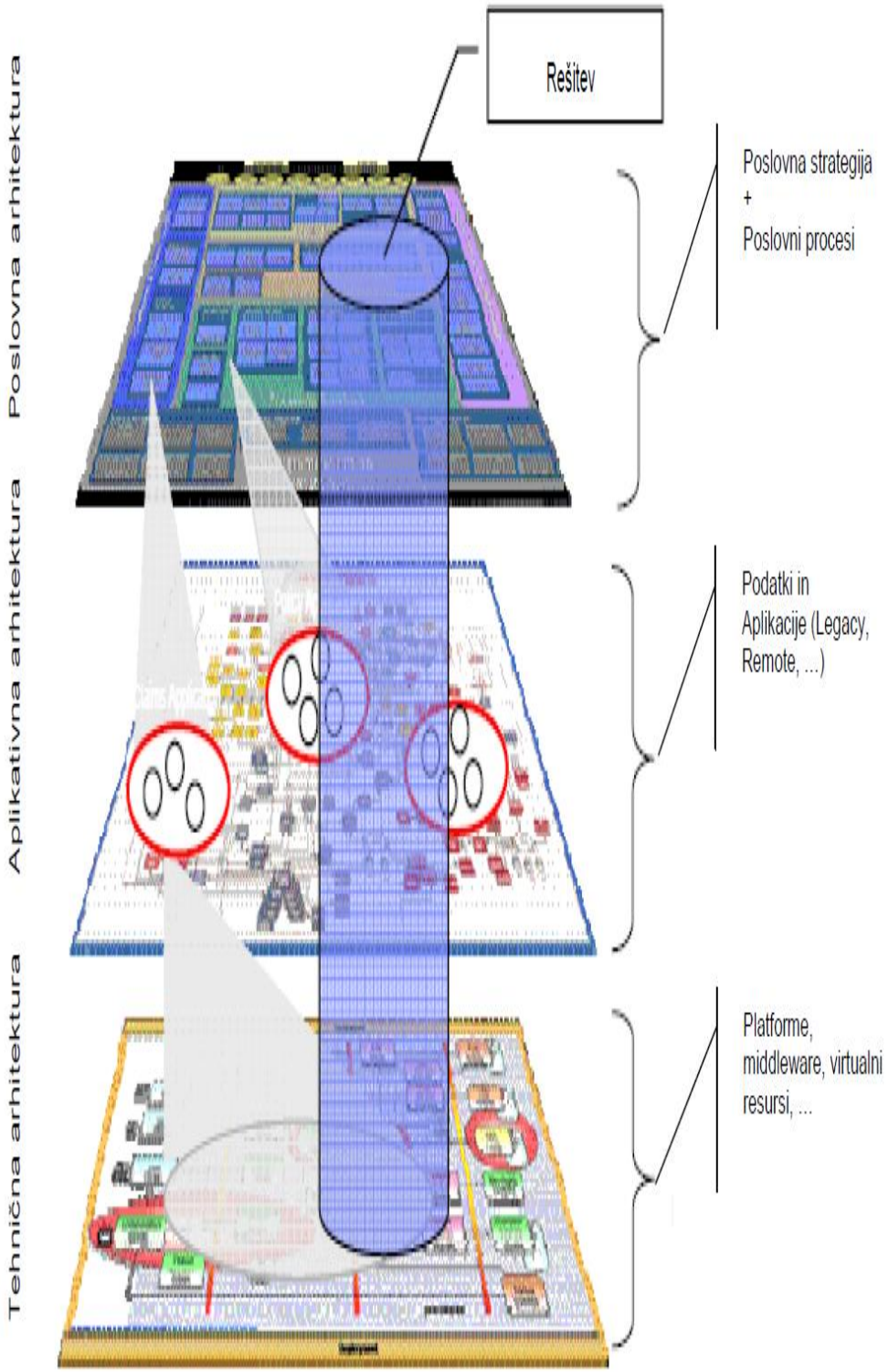
PIA je običajno prikazana v obliki raznih modelov, ki na razumljiv način prikazujejo koncept dejanskega kompleksnega sistema in uporabljajo določene metodologije. 90% vseh organizacij danes uporablja enega od naslednjih štirih modelov oz. frameworkov:

- Zachman Framework, v 80-ih letih ga je razvil John Zachman in je še danes zelo pomembna. Cilj sheme je izbrati popoln opisani sistem, ki bi omogočil učinkovito komunikacijo vsemi udeleženci,
- TOGAF (*angl*. The Open Group Architectural Framework), ta PIA-jo razlaga celostno. Temelji na tehničnem arhitekturnem ogrodju za upravljanje informacij,
- FEA (*angl.* The Federal Enterprise Architecture za vladne organizacije) je standard za razvoj PIA v zveznih agencijah in standard njihovega medsebojnega povezovanja,
- Gartner Methodology (prej se je imenoval Meta Framework).

V izbrani banki je vzpostavljena IT arhitektura. Njeni rezultati so modeli, ki na razumljiv način prikazujejo koncept dejanskega kompleksnega sistema. Modele IT arhitekture uporablja vodstvo, udeleženci razvoja IT rešitev ter drugi uporabniki sistema.

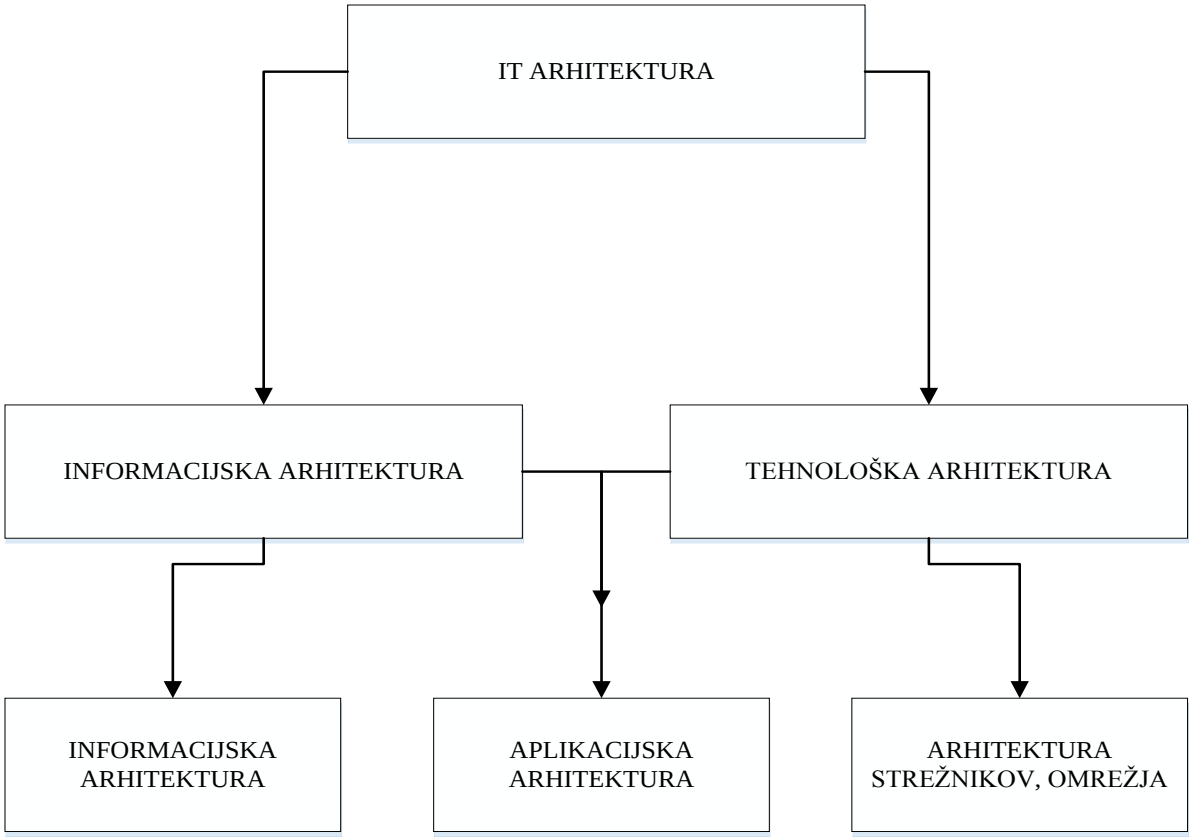
IT arhitektura izboljšuje razumevanje IT podpore in poslovnih zahtev. To pomeni, da je uskladitev medsebojnih pričakovanj eden izmed najpomembnejših učinkov IT arhitekture

*Slika 9: Usklajenost rešitve med poslovno in IT arhitekturo*




*Vir: Izbrana banka, Interni standard IT arhitekture, 2014.*

*Slika 10: IT arhitektura proučuje podatke, informacijske tokove, aplikacije ter tehnološko infrastrukturo*




*Vir: Izbrana banka, Interni standard IT arhitekture, 2014.*

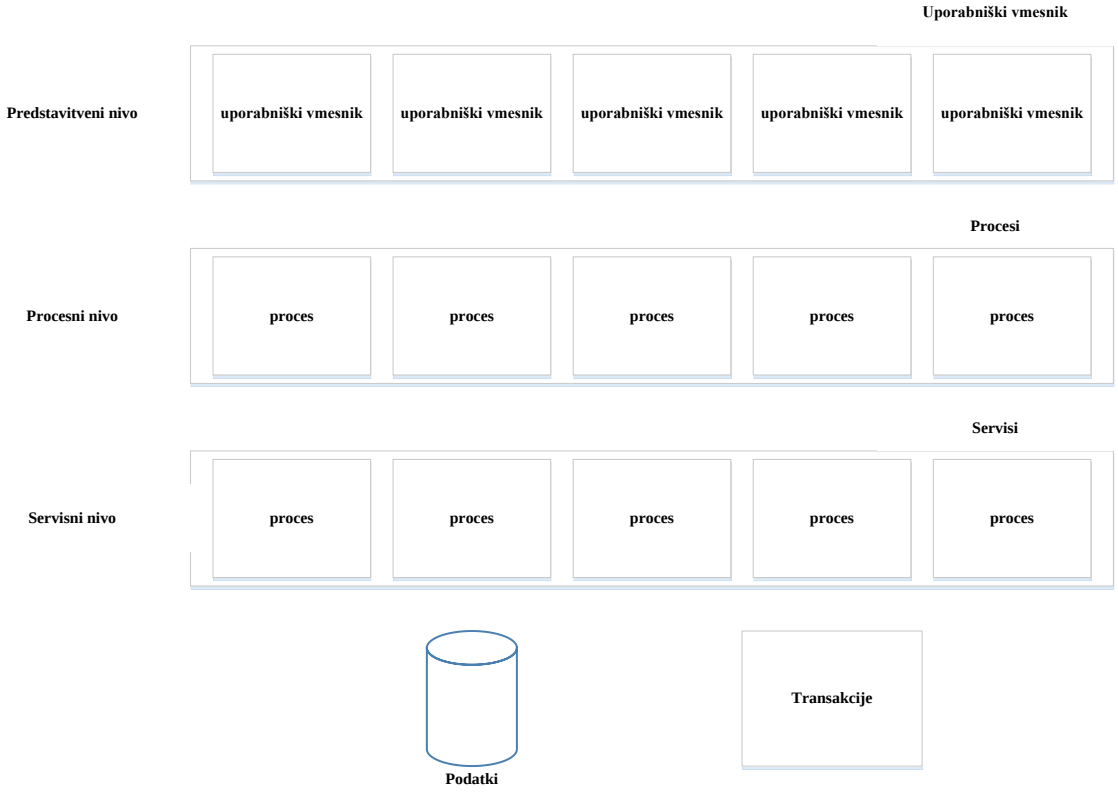
Na ta način hitreje dosegamo poslovne cilje, uvajamo nove rešitve, bolje načrtujemo vire in izboljšujemo komuniciranje med poslovnim in tehnološkim delom banke v dnevnem operativnem delu. IT arhitektura pripomore k enotnejšim rešitvam poslovanja.
IT arhitektura opisuje podprtost poslovanja banke z različnimi elementi informacijske tehnologije, kot so: podatki in informacije, aplikacije, strežniki, odjemalci, omrežja, sistemska okolja in orodja itd.

Zato v okviru IT arhitekture obstaja več (pod)področij:

- informacijska arhitektura (oz. podatkovna arhitektura) je osredotočena na potrebe uporabnikov po informacijah. To pomeni hranjenje in obdelavo podatkov s pomočjo aplikativne podpore. Te potrebe so podprte s storitvami, ki jih zagotavljajo aplikacije, ki obdelujejo poslovne podatke. Vse pa se odvija na tehnološki infrastrukturi;
- aplikacijska arhitektura; pri njej je splošna usmeritev razvoj novih aplikacij v skladu s storitveno usmerjeno arhitekturo (angl. *Service-oriented architecture*, v nadaljevanju SOA) povsod, kjer je to smiselno in cenovno upravičeno. Vrstni red uvajanja principov SOA je od spodaj navzgor:

- servisni nivo: **i**zgradnja enotnih servisov za pogosto uporabljane funkcije, ki se trenutno podvajajo v različnih sistemih, spodbujanje ponovne uporabe že izgrajenih servisov;
- procesni nivo: izločitev procesne logike za pomembne poslovne procese na ločen nivo;
- predstavitveni nivo: **i**zkoriščanje in ponovna uporaba že implementiranih procesov in servisov z nižjih nivojev v namenskih uporabniških vmesnikih;
- tehnološka arhitektura: zajema omrežja, strežnike, odjemalce, operacijske sisteme, baze podatkov itd.

*Slika 11: Servisno usmerjena arhitektura*




*Vir: Izbrana banka, Interni standard IT arhitekture, 2014.*

IT arhitektura mora na vseh nivojih upoštevati tudi pravila informacijske varnosti, neprekinjenega poslovanja, elektronskega arhiviranja itd. Poiskati je potrebno stične točke med različnimi pogledi na IT arhitekturo in širše - na poslovno arhitekturo banke (pogledi poslovnega ali IT stratega, procesnika, poslovnega analitika, načrtovalca, razvijalca, končnega uporabnika, so namreč lahko med seboj zelo različni).

Stične točke, ki jih omenja npr. Zachmann-ov model PIA-e, so navadno: podatek, proces ali lokacija, lahko pa tudi ljudje, čas ali planiranje. Kadar model ni izdelan dovolj podrobno, uporabimo začasno druge stične točke, ki so na voljo.

### 4.1.9 Arhitektura novega sistema

Za uvedbo novih sistemov je potrebno aktivno delo, mnogo znanja, človeških resursov in predvsem denarja. Pri bankah velja tudi pravilo, da tovrstni sistemi niso nikoli do konca razviti. Z zaključkom implementacije glavnega sistema in vseh podsistemov v produkcijsko okolje ter uvedbo njihove medsebojne povezljivosti delo še zdaleč ni končano, temveč se kontinuirano nadaljuje z razvojem novih funkcionalnosti in morebitnih novih vmesnikov oz. podsistemov. Zaradi tega se tovrstne organizacije, v katerih informatizacija predstavlja nenehno dejavnost, soočajo z raznovrstnimi težavami, kot so nezdružljivost posameznih podsistemov, nezdružljivost informacijske infrastrukture (računalniškega omrežja, strežnikov in vmesne programske opreme), nezdružljivost podatkovnih baz različnih uporabniških programov itd. Da bi se izognili temu, je potreben dober načrt, ki vsebuje vse tisto, česar se moramo pri gradnji posameznega dela držati, da bo združljiv s celoto. Še več, v takem načrtu lahko opredelimo zasnovo celotnega informacijskega sistema, da bo služil ciljem podjetja (Gradišar, Jaklič, Turk, 2007).

Podatkovna arhitektura je pomemben del arhitekture poslovnega sistema, saj so podatki in iz njih izvedene informacije eden izmed najbolj pomembnih virov poslovnega sistema.

Ločimo naslednje ravni podatkovne arhitekture poslovnega sistema:

- poslovna področja,
- poslovni pojmovnik,
- konceptualni podatkovni model,
- logični podatkovni model,
- fizični podatkovni model in
- definicija baze podatkov.

Takšna večnivojska podatkovna arhitektura izvira iz potrebe po enoznačni opredelitvi podatkovnih virov skozi vse ravni arhitekture poslovnega sistema. Podatkovni modeli so tudi v storitveno orientirani arhitekturi informacijskega sistema eden izmed njegovih najpomembnejših temeljev. Omogočajo konsistentno uskladitev posameznih podmodelov, ki predstavljajo parcialni pogled na podatke z vidika udeležencev različnih poslovnih procesov na ravni celotnega poslovnega sistema.
Neprecenljiva lastnost zgornjih ravni podatkovne arhitekture (do vključno logičnega podatkovnega modela) je, da jih lahko razumejo tako informatiki kot tudi poslovni domenski strokovnjaki in uporabniki informacijskega sistema, zato so nenadomestljiv temelj za jasno

medsebojno komunikacijo, tako med strokovnimi domenskimi strokovnjaki samimi kakor tudi med njimi in med informatiki.

Umestitev aplikacije v obstoječe okolje je pomembna faza pri načrtovanju. Slika 12 prikazuje arhitekturno zasnovo pri aplikaciji za preprečevanje pranja denarja. Najvišja raven arhitekture je predstavitvena raven, ki se izvaja na delovni postaji v spletnem brskalniku. Iz aplikacijskega strežnika se kliče transakcijsko raven, iz transakcijske pa posamezne podsisteme oziroma storitve.

Uporabniško raven aplikacije predstavlja spletni brskalnik s povezavo do aplikacijskega strežnika. Na vsakemu strežniku mora biti dodatno nameščena še »Silverlight« komponenta. Uporabniki dostopajo do aplikacije preko spletnega brskalnika. Glede na standarde izbrane banke je to Internet Explorer.

Aplikacijsko raven predstavlja spletni strtežnik (angl. *Internet Information Services,* v nadaljevanju IIS) aplikacijski strežnik, na katerem se povezujejo delovne postaje. Na IIS je nameščena spletna aplikacija, ki zagotavlja vse funkcionalnosti »on-line« dela aplikacije. Spletna aplikacija ne hrani podatkov na aplikacijski in predstavitveni ravni, ampak za izvajanje storitev uporablja integracijsko raven (usmerjevalnik), ki je dostopna preko komunikacijskih komponent.

Spletna aplikacija podpira svoje delo z lokalno shranjenimi šifranti, ki jih pridobi s klici ustreznih CICS transakcij ob zagonu ali po potrebi.

Usmerjevalnik – integracijska raven se nahaja na centralnem računalniku in je raven, ki ponuja nabor CICS transakcij, ki jih proži aplikacijska raven, ki se nahaja na spletnem strežniku. CICS transakcije so implementirane skladno z dogovorjenim skupnim vmesnikom in za svoje izvajanje rabijo delujoče zaledne sisteme.

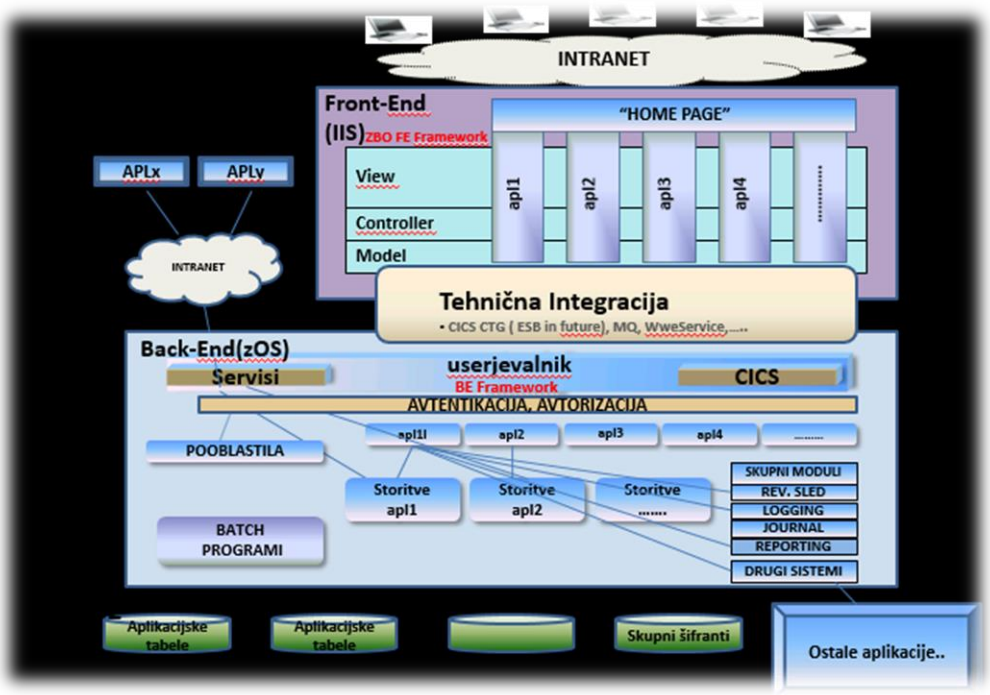
Osnovna arhitektura predvideva minimalno sklopljenost aplikacije z zalednimi sistemi. To dosežemo, če se uporabljajo storitve (transakcije, servisi) zalednih sistemov in se integracija ne izvaja na podatkovni ravni.

Na Sliki 12 so prikazane tudi tehnologije, s katerimi je posamezna raven implementirana. Aplikativna raven je implementirana z Microsoftovimi razvojnimi orodji in IIS strežnikom. Integracijska raven je implementiran v programskem jeziku Cobol in sistemskem okolju CICS.

### 4.1.10 Izdelava

Načrtovalci pripravijo specifikacije za programerje do te mere, da programerji ne potrebujejo nobene druge informacije več. Naloga je le še, da zahteve pretvorijo v izbrano tehnologijo.

*Slika 12: Arhitektura sistema z glavnimi sklopi*




*Vir: Izbrana banka, Tehnična dokumentacija, 2015d.*

Razvoj se deli na dva dela, in sicer na razvoj uporabniškega vmesnika (angl. *Front-End*, v nadaljevanju FE) ter na razvoj zalednega dela z glavno poslovno logiko (angl. *Back-End*, v nadaljevanje BE)

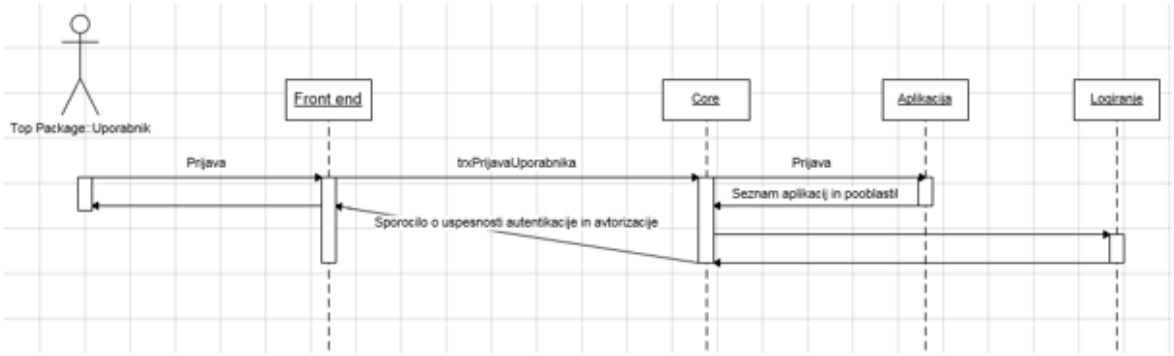
FE razvijalci si iz primerov uporabe zgradijo sekvenčni diagram, ki jim služi kot osnova pri nadaljnjem razvoju. S sekvenčnimi diagrami ponazarjajo zaporedje klicev na različne arhitekturne ravni, nakažejo uporabnikovo izbiro akcije na uporabniškem vmesniku, ponazorijo klic ustrezne transakcije in prikažejo klice ustreznih sistemov ter ne nazadnje ponazorijo vračanje rezultatov.

Diagram zaporedja prikazuje časovno zaporedje sporočil med objekti sistema z zunanjimi akterji. Vsebuje objekte, zveze in sporočila na ravni ene transakcije.

Poleg primerov uporabe in diagramov zaporedja FE razvijalci dobijo še ekranske maske, na katerih je razvidno, katere transakcije se kliče in katere so obvezne kontrole glede na polja.

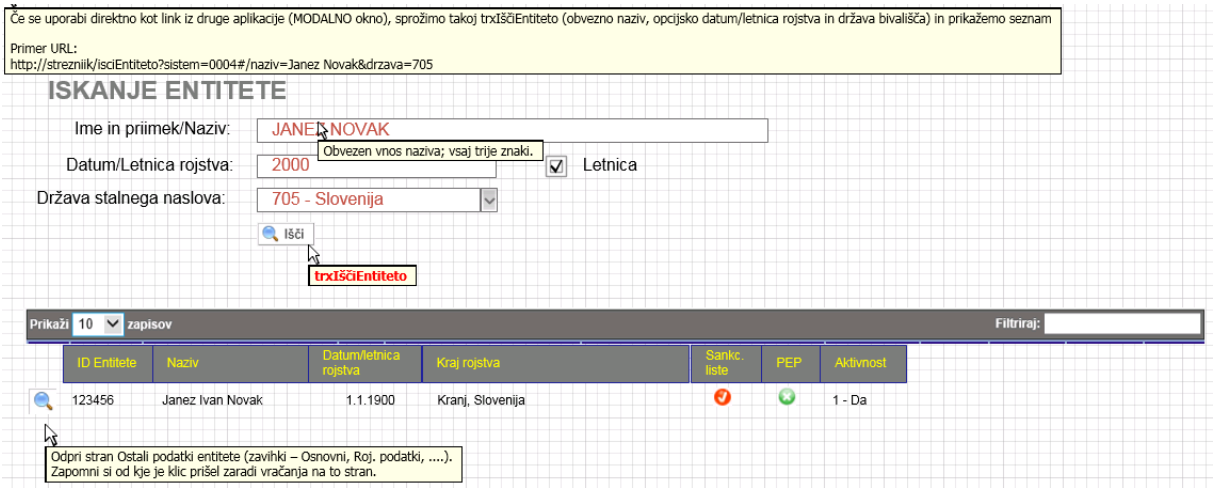
Slika 14 prikazuje ekransko masko, ki jo morajo razviti FE razvijalci. Na njej so predstavljeni: vizualni izgled okna in določene obvezne kontrole na polja ter klici transakcij.

*Slika 13: Diagram zaporedja za prijavo uporabnika*




*Vir: Izbrana banka, Poslovna analiza, 2015e.*

*Slika 14: Ekranske maske za FE razvoj*




*Vir: Izbrana banka, Poslovna analiza, 2015e.*

Drugi del razvoja je razvoj zalednega dela z glavno poslovno logiko, ki obsega online programiranje. Narejen je s pomočjo CICS-a (angl. *Customer Information Control System*, v nadaljevanju CICS). To je družina aplikacijskih strežnikov, ki zagotavlja trdnost upravljanja spletnih transakcij in povezljivost za kritične aplikacije na IBM Mainfram sistemu z/OS in z/VSE.

CICS skrbi za (CICS, 2016) :

- kontrolo nad hkrati delujočimi programi,
- dostop do datotek in baz,
- funkcije, ki jih zahteva program za komunikacijo s terminali in podsistemi, in
- možnost komuniciranja med različnimi CICS-i in podatkovnimi bazami.

Poleg online programiranja BE razvoj zajema tudi batch programiranje. To so programi, ki tečejo neodvisno od uporabnikovih aktivnosti v ozadju in imajo po navadi manjšo prioriteto kot online programi.

Specifikacije za BE razvoj vsebujejo transakcije in funkcije, ki imajo vhodne in izhodne parametre. Pomembna pa je tudi kontrola za določena polja, in sicer ali so ta obvezna ali samo opcijska.

Za psevdo kodo se uporablja ogrodje preprostega programskega jezika, v glavnem psevdo kodo sestavljajo stavki z »If-then-else« logiko in tabele s pripadajočimi SQL stavki.
Slika 15 prikazuje vhodne parametre, ki jih morajo napolniti FE razvijalci, in kontrolo za vhodna polja.

*Slika 15: Specifikacija za BE razvoj*

**Vhodni parametri** *(In-parameters)*

| Atribut | Št. ponovitev | Tip atributa | Opis |
|---|---|---|---|
| idEntitete | 1 | num(9)* | *ID entitete |

*Obvezen iskalni podatek

**Izhodni parametri** *(Out-parameters)*

| Atribut | Št. ponovitev | Tip atributa | Opis |
|---|---|---|---|
| stZapisovSRPE | 1 | num(2) | Število zapisov. |
| seznamRojPodEntitete(srpe) | 1 | Lista | Seznam vrnjenih datumov. Max. 80 zapisov. |
| srpe.datumRojstva | 1..n | txt(10) | Datum rojstva v tekstovni obliki (ker manjkajo lahko podatki in da na FE ne pade). |
| srpe.opombe | 1..n | txt(255) | Opombe. |

*Vir: Izbrana banka, Specifikacija programskega vmesnika, 2015f.*

Slika 16 prikazuje preprosto psevdo kodo za iskanje osebnih podatkov glede na iskano entiteto.

Poleg online programov se izdela tudi batch programe, ki izvajajo paketne obdelave v naprej določenem času, programi se med seboj povežejo v proces (angl. *Job Control Language*, v nadaljevanju JCL).

Na Sliki 17 je shematičen prikaz obdelave podatkov, programi si podajajo podatke po vrstnem redu, vse te pa povezuje JCL.

*Slika 16: Psevdo koda specifikacije*

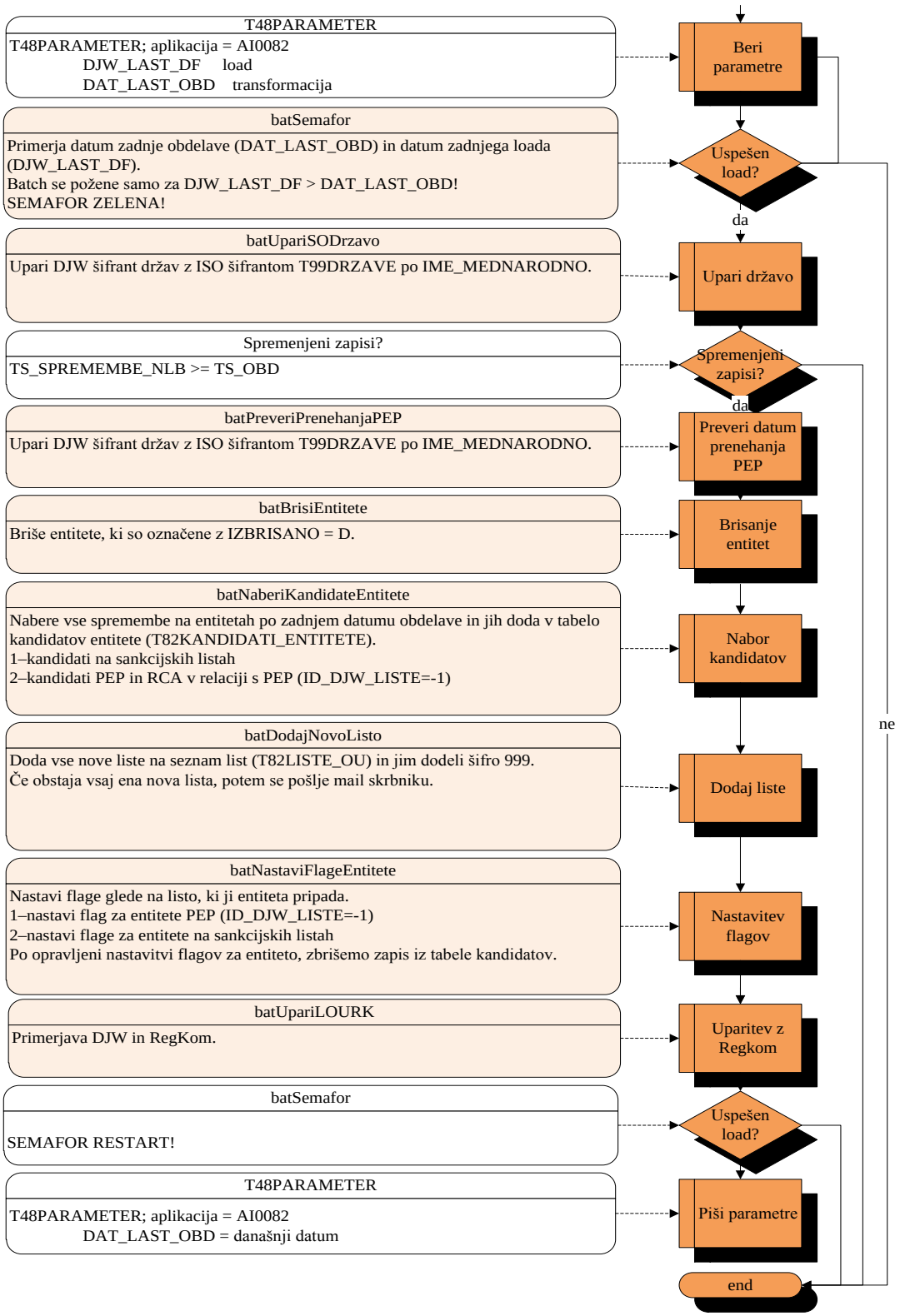
**Psevdo koda**

```
If input ni OK
   return Napaka: 'Napačni vhodni parametri.'
End


/* za vse poizvedbe (seznam*) omeji maksimalno število vrnjenih zapisov: */
if št. zapisov > seznam.maxStZapisov
   Opozorilo: 0003_Poizvedba vrne preveliko število zapisov
end if

/* seznam dokumentov*/
seznamImen = (

   SELECT
   A.IME,
   A.SREDNJE_IME,
   A.PRIIMEK,
   A.NAZIV,
   A.TIP_IMENA,
   C.TIP_ENTITETE
FROM
   T82IME_ENTITETE A
   INNER JOIN T82ENTITETA C ON A.ID_ENTITETE = C.ID_ENTITETE
WHERE
   A.ID_ENTITETE = i.idEntitete AND
   A.TIP_IMENA <> 1
ORDER BY A.TIP_IMENA, A.PRIIMEK, A.IME, A.SREDNJE_IME, A.NAZIV
WITH UR
);
```

```
/* mapiranje na izhod */

for each (ie in seznamImen)

   if entiteta.TIP_ENTITETE = 'E'
      o.imeEn.nazivEntitete      = ie.NAZIV;
   else
      o.imeEn.nazivEntitete      = sestavi naziv iz ie.IME, ie.SREDNJE_IME in ie.PRIIMEK,
      ločeno s presledki;
   end if

   o.imeEn.tipImena           = ie.TIP_IMENA

   mapiraj ie iz seznamImen na out /* OUTPUT */

end for
```

*Vir: Izbrana banka, Specifikacija programskega vmesnika, 2015f.*

*Slika 17: Slika zaporedja paketnih obdelav*




*Vir: Izbrana banka, Tehnična dokumentacija, 2015d.*

### 4.1.11 Izdelava program za prenos list

Program za polnjenje list pobira podatke preko spletni servisov, napisan je v programskem jeziku C# (»si šarp«), ki je razmeroma nov programski jezik, razvit v podjetju Microsoft. Programski jezik potrebuje za svoje delovanje .NET Framework, z njim lahko programiramo v razvojnem okolju Visual Studio.

*Slika 18: Osnovni program za prenos list*

```
/// <summary>
/// action=deleteAll
/// action=parseXML file=d:\tmp\pfa2_201502282200_f.zip parseMode=Full
/// action=importNext parseMode=Increment
/// action=importFull parseMode=Full
/// </summary>
/// <param name="args"></param>
static void Main(string[] args)
{
    DJWProperties prop = new DJWProperties();

    FileInfo _lockFile = new FileInfo(Path.Combine(HelperClass.getExeAssemblyPath(), ".lock"));
    FileStream fsLock = null;

    try
    {
        // read properties
        prop.Load();

        //lock (only one instance can run)
        try
        {
            fsLock = new FileStream(_lockFile.FullName, FileMode.OpenOrCreate, FileAccess.ReadWrite);
            StreamWriter sw = new StreamWriter(fsLock);
            sw.Flush();
        }
        catch (IOException ioe)
        {
            throw new Exception("Application allready running!!!", ioe);
        }


        getInParameters(args);

        //Test_ImportToDb();

        DjwProcess djw = new DjwProcess(prop);

        //
        string action = inParams.GetValueOrDefault("action", "importNext");
        string parseMode = inParams.GetValueOrDefault("parseMode", "Increment");
        DjwProcess.ParseMode pm = DjwProcess.ParseMode.Increment;
        if (parseMode == "Increment")
```

*Vir: Izbrana banka, Specifikacija programskega vmesnika, 2015f.*

Program za pobiranje list je razdeljen na več delov, ki so odvisni od parametrov:

- parameter »deleteALL« izbriše vse podatke po tabelah, naredi prazne tabele,
- parameter »parseXML« uvozi iz določene datoteke, ki je lokalno na sistemu.
  V načinu uvoza sta možna še dva načina:
  - »ParseMode=Incremental«, pomeni, da se bodo uvozile samo spremenjene liste, glede na datum spremembe,
  - »Parsemode=Full«, uvozijo se vse liste ne glede na datum spremembe.

Ko je uspešno izveden load podatkov v tabelo se zažene programe, ki so prikazani na Sliki 17.

### 4.1.12 Testiranje

Ko je aplikacija sprogramirana, se začne faza testiranja. Ta faza obsega preverjanje delovanja programskega paketa glede na specifikacijo. Izvesti je treba vsebinske teste, testirati je potrebno robustnost in učinkovitost programskega paketa. Vsebinski testi potrdijo ali ovržejo, ali so vse funkcionalnosti specificirane. Testiranje robustnosti nam da rezultate o tem, ali je programski paket mogoče pripraviti do nepredvidenega oziroma neželenega stanja.

Ker arhitektura sistema obsega več ravni, se testiranje izvaja v različnih okoljih.
V razvojnem okolju za Back-end se preveri delovanje programa glede na specifikacijo in vrsto programa:

- Pri online programih se testirajo vhodni parametri, obveznost le-teh, izvedba SQL-ov ter izhodna polja. Za ta namen se uporablja aplikacija, v katero se vstavi vhodni parameter, ki je strukturiran na komunikacijski in aplikacijski del.
- Pri batch programih se naredi primer vhodne datoteke in pripravi proceduro za testiranje programov. Programe se spusti skozi debug programe, kjer se preveri delovanje programov.

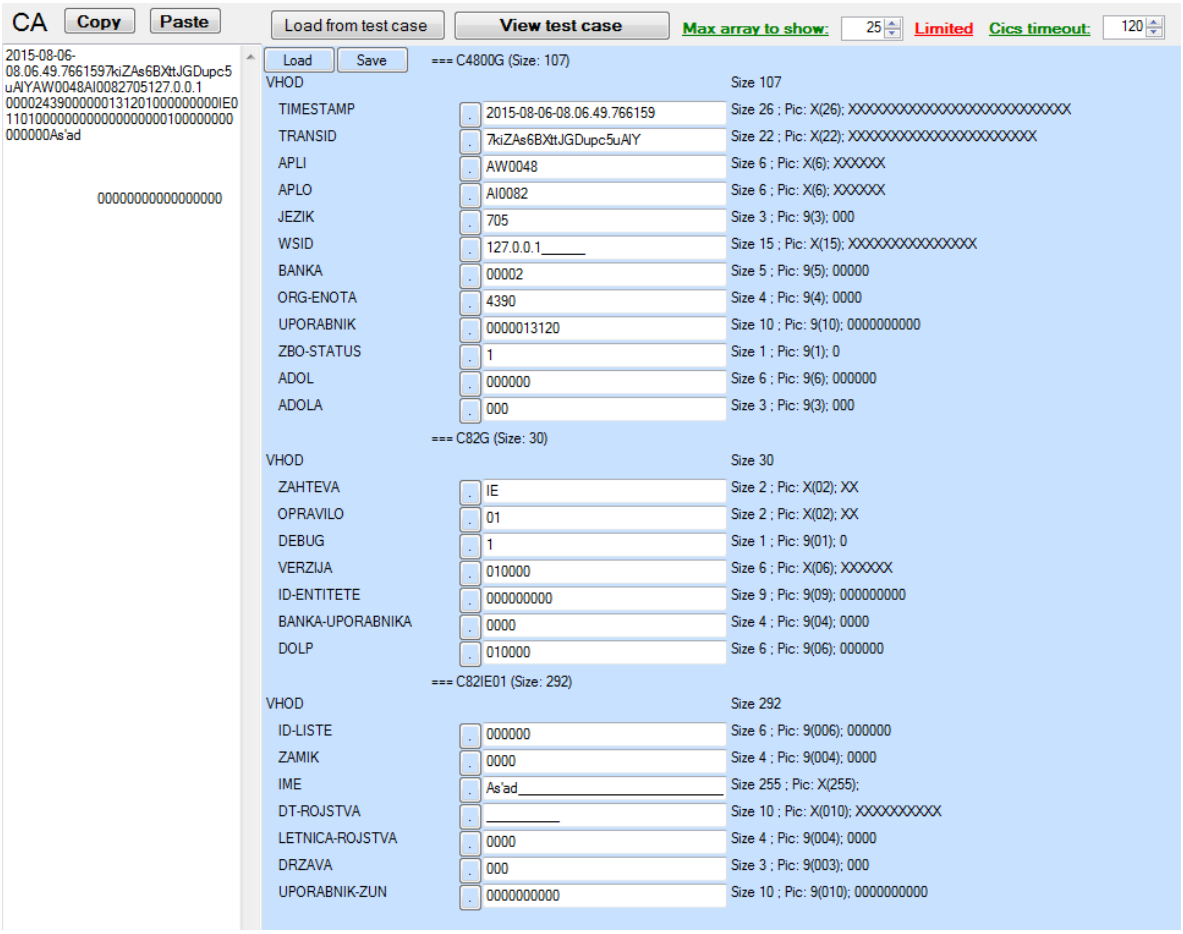
V razvojnem okolju za Front-end pa se preveri validacijo za polja, klice transakcij in prikaz podatkov.

V testnem okolju testirajo tehnologi in načrtovalci. V tem okolju se testira funkcionalnost, in sicer po vnaprej pripravljenih testnih scenarijih.

Na koncu nastopi uporabniško testno okolje, kjer se izvaja testiranje z drugimi sistemi in končnimi uporabniki. Tudi tukaj poteka testiranje po vnaprej pripravljenih scenarijih. Preverja pa se tudi povezave z drugimi aplikacijami, v kolikor to nova aplikacija zahteva.

Slika 19 prikazuje okno testne aplikacije – v zgornjem delu so komunikacijski parametri, ki povedo, od kod je prišla zahteva, kdo je uporabnik, iz katere banke itd., v aplikativnem delu pa so določeni vhodni parametri, ki so pomembni za aplikacijo.

*Slika 19: Primer aplikacije za online funkcionalno testiranje*




*Vir: Izbrana banka, Tehnična dokumentacija, 2015d.*

Pri uporabniškem testiranju je v veliko pomoč avtomatizacija testiranja. Izbrana banka uporablja orodja za testiranje, in sicer smo uporabili Rational Performance Tester. To je orodje za testiranje učinkovitosti poslovnih aplikacij z namenom odkrivanja ozkih grl. Uporaba je preprosta in za delo ni potrebno programersko znanje. Testiranje se opravlja na podlagi posnetka »dela« enega uporabnika, program potem na enak način »dela« po posnetku, s tem da lahko simulira delo večih uporabnikov ter tako preizkuša zmogljivosti povezanih spletnih aplikacij in strežnikov, hkrati pa zbira informacije o uspešnosti v realnem času, katere tudi prikaže v različnih oblikah (grafi, tabele …).

Rational Performance Tester omogoča:

- hitrejšo izvedbo testiranja in analiziranja aplikacije,
- pripravo testnih podatkov brez programiranja,
- analizo performančnih težav,
- da se testni podatki lahko črpajo iz vnaprej pripravljenih datotek in

- produkcijsko okolje.

Tako imamo v vsakem okolju ločene podatkovne baze in tudi izvajalne programe.

Nasprotniki slapovnega procesa običajno najbolj kritizirajo prav to fazo, saj se tveganje projekta poveča, če testiranje poteka šele na koncu. Naročnik do zadnjega trenutka ne more biti prepričan, ali bo dobil naročeno pravočasno ali ne. V fazi testiranja lahko pride na dan veliko napak, ki jih je treba odpraviti, kar podaljša trajanje in poviša ceno projekta. Po končani fazi testiranja oziroma ko s testnimi primeri dokažejo pravilno delovanje programskega paketa, ga vgradijo pri naročniku. Trajanje faze vgradnje je odvisno od posameznega projekta.

### 4.1.13 Uvedba

V okviru te aktivnosti IT skrbnik s pomočjo načrtovalca IS, FE in BE razvijalca, DBA, sistemskega inženirja in poslovnega analitika pripravi scenarij prehoda, zbere vso potrebno dokumentacijo, ki jo mora pregledati skupina za kakovost informacijske tehnologije, ter izvede napoved prehoda. Po potrditvi napovedi prehoda IT skrbnik s pomočjo prej omenjenih sodelavcev izvede namestitev IS v produkcijsko okolje. Če prehod v produkcijo ne uspe, se torej delo odvija po rezervnem scenariju, ki je vedno opredeljen v okviru načrta posega v produkcijo. To fazo opravi naročnik, potem ko je aplikacijo že prejel. Njegova naloga je preveriti, ali bo programski paket služil svojemu namenu. Tako kot faza testiranja je tudi faza prevzema pogosta tarča kritikov slapovnega procesa, saj lahko naročnik ugotovi, da ni dobil natančno tistega, kar je pričakoval, čeprav je bil projekt izveden dosledno. V takem primeru je treba spremeniti začetne zahteve.

V prvih dveh tednih po uvedbi IS v produkcijsko okolje se izvaja stabilizacija sistema. Nosilec te aktivnosti je IT koordinator, sodelujejo pa še naslednji: poslovni analitik, načrtovalec IS, BE in FE razvijalec, DBA, sistemski inženir in IT skrbnik. V okviru te aktivnosti morajo omenjeni poskrbeti za analizo in oceno kritičnosti napak, odpravo najbolj kritičnih in resnih napak ter planiranje nove verzije IS.
Ta faza pomeni podporo uporabnikom za čim učinkovitejšo uporabo programskega paketa. V tej fazi odpravljajo tudi napake, ki jih je odkril naročnik, izboljšujejo programski paket, da sledi novim tehnologijam, in ga dopolnjujejo z novimi funkcionalnostmi.

V času izvajanja funkcionalnega in regresijskega testiranja lahko analitiki in uvajalci identificirajo tehnične in vsebinske napake v delovanju. Napake analizirajo in jih prijavijo ustreznemu IT strokovnjaku (odvisno od tipa in področja napake). V primeru identifikacije tehnično kritičnih napak je običajno treba cikel testiranja ponoviti.
V primeru identifikacije vsebinskih kritičnih napak analitik glede na napako pozove lastnika in se z njim dogovori o nadaljevanju in/ali morebitnem zamiku nadaljnjih aktivnosti:

- Če gre za ustrezne, a nepopolne funkcionalnosti razvoja, se izvajanje testiranja nadaljuje, lastnik zahtevka pa prijavi zahtevek za dopolnitev funkcionalnosti, ki se bo obravnaval preko celotnega razvojnega procesa. Sledi ocena analitika, kdaj se bo vsebina lahko realizirala (v okviru testirane verzije ali v eni izmed naslednjih verzij aplikacije).
- Če gre za neustrezno razvite funkcionalnosti razvoja, se izvajanje testiranja prekine, analitik pa prijavi kritično napako. Testiranje se po popravku ponovno začne.

Načrtovalec IS v sodelovanju s FE in BE razvijalcem ter DBA odpravi morebitne napake, ki se pojavijo med funkcionalnim in regresijskim testiranjem. Če je bilo zaradi napake potrebno spremeniti programsko kodo, načrtovalec IS skupaj z razvijalcem, DBA in sistemskim inženirjem poskrbi za namestitev nove verzije v testno okolje.

### 4.1.14 Stroškovni vidik implementacije sistema za preprečevanje pranja denarja v banki

Raziskave kažejo, da so se v zadnjem desetletju znatno povečali vsi stroški, in sicer z namenom zagotavljanja skladnosti z zahtevami zakonodaje in nujnosti vlaganja v usposabljanje zaposlenih ter za vzpostavitev učinkovitih sistemov.

Vzpostavitev sistema za preprečevanje pranja denarja (v nadaljevanju PPDFT) je za banko obvezna, zato se banka ne more odločati, ali ukrepe želi izvajati ali ne. Vseeno je pomembno, da banka upošteva tudi stroške, ki jih implementacija povzroča, ter koristi, ki jih banka lahko pri tem pričakuje. Banka mora preučiti predvideno višino stroškov, učinkovito razporediti sredstva za dosego postavljenega cilja ter s tem zagotoviti čim večjo možno korist (Sproat, 2007, str. 278).

Pri vzpostavitvi sistema za PPDFT je zelo težko ali kar nemogoče izdelati klasično analizo stroškov in koristi. Večji del stroškov je namreč precej težko merljiv ali pa celo nemerljiv. Med takšne stroške lahko štejemo npr. stroške ugleda banke ali npr. stroške potencialnih sankcij zaradi neskladnosti z zakonodajo. Večina slovenskih bank niti ne spremlja natančno stroškov, povezanih s samo implementacijo zakonskih zahtev. Po drugi strani pa je še težje ovrednotiti neposredne koristi. Koristi, ki jih ima banka od uvedbe takšnega sistema, lahko namreč obravnavamo širše, z vidika koristi za celotno državo, za njeno prebivalstvo ter koristi za širšo mednarodno skupnost. Seveda je tudi dolgoročno uspešno poslovanje banke pogojeno s stabilnim finančnim sistemom države in širšega poslovnega okolja, v katerem banka posluje. Ne smemo pa pozabiti tudi na ugled in boniteto banke v domačem in mednarodnem poslovnem okolju, ki je predpogoj za uspeh in rast poslovanja. Banko lahko poleg kazni nadzornih organov tudi zelo hitro doleti izguba konkurenčne prednosti in tržnega deleža, če je povezana s pranjem denarja ali financiranjem terorizma. Vse to so posredne koristi, ki jih je nemogoče izmeriti in ovrednotiti.

Pri vzpostavitvi sistema za PPDFT v bankah nastopijo različni stroški (Sathye, 2008, str. 7):

- operativni stroški, ki nastanejo zaradi vzpostavitve sistema in izvajanja aktivnosti:
  - začetni stroški (stroški vzpostavitve in/ali dopolnitve informacijske podpore, organizacijski stroški, stroški pravnih in drugih svetovalcev),
  - stroški vzdrževanja sistema (usposabljanje in izobraževanje zaposlenih, stroški zaposlenih, ki izvajajo zahteve, pritožbe strank zaradi obremenjujočih zahtev),
- oportunitetni stroški, ki nastanejo zaradi izgube potencialno profitabilnih poslovnih razmerij zaradi zahtev zakonodaje,
- dodatni stroški, ki nastanejo zaradi drugih aktivnosti, ki sicer niso eksplicitno navedene v zakonodaji, vendar jih mora banka izvesti za učinkovitejše izvajanje zahtev zakonodaje ali zaradi priporočil nadzornih organov (kot so na primer stroški dodatnega usposabljanja, stroški izdelave ali nakupa informacijske podpore, ki olajša izvajanje aktivnosti oziroma preprečuje nastanek napak).

Banka mora biti zelo skrbna, da je ne doletijo zelo visoki stroški v obliki kazni v primeru nezagotavljanja takšnega poslovanja, kot ga predpisuje zakonodaja. V tem primeru je težko ovrednotiti potencialno škodo, saj ima banka v tem primeru poleg zakonske kazni še stroške, ki jih povzroči izguba ugleda banke in morebitna izguba potencialnih prihodnjih poslovnih razmerij.

Banka se mora zavedati, da je odločilni kriterij zagotavljanje skladnosti z zakonodajo, ki banki prinaša znatne stroške. Zahteve so za vse banke enake, zato morajo paziti, da izpolnjujejo zakonske zahteve, hkrati pa da njihove zahteve do strank ne presegajo zahtev njenih konkurentov.

# SKLEP

V magistrskem delu sem predstavil vlogo informacijske rešitve pri preprečevanju pranja denarja v bančnem sektorju. Skozi postopek pisanja magistrskega dela sem ugotovil, da je problematika pranja denarja precej kompleksna. Uradne ustanove, ki bdijo nad tem problemom, neprestano tudi spreminjajo zahteve bankam, ki jim morajo le-te slediti in jih izpolnjevati, sicer jim grozijo denarne kazni, ki običajno niso zanemarljive. Poleg teh stroškov je še bolj zaskrbljujoča morebitna izguba ugleda banke pri poslovnih partnerjih in komitentih, saj lahko le-to pomeni tudi ogrožanje obstoja banke.

Informatizacija procesa iskanja pralcev denarja v bankah veliko pripomore k uspešnejšemu in hitrejšemu soočanju s problemom. Informacijska podpora za ta problem namreč precej olajša in poenostavi samo iskanje pralcev denarja. Hkrati pa je tovrstna podpora precej zapletena in zahteva neprestano prilagajanje, saj je praktično vsak primer pranja denarja drugačen. Zaradi tega mora biti program v bankah, ki je namenjen postopku iskanja, zelo

kompleksen, a hkrati precej prilagodljiv in odprt za neprestano nadgradnjo. Stalna nadgradnja pa pomeni imeti dobre vzdrževalce sistemov in uporabnike, ki so odprti za neprestane novosti. S tega vidika gre za precej zahtevno aplikacijo. Hkrati pa takšna programska oprema predstavlja za bančne institucije veliko pomoč in avtomatizacijo procesov, saj odpade veliko ročnega dela, kar zmanjša možnosti napak in verjetnost slabega ugleda banke v primeru spregledanega postopka pranja denarja.

Na trgu obstaja množica ponudnikov informacijske podpore za preprečevanje pranja denarja. Sam sem mnenja, da je uvedba zunanjih, lahko rečemo »instant« programov kljub njihovemu prilagajanju potrebam banke še vedno precej zapletena in da je lasten razvoj tovrstne opreme veliko boljši in zanesljivejši ter verjetno konec koncev tudi cenejši. Poleg tega je vsaka nadgradnja z dobro interno podporo boljša in cenejša ter verjetno tudi hitrejša. Banka se na tak način lažje in hitreje prilagaja neprestanim zahtevam, program je v koraku s časom in lažje »polovi« morebitne storilce.

V izbrani banki sem sodeloval pri svetovanju, načrtovanju in umestitvi aplikacije v celotno arhitekturo. Poleg tega sem bil razvijalec back-end dela, izvajal sem testiranje in implementacijo v produkcijsko okolje. Moja vloga se na tej točki ne zaključuje, saj sem vpet tudi v vzdrževanje aplikacije.

Glede na teoretično znanje, ki sem ga pridobil tekom pisanja naloge in v času razvoja programske opreme za preprečevanje denarja, lahko trdim, da je za banko vsekakor boljše imeti lasten razvoj tako zahtevne programske opreme, kot pa kupiti enega od produktov na trgu. Nakup tovrstne opreme od ponudnikov na trgu je že v osnovi drag in ga je potrebno po nakupu prilagoditi banki, kar seveda predstavlja dodatne stroške in čas ter nekaj zaposlenih, ki so na razpolago ob tovrstnih prilagoditvah. Poleg tega se pri nakupu programske opreme pojavljajo tudi vprašanja o vzdrževanju in z njim povezanimi stroški. Razvoj lastnega produkta je po mojih izkušnjah hitrejši, bolj prilagodljiv in finančno ugodnejši v vseh fazah razvoja, implementacije in tudi vzdrževanja. S tem mnenjem lahko tudi potrdim zastavljeno hipotezo.

# LITERATURA IN VIRI


1. *Anti money laundering solution*. Najdeno 1. maja 2016 na spletnem naslovu http://www.bobsguide.com/anti-money-laundering-solutions/
2. Advancing Financial Crime Professionals Worldwide. (2016). *The Challenge of AML Models Validation*. Najdeno 10. maja 2016 na spletnem naslovu http://files.acams.org/pdfs/2016/The_Challenge_of_AML_Model_Validations_R_Al_Rabea_Updated.pdf
3. Bajec, M., & Krisper, M. (2003). *Izbrana načela agilnega načrtovanja*. Ljubljana: Fakulteta za računalništvo in informatiko.
4. Banka Slovenije. (2008). *Usmeritve pri izvajanju ukrepov na področju preprečevanja pranja denarja in financiranja terorizma za bančni sektor*. Ljubljana: Banka Slovenije.
5. Brigitte, U., & Linde, D. (2013). *Research Handbook on money Laundering.* Ultrecht:University School of Economics
6. *Coindesk.* Najdeno 30. junija 2016 na spletnem naslovu http://www.coindesk.com/information/what-is-bitcoin/
7. *Customer Information Control System.* Najdeno 20. maja 2016 na spletnem naslovu https://www-01.ibm.com/software/htp/cics/
8. Cox, D. (2009). *An Introduction to Money Laundering Deterrence*. London: John Wiley & Sons.
9. Cox, D. (2014). *Handbook of Anti-Money Laundering*. London: John Wiley & Sons.
10. Debelak, M. (2002). *Strateški informacijski sistem kot ključ pri doseganju konkurenčne prednosti podjetja* (magistrsko delo). Ljubljana: Ekonomska fakulteta.
11. Federal Financial Institutions Examination Council. (b.1.). *Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase.* Najdeno 30. junija 2016 na spletnem naslovu https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm
12. *Gartner IT Glossary*. Najdeno 8. julija 2016 na spletnem naslovu http://www.gartner.com/it-glossary/enterprise-architecture-ea/
13. Gruden, M. (2014). *Izboljšanje razvoja procesa programske opreme na primeru sistema za bančno poslovanje* (magistrsko delo). Ljubljana: Fakulteta za računalništvo in informatiko.
14. Gradišar, M., Jaklič, J., & Turk, T. (2007). *Osnove poslovne informatike*. Ljubljana: Ekonomska fakulteta.
15. Gradišar, M., & Resinovič, G. (1998). *Informatika v organizaciji*. Ljubljana: Ekonomska fakulteta.
16. Gradišar, M. (2003). *Uvod v informatiko*. Ljubljana: Ekonomska fakulteta. .
17. Izbrana banka. (2016). *Aplikacija za preprečevanje pranja denarja in financiranja terorizma.* Ljubljana: Izbrana banka.
18. Izbrana banka. (2014). *Interni standard IT arhitekture.* Ljubljana: Izbrana banka.
19. Izbrana banka. (2015a). *Dow Jones analiza.* Ljubljana: Izbrana banka.
20. Izbrana banka. (2015b). *Primeri uporabe.* Ljubljana: Izbrana banka.

21. Izbrana banka. (2015c). *Podatkovni model.* Ljubljana: Izbrana banka.
22. Izbrana banka. (2015d). *Tehnična dokumentacija.* Ljubljana: Izbrana banka.
23. Izbrana banka. (2015e). *Poslovna analiza.* Ljubljana: Izbrana banka.
24. Izbrana banka. (2015f). *Specifikacija programskega vmesnika.* Ljubljana: Izbrana banka.
25. Izbrana banka. (2016). *Izvajanje procesa razvoja z IT komponento.* Ljubljana: Izbrana banka.
26. Kazenski zakonik RS. *Uradni list RS* št. 63/94, št. 23/99 in št. 40/04.
27. Kevin, S. (2015). *Anti-Money Laundering in a Nutshell. Awareness and Compliance for Financial Personnel and Business Managers*. New York: Apress.
28. Lilley, P. (2001). *Dirty dealing: The untold truth about global money laundering*. London: Kogan Page.
29. Mitchell, D. J. (2005). Fighting Terror and Defending Freedom*:* The Role of Cost-Benefit Analysis. *Pace Law Review*, *25*(2), 219–232.
30. Sathye, M. (2008). Estimating the cost of compliance of AMLCTF for financial institutions in Australia. *Journal of Financial Crime*, 15(4), 347–363.
31. Slapnik, M. (2010)). *Strategija preprečevanja pranja denarja* (diplomsko delo). Ljubljana: Univerza v Mariboru.
32. Sproat, P. A. (2007). The new policing of assets and the new assets of policing. A tentative financial cost-benefit analysis of the UK´s anti-money laundering and assets recovery regime. *Journal of Money Laundering Control*, 10(3), 277–299.
33. Sullivan, K. (2015). *Anti-Money Laundering in a Nutshell. Awareness and Compliance for Financial Personnel and Business Managers*. New York: Apress.
34. Sturm, Jake (1999). *VB6 UML Design and development*. Birmingham: Wrox Press.
35. Šeme Hočevar, V. (2006). Globalizacija problema pranja denarja. *Bančni vestnik, 55* (12), str. 14-17.
36. Šeme Hočevar, V. (2007). *Pranje denarja*. Ljubljana: GV Založba.
37. Wood, L. (2016, 18. april). Global Anti-money Software Market 2016-2020. *Globebewswire.*
    Najdeno 8. maja 2016 na spletnem naslovu https://globenewswire.com/news-release/2016/04/18/829865/0/en/Global-Anti-money-Laundering-Software-Market-2016-2020.html
38. Zakon o preprečevanju pranja denarja in financiranja terorizma. *Uradni list RS* št. 60/2007.

# PRILOGA

**PRILOGA: Seznam v delu uporabljenih kratic**

| Kratica | Pomen | Slovenski prevod |
|---|---|---|
| AML | Anti-money laundering | Preprečevanje pranja denarja |
| BE | Back End | Zadnji del |
| CICS | Customer Information Control System | Jezikovno mešanih strežnikov |
| DBA | Database administrators | Skrbnik podatkovnih baz |
| EUR | Enotna valuta Evropske unije | |
| FBE | European Banking Federation | Evropsko bančno združenje |
| FE | Front End | Sprednji del |
| ID | Identity Document | Identifikacijsko številko |
| IS | Information System | Informacijski Sistem |
| IT | Information tehnology | Informacijska tehnologija |
| OFAC | Office of Foreign Assets Control | |
| PEP | Politically Exposed Person | Politično izpostavljene osebe |
| PIA | Enterprise Architecture | Poslovna informacijska arhitektura |
| PPDFT | Preprečevanje pranja denarja in financiranju terorizma | |
| SOA | Service-Oriented Architecture | Storitveno Orientirana Arhitektura |
| UPPD | Urad za preprečevanje pranja denarja | |
| VIZ | Varovanje informacijskih sistemov | |
| ZPPDFT | Zakon o preprečevanju pranja denarja in financiranje terorizma | |