UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

KAREL REK

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

UPRAVLJANJE S SPREMEMBAMI KOT DEJAVNIK ZMANJŠEVANJA OPERATIVNIH TVEGANJ V BANČNEM INFORMACIJSKEM OKOLJU NA PODROČJU PLAČILNIH SISTEMOV

Ljubljana, september 2016 KAREL REK

IZJAVA O AVTORSTVU

Podpisani Karel Rek, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Upravljanje s spremembami kot dejavnik zmanjševanja operativnih tveganj v bančnem informacijskem okolju na področju plačilnih sistemov, pripravljenega v sodelovanju s svetovalcem prof. dr. Andrejem Kovačičem

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 30.9.2016 Podpis študenta :

KAZALO

UVOD

Napredek in nenehne spremembe na področju informacijskih sistemov *(*angl. *Information System*, v nadaljevanju IS*)* in informacijske tehnologije (angl. *Information Technology*, v nadaljevanju IT) kot njihovega pomembenega dela, zadnjih petnajst let prinašajo velike spremembe v poslovanje bank, kar zahteva poglobljeno spremljanje, planiranje, organiziranje in implementiranje sprememb v bančno okolje.

Bančni sistem je v pogojih zaostrene domače in tuje konkurence izpostavljen tudi spremembam na področju razvoja novih finančnih produktov in razširjenim poslovnim odnosom s ključnimi strankami, zagotavljati mora 24-urno razpoložljivosti dostopa do bančnih produktov, istočasno je vse bolj in bolj odvisen od informacijske podpore in novih tehnologij ter mora zadostiti vedno bolj strogi zakonski regulativi, ki jo narekujeta EU in tudi domači zakonodajalec.

Banka potrebuje sodobno strateško načrtovanje informatike, ki mora izhajati iz potreb po nenehnem in sprotnem prilagajanju poslovnih procesov, ki jih narekuje hitro spreminjajoče se in nepredvidljivo poslovno okolje (Kovačič & Bosilj Vukšič, 2005, str. 10).

V bankah je prisotno vedno več avtomatiziranih postopkov, toda človeški faktor ostaja še vedno najpomembnejši. Spremembe na področju IS in IT so vsakodnevne, to pa pomeni, da se z vsako novo spremembo pojavi možnost izpostavljenosti novim operativnim in drugim tveganjem.

Z napredkom na področju razvoja IS so se razvijali tudi modeli za prenovo poslovanja (Kovačič & Bosilj Vukšič, 2005, str. 48), s katerimi upravljamo in obvladujemo posamezne pomembne dejavnike IS. Potrebno se je zavedati, da bo banka vedno izpostavljena določenemu obsegu tveganja. Pomembno pa je, da se banka zaveda vseh vrst tveganj in da ima vzpostavljene ustrezne obrambne mehanizme za obvladovanje le-teh.

Banke so zadnja leta izvedle velike investicije v razvoj novih metodologij, procedur in kontrol z namenom boljšega identificiranja, merjenja in upravljanja tveganj. Upravljanje s tveganji in upravljanje s spremembami sta neločljivo povezana in soodvisna. Ker gre pri upravljanju sprememb za uvajanje obsežnih in kompleksnih sprememb, je banka običajno izpostavljena velikim tveganjem, vendar je tudi v primeru majhnih sprememb, ki vplivajo na več področij lahko izpostavljena večjim tveganjem.

Tveganja pa lahko zmanjšamo, če že v fazi uvajanja sprememb upoštevamo možne "črne" scenarije. Banka pa se ne sme zadovoljiti samo z odpravljanjem tveganj, ki nastajajo kot posledica nenehnih sprememb, tako pri zaznavanju, analiziranju kot pri načrtovanju in

implementaciji sprememb. Pomembno je, da razmislimo, ali lahko že v fazi strateškega načrtovanja sprememb predvidimo tveganja, ki bodo nastala pri rednem, vsakodnevnem operativnem delu v produkcijskem okolju. Obvladovanje sprememb in tveganj je nujnost, še posebej v bančnem okolju.

Za obvladovanje vedno novih in vedno hitrejših sprememb je pomembno, da jih banka zna identificirati in ima izdelano strategijo za njihovo obvladovanje. V bankah običajno obstaja interni akt o upravljanju projektov, toda če v ozadju ni organizacijsko in kadrovsko podprte funkcije za upravljanje sprememb v obliki oddelka, je to premalo za učinkovito upravljanje. Za uspešno realizacijo sprememb je pomembno, da je upravljanje sprememb premišljeno in pravilno vodeno s strani Uprave banke. Vprašanje, ki si ga zastavim v magistrskem delu se nanaša na obvladovanje sprememb v izbrani banki in vpliv, ki ga neučinkovito upravljanje tega področja, prinaša na področje operativnih tveganj. Proučevanje se nanaša na obstoječe stanje obvladovanja sprememb in operativnih tveganj na področju plačilnega prometa, z rezultatom analize pa se pokaže pomembnost upravljanja s spremembami.

Eno izmed tveganj, ki nastaja kot posledica uvajanja sprememb v bančnem poslovanju, je operativno tveganje. Baselski odbor za bančni nadzor (angl. *The Basel Committee on Banking Supervision*) operativno tveganje opredeljuje kot tveganje izgub, ki nastanejo zaradi neprimernega ali neuspešnega izvajanja notranjih procesov, ravnanj ljudi ali delovanja sistemov oziroma zunanjih dejavnikov.

Operativno tveganje nekateri avtorji opredelijo nekoliko širše, in sicer kot tveganje delovanja, in ga glede na dejavnike tveganja razvrstijo v štiri sklope (Berk & Peterlin, 2005, str. 182):

- tveganja zaposlenih (napake zaposlenih, zlorabe, prekoračitev pooblastil),
- tveganja razmerij (s strankami, z delničarji, s tretjimi osebami,
- tveganja poslovnih procesov in tehnologije (zunanje sistemske motnje in notranje sistemske motnje),
- zunanja tveganja (premoženjsko tveganje, zlorabe tretjih, tveganje sprememb zakonodaje).

Operativno tveganje je torej mešanica številnih med seboj nezdružljivih tveganj. Dogodki iz naslova operativnega tveganja tako vključujejo prevare s strani zaposlenih kot tudi strank in »ostalega sveta«, računovodske napake, tožbe, naravne katastrofe, napake v modelih, napake pri poravnavah na računih itd. In prav raznolikost operativnega tveganja je njegova ključna težava in povzroča težave pri njegovem merjenju (Rotovnik, 2004, str. 39). Ljudje, procesi in sistemi znotraj banke so nepopolni in zaradi nepopolnosti nastajajo napake pri izvajanju procesov in zahtevanih funkcij ter tako lahko povzročijo izgubo bodisi ugleda bodisi finančno ali v obliki izgube strank.

Z upravljanjem sprememb (angl. *Change Mamagement*) se srečujemo v bankah na vsakem koraku. Spremembe, ki vplivajo na delovanje banke in jih mora banka najprej zaznati oz. biti o njih obveščena, nastajajo zunaj banke (zakonodajalec, nadzornik, upravljavec sistemov, zunanji partnerji) in znotraj banke (spremembe poslovnih procesov, spremembe informacijske tehnologije, spremembe pogojev poslovanja, organizacijske spremembe, kadrovske spremembe).

Spremembe, ki nastajajo v bankiah le-ta obvladuje z razpoložljivimi resursi, spremembe, ki nastajajo v okolju in na katere banka nima vpliva, pa predstavljajo motnjo, ki pomembno vpliva na delovanje banke in ponavadi zahteva dodatne resurse.

Upravljanje in obvladovanje sprememb je ključnega pomena za zmanjševanje operativnih tveganj. Ker se pristop k obvladovanju tveganj v bankah nenehno dopolnjuje in razvija, pomeni, da je tudi implementacija obvladovanja tveganj v bankah vedno bolj zahtevna. V kolikor banke ne bi bile neposredno prisiljene v obvladovanje tveganj s strani nadzornika, bi to pomenilo večjo nedoslednost pri obvladovanju operativnih tveganj.

Žal gre pri obvladovanju sprememb in obvladovanju tveganj v bankah običajno za dve ločeni in nepovezani funkciji, zato je pri uvajanju sprememb bistvenega pomena, da se banka zaveda operativnih tveganj in jih pri obvladovanju sprememb upošteva oz. jih upošteva v primeru vzpostavitve projekta za nadgradnjo informacijske tehnologije.

Operativna tveganja v bančnem okolju so raznolika in se izražajo v vseh ključnih dejavnikih poslovanja (strategija, tehnologija, procesi, kadri). Prav zaposleni so najpomembnejši in hkrati najšibkejši člen obvladovanja sprememb in obvladovanja operativnih tveganj.

Uspešen sistem za spremljanje in uvajanje sprememb, je za obvladovanje operativnega tveganja velikega pomena. Z njim lahko hitro odkrijemo možna operativna tveganja in napake v novih oz. prenovljenih poslovnih procesih. Odkrivanje in odpravljanje tveganj pred nastankom dogodka, ki lahko povzroči izgubo, v veliki meri zmanjša nevarnost izgub zaradi potencialnih škodnih dogodkov, ki spadajo pod operativna tveganja.

Glede na to, da je upravljanje sprememb ena najpomembnejših komponent pri prenovi poslovnih procesov v bankah in njihovo »ne«upravljanje glavni vzrok za nastanek operativnih tveganj, je v nalogi glavna pozornost namenjena uvedbi novega sistema za upravljanje sprememb.

Namen. Pri delu v banki X na področju plačilnih sistemov v oddelku plačilni promet, sem zaznal težave, ki so nastajale zaradi nenehnega uvajanja sprememb (organizacijskih, tehnoloških in kadrovskih) in povzročale operativna tveganja. Namen magistrske naloge je

predstaviti predlog za uvedbo novega sistema upravljanja sprememb na področju plačilnih sistemov v banki X. Nov izboljšan sistem bo temeljil na analizi obstoječega stanja na področju obvladovanja sprememb in obvladovanja operativnih tveganj v plačilnih sistemih. Z upoštevanjem teoretičnih izhodišč bom podal konkretne predloge za sistematično uvajanje sprememb, ki bodo v povezavi z identifikacijo operativnih tveganj vplivali na zmanjševanje le-teh in omogočali oddelku za plačilni promet sistematično spremljanje in upravljanje sprememb v prihodnje.

Ker sta upravljanje in obvladovanje sprememb (od njihovega načrtovanja, uvajanja in izvajanja do odpravljanja odporov in usmerjenosti h kvalitetnim storitvam) in upravljanje in obvladovanje tveganj neločljivo povezana, bom z upoštevanjem sprememb na področju posameznih dejavnikov IS poskušal določiti ključna tveganja na področju plačilnih sistemov.

Podatki, ki so mi bili na razpolago, so omejeni zaradi zaupnosti le-teh, saj banke o obvladovanju in evidentiranju tveganj z vidika svojih »internih« težav praviloma ne obveščajo javnosti, zato prihaja do odsotnosti relevantnih podatkov o škodnih dogodkih (Tomisits, 2012, str. 26). Izjema so težave, ki neposredno vplivajo na komitente banke (motnje pri dvigu gotovine na okencu, izpad bankomatov) in jih banka, v kolikor so motnje vnaprej predvidene, tudi javno objavi.

Motenj v delovanju plačilnih sistemov (težav pri posredovanju in prejemu plačilnih nalogov v oz. iz plačilnih sistemov banke) komitenti praviloma ne občutijo, v kolikor gre za začasno oz. kratkotrajno prekinitev.

Cilji. Cilji magistrske naloge so proučiti teoretična spoznanja na področju upravljanja sprememb in teoretična spoznanja na področju upravljanja tveganj, s poudarkom na upravljanju sprememb, ter ugotoviti vpliv načina upravljanja s spremembami na pojave operativnega tveganja. V nalogi bom ugotavljal, ali je vpliv možno meriti ali samo oceniti. Na primeru banke X bom ocenil povezanost upravljanja sprememb in upravljanja operativnih tveganj in podal predlog za izboljšanje ravnanja in upravljanja s spremembami in s tem zmanjševanja operativnih tveganj.

Metodologija. Metode proučevanja obravnavanega problema temeljijo na analitičnem pregledu domače in tuje literature ter virov, ki obravnavajo upravljanje sprememb in upravljanje tveganj v bančnem informacijskem okolju. V raziskovalnem delu se bom opiral na deskriptivni način raziskovanja in proučil literaturo, ki obravnava navedena področja s tehnološkega, kadrovskega in organizacijskega vidika, ter opisal teoretične osnove upravljanja sprememb in operativnih tveganj.

S pomočjo naštete literature in pridobljenega znanja pri študiju želim v raziskovalnem delu analizirati obstoječe stanje obvladovanja sprememb v banki X in prikazati posledice

neustreznega obvladovanja sprememb, ki vplivajo na obvladovanje tveganj na področju plačilnega prometa.

Da bi v predlaganih ukrepih za celovito obvladovanje sprememb pridobil podatke za oceno sedanjega in želenega stanja, bom analiziral stanje upravljanja sprememb v banki X in opravil intervju z vodjem plačilnega prometa (Priloga 1).

Analiza stanja opredeljena v petem poglavju vsebuje pregled področja upravljanja s spremembami (identifikacija, metode, načrtovanje, izvajanje, spremljanje, dokumentiranje, analiza) in pregled področja upravljanja s tveganji (identifikacija, metode, monitoring, analiza, ukrepi) ter predlog izboljšanja stanja s spremembo organiziranosti banke z uvedbo novega oddelka za upravljanje s spremembami.

1 OBVLADOVANJE SPREMEMB

1.1 Metode uvajanja sprememb

V bančnem sektorju so spremembe stalnica, razlika je v obsegu informacijski podpore, ki jo zagotavlja IT ostalim komponentam IS. Spremembe lahko nastajajo v banki (sprememba internih aktov), lahko jih povzročijo drugi (konkurenca, zakonodaja), lahko pa spremembe generira sama s ciljem izboljšanja poslovanja in ohranjanja konkurenčnih prednosti. Vsako spreminjanje obstoječega stanja nosi v sebi določeno stopnjo tveganja. Kolikšno je to tveganje, je odvisno od hitrosti spreminjanja okolja, od obsega sprememb in od časovnega obdobja, v katerem je potrebno uvesti spremembe.

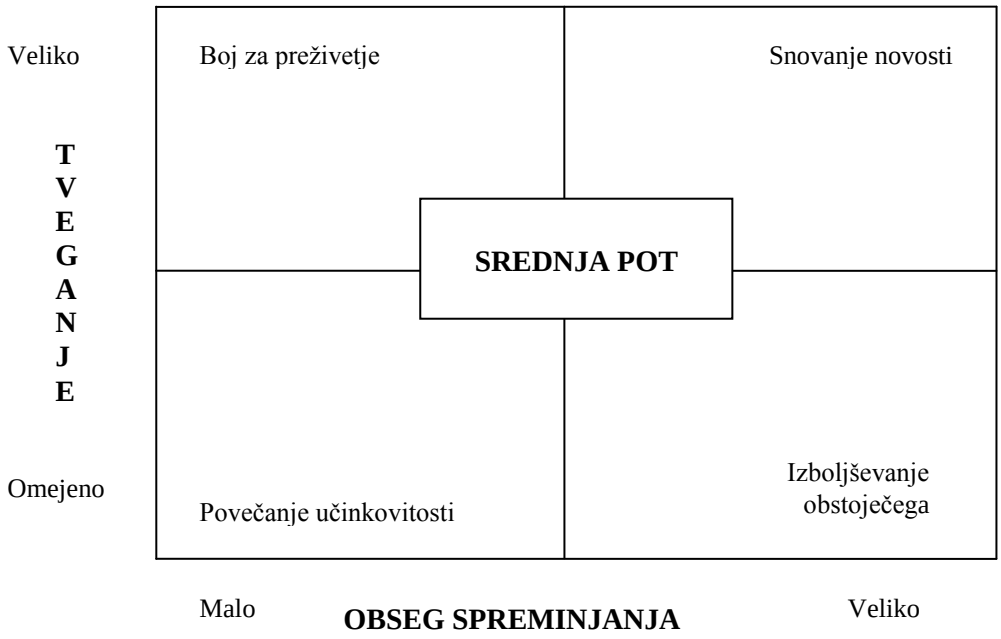
Slika 1 kaže odnos med tveganjem in obsegom spreminjanja. Slovenski bančni prostor deluje v pogojih velike konkurence (veliko domačih in tujih bank), zato mora biti vedno pripravljen na snovanje novosti, pri tem pa permanentno izvajati aktivnosti za povečanje učinkovitosti.

Glede na to, da bančni sektor deluje v razmerah močne in globalne konkurence, je obseg spreminjanja velik, občasno zelo velik, saj zajema tako nenehno posodabljanje informacijskih sistemov kot tudi uvajanje novih in prenovo obstoječih poslovnih procesov.

Če je banka izpostavljena boju za preživetje, se seveda povečuje stopnja tveganja, saj mora banka ob enakem obsegu sprememb sprejemati odločitve, ki prinašajo večjo stopnjo tveganja (popolna prenova poslovnih procesov, zagotavljanje informacij pomembnih za odločanje, vlaganje v informacijsko opremo) s tem, da večji obseg uvajanja sprememb sam po sebi še ne zagotavlja »okrevanja« in višjih prihodkov. Prenova poslovnih procesov in višja vlaganja v posodobitev tehnološke podpore ne pokažejo rezultatov poslovanja kratkoročno.

Spremembe se nanašajo tudi na spremembe poslovnih procesov, v okviru katerih pa gre za spremembe na kadrovskem, tehnološkem in organizacijskem področju.

Slika 1 : Prikaz razmerja tveganje – obseg spreminjanja



Vir: S. Možina, S. Rozman, R. Tavčar, D. Pučko, Š. Ivanko, B. Lipičnik, J. Gričar, M. Glas, J. Kralj, M. Tekavčič, V. Dimovski & B. Kovač, Management, nova znanja za uspeh, 2002, str. 742.

Vodstvo se lahko na spremembe odziva načrtovano ali nenačrtovano (v primeru, da je sprememba nenadna in ne v naprej načrtovana). Ker vsaka sprememba nosi v sebi nekaj novega in s tem določeno tveganje, se v bankah pojavljajo odpori proti spreminjanju.

Odpori se pojavljajo tako pri posameznih zaposlenih, kot pri skupinah zaposlenih (npr. v poslovni funkciji, če se sprememba nanaša na prenovo procesov, ki s sabo prinašajo določene posledice za oddelek) ter pri vodilnih na srednji ravni, če so spremembe v nasprotju z njihovimi interesi (npr. zmanjšanje vpliva oddelka, zmanjšanje števila zaposlenih v oddelku, ukinitev oddelka).

Metode uvajanja sprememb se skozi čas in različne avtorje razlikujejo predvsem glede na obseg področja, na katerega se fokusirajo in intenzivnost, s katero želimo doseči realizacijo potrebnih nujnih in manj nujnih sprememb.

Splošna enačba uspešnosti sprememb (Kovačič & Bosilj Vukšič, 2005. str. 50):

$$S = N \times V \times P \qquad (1)$$

kjer je:
N – nezadovoljstvo z razmerami
V – vizija prihodnosti
P – zaupanje v pot do sprememb

Kot je razvidno iz enačbe (1), je uspešnost uvajanja sprememb pogojena z »nujnostjo« uvedbe sprememb, izdelane vizije prihodnosti in zaupanjem zaposlenih v način, kako spremembe doseči. Višja uspešnost uvedbe sprememb pa, ne nujno, v sebi nosi zmanjševanja tveganj izvajanja poslovnega procesa. Sprememba je lahko uspešno implementirana, toda če niso zagotovljeni pogoji za nemoteno izvajanje procesa, bo prihajalo do odklonov in potencialnih škodnih dogodkov.

1.2 Pristopi k prenovi poslovanja

Pristope k prenovi poslovanja v osnovi delimo na način trde prenove in način mehke prenove poslovanja (Kovačič & Bosilj Vukšič, 2005, str. 62). Pri pristopu na način trde prenove poslovanja gre za naslednje značilnosti:

- načrtovanje in vodenje sprememb je nujno in radikalno,
- prenova procesov, velik obseg sprememb,
- izvedba sprememb na področju tehnologije v kratkem času,
- spremembe so učinkovite in uspešne,
- spremembe izvajajo ključni izvajalci, odpor večine zaposlenih,
- tveganje za dosego ciljev je veliko.

Pri pristopu na način mehke prenove poslovanja gre za naslednje značilnosti:

- načrtovanje in vodenje sprememb je postopno,
- obseg sprememb je obvladljiv,
- izvedba sprememb v "normalnih"rokih,
- odpor posameznikov je manjši, sodelujejo vsi,
- tveganje za dosego ciljev ni veliko.

Trdi načini prenove poslovanja dejansko zahtevajo drastične spremembe v organizaciji in to na vseh področjih poslovanja. Najbolj znana med metodami je t. i. popolna prenova poslovnih procesov (angl. *Business Process Re-engineering,* v nadaljevanju BPR*)* metoda, ki že v samem pristopu nosi oznako velikega tveganja za dosego ciljev.

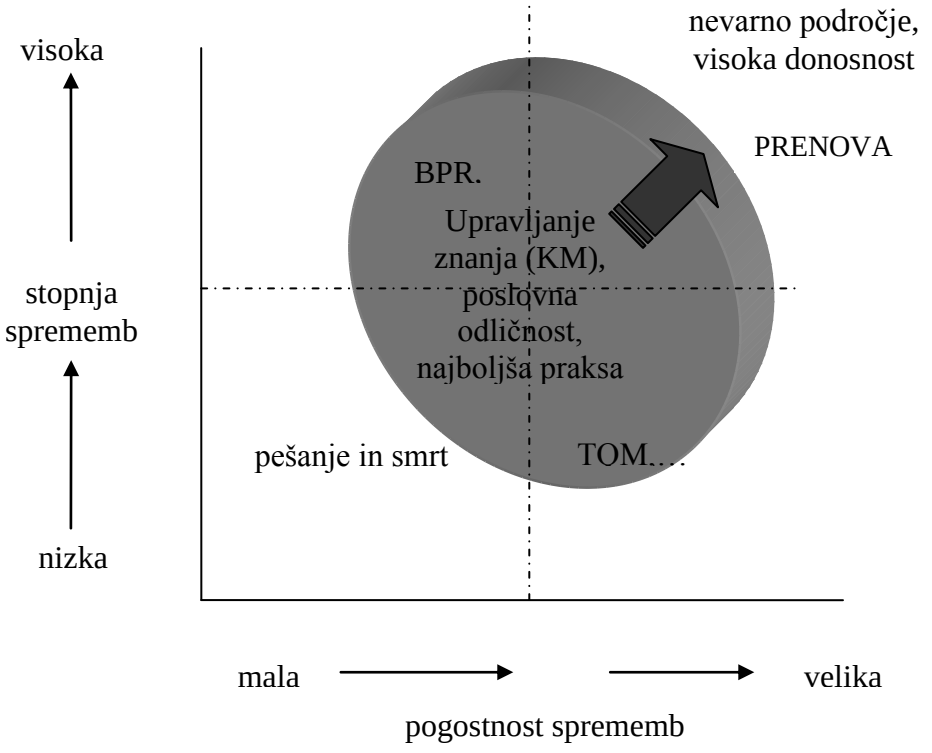
Pri mehkih načinih prenove poslovanja gre za postopno uvajanje sprememb. Razliki med trdimi in mehkimi pristopi določata obseg sprememb v organizaciji in čas, ko naj bi se te spremembe udejanjile. Najbolj znane in uporabljene mehke metode so :

- TQM (angl. *Total Qualitiy Management*),
- PDCA (angl. *Plan-Do-Check-Act*),
- metoda najboljše prakse,
- metoda poslovne odličnosti,
- metoda 20 ključev.

Če ocenimo, da je permanentna prenova poslovnih procesov v bankah dejstvo, lahko v nadaljevanju zaključimo, da se pri prenovi informacijskih sistemov uporabljajo mehki pristopi, ki so v nadaljevanju na kratko opisani. Metoda mehkih pristopov temelji na postopnem izboljšanju stanja na kadrovskem, tehnološkem in organizacijskem področju. Pomembno je, da se spreminja kultura organizacije, sodelovanje med zaposlenimi in kvalitetnejše in pogostejše izobraževanje zaposlenih.

Celovita prenova poslovanja je opredeljena kot tista metoda, ki vključuje oba predhodno navedena načina upravljanja s spremembami in se pri prenovi poslovanja običajno tudi uporablja (Slika 2).

Slika 2: Vzvodi celovite prenove poslovanja



Vir: A. Kovačič & V. Bosilj Vukšič, Management poslovnih procesov, 2005, str. 53.

Upravljanje znanja in poslovna odličnost sta cilja, ki bi ju morala uresničiti vsaka finančna institucija. Težava je v tem, da za doseganje teh ciljev ni pogojev, saj so zaposleni običajno

obremenjeni z rutinskimi opravili in opravili, ki zahtevajo takojšnjo odzivnost npr. reševanje reklamacij, za izobraževanje in doseganje poslovne odličnosti pa zmanjka časa.

1.2.1 Mehki in trdi načini prenove poslovanja

1.2.1.1 Demingov krog

Ena najstarejših metod uvajanja sprememb s postopnimi koraki, je t. i. PDCA metoda oz. Demingov krog, ki temelji na procesnem pristopu in se izvaja v štirih fazah (Kovačič & Bosilj Vukšič, 2005, str. 94):

- **P**lan – načrtuj,
- **D**o – izvedi,
- **C**hek – preizkusi,
- **A**ction – deluj.

V prvi fazi (Plan) formiramo delovne skupine, naredimo opis projekta, opis indikatorjev uspešnosti projekta in oblikujemo cilje projekta

V drugi fazi (Do) izvajamo analizo obstoječega stanja in zbiranmo potrebne informacije od zaposlenih, oblikujemo stališča do sprememb, predlagamo ideje in usmeritve za njihovo uresničitev ter sprejmemo načrt aktivnosti za izvedbo sprejete rešitve.

V tretji fazi (Check) spremljamo izvajanje in učinkovitost predlagane rešitve, ki jo izvajamo na način, da posamezni člani projektne skupine o izvedbi in izvajanju rešitve poročajo vodji projekta. Na osnovi poročil projektna skupina sprejeme odločitve o poteku nadaljnjih aktivnosti.

V četrti fazi (Act) preverjamo delovanje rešitve in v primeru, da je preverjanje uvedenih sprememb pokazalo pomanjkljivosti, se vrnemo na fazo Plan.

Metoda je pomembna, ker nosi v sebi spremljanje in preverjanje oz. kontrolo izvajanja aktivnosti in na podlagi povratnih informacij izboljšuje izvajanje aktivnosti.

1.2.1.2 Metoda 20 ključev

Ena od mehkih metod upravljanja s spremembami je tudi metoda 20 ključev. Metoda je primerna za: izboljšanje kakovosti, zmanjševanje stroškov in skrajševanje pretočnih časov. Sistem 20 ključev je ena od poti za vzpostavitev okolja, ki organizaciji omogoči hitrejše prilagajanje sodobnemu tržnemu okolju in kot taka predstavlja način obvladovanja sprememb. Ključ št. 18 opredeljuje računalniško podporo poslovanju in v okviru podpore učinkovito rabo informacijske tehnologije (Kobayashi, 1995).

Razdeljen je na pet nivojev in v zadnjem petem nivoju je podana strategija za vzpostavitev informacijskega sistema, ki bo prilagojen organizaciji. Informacijski sistem prilagojen organizaciji pomeni, da zadovoljuje vse njene trenutne potrebe in je pripravljen na implementacijo morebitnih sprememb.
Sistem 20 ključev ne omenja upravljanja s tveganjem, najbolj se temu pojmu približa v 18. ključu v četrtem nivoju, ki zahteva uskladitev ciljev vseh zaposlenih in s tem omogoči, da je organizacija »odporna na vreme« in s tem zmožna odziva na spremembe v okolju.

1.2.1.3 Celovito obvladovanje kakovosti

Zelo, če ne najbolj razširjena metoda je metoda celovitega obvladovanja kakovosti (angl. *Total Quality Management*, v nadaljevanju TQM). To je način stalnega izboljševanja dela s poudarkom na ljudeh in postopnem, "nebolečem" spreminjanju poslovnih procesov, zajema pa vse organizacijske enote in vse poslovne funkcije. Način stalnega izboljševanja temelji na neprekinjeni analizi obstoječega stanja in iskanju izboljšav.

1.2.1.4 Metoda najboljše prakse

Metoda, ki je pogosto uporabljena za uvajanje sprememb v bančnem okolju in temelji na uporabi znanih in preizkušenih preteklih »pozitivnih« postopkov pri izvajanju sprememb bančnih poslov. V slovenskem bančnem prostoru je bila v bankah uporabljena pri vzpostavitvi plačilnega sistema Target2.

1.2.1.5 Popolna prenova poslovnih procesov

Izraz BPR pomeni temeljito prenovo in preureditev organizacije oziroma njenih ključnih poslovnih procesov. Gre za metodo šokov, ki naj bi prinesla čimboljše rezultate v čimkrajšem času. Rezultati BPR so radikalne izboljšave v izvajanju procesov in delovanju organizacij, ki se odražajo na za organizacije najpomembnejših kazalcih, kot so stroški izvajanja, kakovost storitev, roki izvedbe.

Metoda se ponavadi uporabi v času, ko se v organizaciji pojavijo težave v zvezi s stroški, kakovostjo, roki. Pri izvedbi BPR je vključitev informacijske tehnologije nujna in za samo izvedbo je njena vloga ključna.

Pri izvajanju BPR vsaka nova informacijsko podprta rešitev prinaša tudi nova tveganja. Zaposleni so v svojem poslovanju kot posamezniki preveč odvisni od tehnologije in postavlja se elementarno vprašanje (še posebej v bančnem sektorju): kako naprej, če odpove računalnik, če zmanjka elektrike, če ni zagotovljene ustrezne tehnološke podpore.

Pri prenovi poslovnih procesov v bančnem okolju gre za zahteven in celovit projekt, ki se kaže v prepletenosti različnih področij in z obsegom vključenih sprememb v bančno prakso. Prenova poslovnih procesov zahteva ustrezno višino sredstev, ki so potrebna za

realizacijo in ustrezno število v projekt vključenih zaposlenih iz bančnega okolja in zunanjih strokovnih sodelavcev in specialistov.

Pri prenovi poslovnih procesov v velikem obsegu se v vseh fazah prenove odpirajo nova vprašanja in iščejo nove najustreznejše rešitve. BPR prinaša velike spremembe in posledično velika tveganja ter negotovost, kratke roke za realizacijo, zato pri zaposlenih povzroča odklanjanje. Odpori pri uvajanju sprememb v velikem obsegu so pri zaposlenih v bančnem okolju veliki.

Običajno velike spremembe prinašajo spremembo v izvajanje poslovnih procesov, kar lahko za določe zaposlene pomeni izgubo delovnega mesta. Za druge lahko pomeni dodatno izobraževanje in delo, ki bo popolnoma drugačno od sedanjega. Sprememba lahko pomeni tudi, da bo zaposleni poleg rednega dela opravljal še dodatna opravila.

1.3 Standardi ISO

Poslovanje izboljšujemo tudi s pomočjo standardov ISO, ki jih izdaja mednarodna organizacija za standarde (angl. *International Organisation for Standardisation*), ki določajo splošne smernice za učinkovito zagotavljanje kakovosti oz. drugih ustreznih smernic (varnost informacijskega sistema, zaščita podatkov) pri poslovanju banke.

Standardi ISO obsegajo različna področja. Na tem mestu bom izpostavil dve področji, ki sta pomembni za obvladovanje operativnih tveganj v Plačilnih sistemih, to sta ISO standard za Zagotavljanje kakovosti (standard ISO 9001 in standard ISO/IEC 27001) in ISO standard za varnost in zaščito podatkov (standard BS 7799 in standard ISO/IEC 27005), ki zajema tudi upravljanje s tveganji.

Obrambo pred operativnimi tveganji predstavlja učinkovita zaščita tehnoloških komponent na različne načine. Pri tem so načrtovalcem v pomoč standardi, ki opredeljujejo ključna področja varovanja tehnoloških komponent (standard PSIST BS 7799).

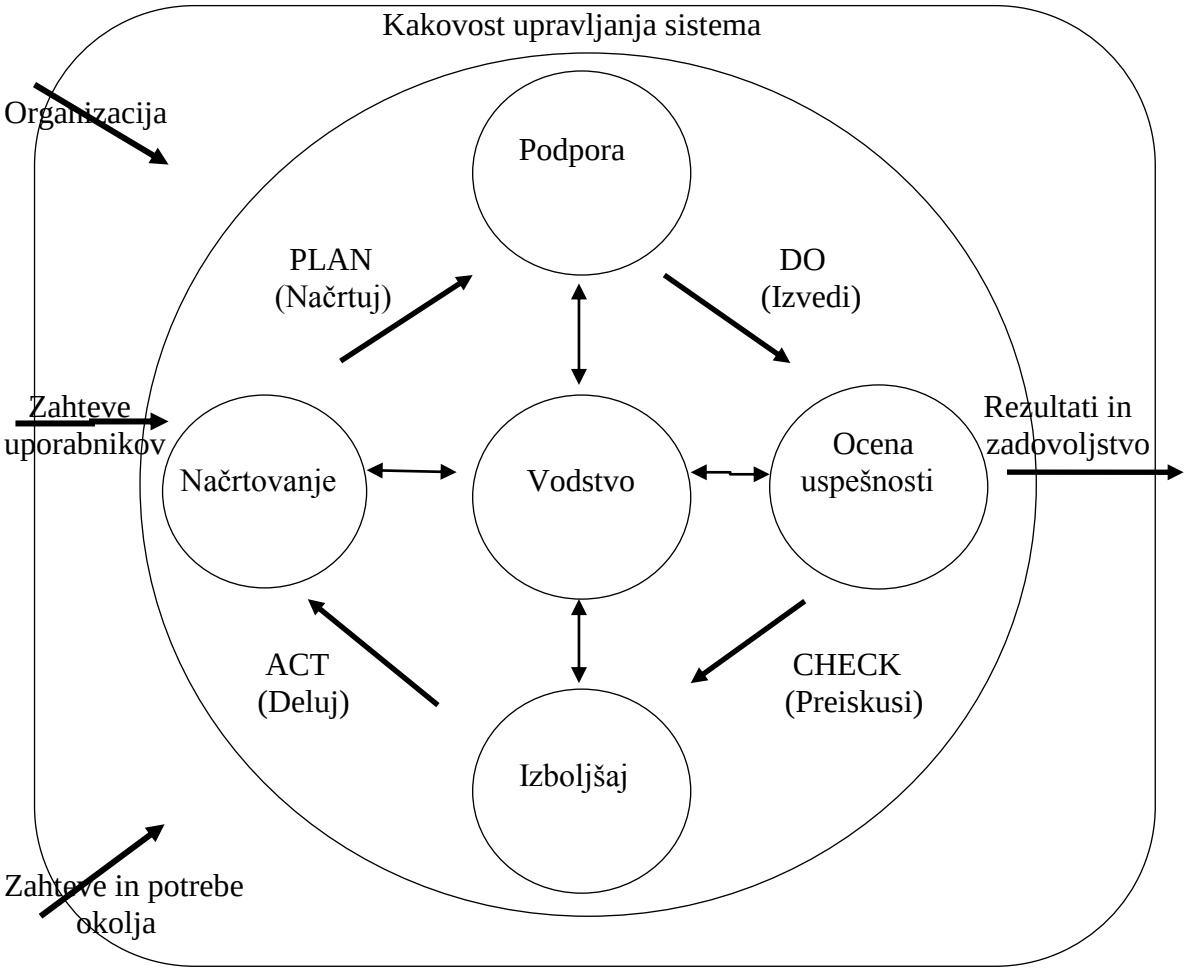
Izpostavljenost informacijskega sistema tveganjem je glede na pretekle dogodke (izredni dogodki v največjih svetovnih bankah) največja prav s strani zaposlenih.

Zato je potrebno upravljanje s spremembami obravnavati celovito, kar pomeni, da je potrebno pri obvladovanju sprememb in tveganj upoštevati tudi dejavnike, ki niso samo tehnološke narave, upoštevati je potrebno tudi organizacijo in kadre, ki pomembno vplivajo na večjo ali manjšo izpostavljenost tveganjem.

ISO standard 9001 emelji na procesnem pristopu, ki vključuje Plan-Do-Check-Act metodo in pristopom, ki upošteva tudi možna tveganja. Procesni pristop omogoča organizaciji, da načrtuje poslovne procese in njihove interakcije.

Metoda sicer upošteva tveganja, analizira morebitne neskladnosti, ki se pojavljajo v poslovanju in zahteva izvajanje preventivnih ukrepov za odpravo morebitnih neskladnosti ter ukrepe, ki preprečujejo ponovitev napake oz. neskladnosti, ni pa eksplicitno navedeno, da je potrebno v fazi planiranja opredeliti vsa možna operativna tveganja. Identifikacija operativnih tveganj zahteva zelo dobro poznavanje poslovnega procesa, s tehnološkim razvojem pa je potrebno identifikacijo tveganj opravljati vedno znova. Procesni pristop omogoča organizaciji, da načrtuje svoje procese in njihove interakcije v skladu z mednarodnimi standardi.

Slika 3: Struktura ISO standarda 9001 v ciklu PDCA



Vir: International Organisation for Standardisation, Quality management systems, 2015.

Prikaz ISO standarda 9001 v ciklu PDCA je prikazan na sliki 3 in zajema sledeče elemente:

- organizacijo
- zahteve uporabnikov
- vodenje kot osrednji element vodenja kakovosti
- zaposleni

- zadovoljstvo strank
- nenehne izboljšave
- odločanje na podlagi uspešnosti
- upravljanje odnosov

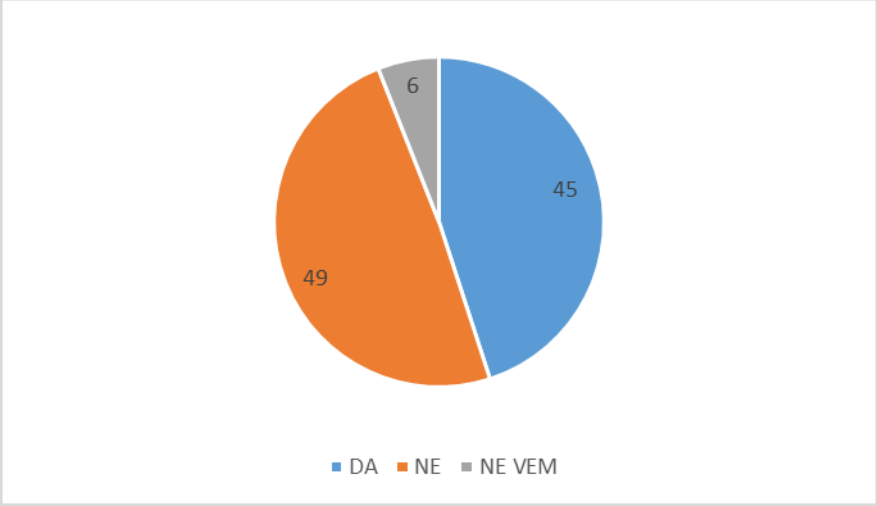
1.4 Merjenje učinkovitosti upravljanja s spremembami

Kako meriti učinkovitost upravljanja s spremembami? Lahko primerjamo znesek vloženih sredstev v prenovo poslovanja z zneskom iz naslova povečanih prihodkov banke (težava je v tem, da povečanih prihodkov ne gre jasno pripisati prenovi poslovanja), lahko izmerimo, kako so spremembe vplivale na zaposlene (delajo učinkoviteje, hitreje, z manj napakami).

Poročanje o učinkovitosti upravljanja sprememb upravi je v bankah stalna praksa. Ponavadi uprave bank ne zahtevajo te vrste poročil, ampak poročilo o uspešno izvedenem projektu. Raziskava, ki jo je opravilo podjetje Prosci Inc. (slika 4), kaže, da je poročanje o učinkovitosti upravljanja sprememb upravi dokaj pogosto.

Glede na to, da se spremembe v bankah izvajajo vsakodnevno, je nemogoče izmeriti natančno učinkovitost implementiranih sprememb. V nalogi bom učinkovitost upravljanja s spremembami ocenjeval z vidika zadovoljstva zaposlenih, z vidika komuniciranja med oddelki in z vidika povečevanja baze znanja v banki na podlagi opravljenih razgovorov z zaposlenimi.

Slika 4: Poročanje o učinkovitosti upravljanja sprememb v %



Vir: Prosci Inc., Reported on Change Management, 2014.

Za upravljanje sprememb v bankah so zadolženi vodje oz. direktorji posameznih oddelkov, ki spremembe v okviru delokroga implementirajo v skladu s svojim znanjem in izkušnjami. Uspešnost njihovega delovanja se kaže tudi skozi rezultate poslovanja banke.

Pri načrtovanju, organiziranju in kontroli uspešnosti upravljanja sprememb je pomembno, da imajo podporo uprave in da delujejo v skladu z vrednotami banke. Kultura usmerjenosti banke k komitentom v smislu »komitent je kralj«, vodi k izboljšanju storitev banke in odnosov s komitenti ter dvigu ugleda banke.

V primeru, da storitev, ki jo komitent pričakuje, ni izvršena v skladu z njegovimi pričakovanji (npr. odprtje transakcijskega računa v dveh dneh, prejem naročene kreditne kartice v treh dneh) in pride do reklamacije, se zgodi, da banka običajno ne preveri vseh vidikov, ki so povzročili reklamacijo in trmasto vztraja pri vodilu »komitent je kralj«.

V primeru, da reklamacija stranke ni upravičena oz. je vzrok za reklamacijo izven banke, je potrebno zaposlene zaščititi. Banke po eni strani zagotavljajo, da so zaposleni največja vrednota bank, po drugi strani pa so zaposleni vedno bolj izpostavljeni povečanemu obsegu dela, pritiskom vodij in uprave ter pritožbam komitentov.

Upravljanje sprememb je kompleksno področje, ki posega v delitev dela, v učinkovitost storilnosti dela, izboljšanje kakovosti storitev s končnim ciljem zniževanja stroškov. Vse to pa zahteva znanja, sposobnosti in izkušnje vodij, ki spremembe uvajajo in implementirajo. Prav tako je pomembna organiziranost banke, ki bo zagotovila, da se vodje oddelkov dejansko vodijo oddelek. Morebitne težave, ki se pojavljajo v majhnih bankah so naslednje:

- vodje oddelkov so preveč zaposleni z nalogami, ki jih delegira uprava (različne komisije, odbori, usklajevanja, popisi, sestanki), za vodenje oddelka in usklajevanje nalog pa zmanjka časa,
- vodje oddelkov so preveč vpeti v operativno delo oddelka (z enakimi zadolžitvami kot njihovi podrejeni in s tem dodatno obremenjeni), za vodenje in usklajevanje nalog v oddelku pa ni dovolj časa.

Napaka, ki sem jo zaznal v organiziranosti oddelkov se kaže v različnem pristopu vodij do vodenja svojega oddelka. Nekateri se usmerijo v operativno delo, drugi so vedno na voljo upravi, vodenje odelka pa prepustijo enemu od sodelvcev v oddelku. S tem se povečuje nezadovoljtvo zaposlenih, ki nimajo »pravega« vodje.

Celovito upravljanje sprememb zahteva upravljanje sprememb na področju celotne banke in zajema spremembe na področju organiziranosti banke, na področju kadrovskih potreb banke, na področju upravljanja odnosov med zaposlenimi, na področju vodenja oddelkov z novimi pristopi, pri tem pa slediti zahtevam strank, jim zagotavljati odlične storitve. Na podlagi dosežene uspešnosti in povratnih informacij zaposlenih in strank, mora banka izdelati bazo znanja, kjer bodo zajete vse dobre prakse, predlogi za izboljšanje poslovanja, omogočena pa bo tudi izmenjava znanja. Izobraževanju zaposlenih v bankah je namenjeno premalo časa in premalo sredstev. V kolikor banka želi v korak s časom, uvajati nove

produkte in širiti poslovanje, mora zaposlenim omogočiti odlična strokovna znanja, poleg tega pa še znanja jezikov, znanja medsebojnega komuniciranja, znanja vodenja in znanja s področja trendov na področju bančništva.

Običajno so navedena znanja omejena na ozek krog zaposlenih, kar ni dovolj. V bankah je izobrazbena struktura na višji ravni kot v drugih panogah, zato je pomembno, da v izobraževanje vključimo čim širši krog zaposlenih. Vlaganje v izobraževanje zaposlenih pomeni tudi obliko nagrade za zaposlene in s tem vzpostavitev povečanega zaupanja v banko. Zaposleni bodo na osnovi izobraževanj lažje, hitreje in bolj strokovno opravljali svoje zadolžitve.

Banke premalo pozornosti namenjajo izkoriščanju znanj in predlogov zaposlenih za spremembe oz. izboljšave. Vsaka sprememba naj bi v svoji osnovi izboljšala delovanje poslovnih procesov in razbremenila banke nepotrebnih opravil. Ideje zaposlenih, ki vsakodnevno opravljajo operativne aktivnosti v večini bank niso sprejete. Razlogov za tako stanje je več.

Najpomembnejši je v nenagrajevanju dobrih, odličnih pa tudi povprečnih predlogov in v zavračanju vsakršnih predlogov s strani zaposlenih. Vodje oddelkov ne želijo sprejeti predlogov in jih posredovati upravi. Uprava v letnih planih določi višino razpoložljivih sredstev za določene aktivnosti in pri tem vztraja. Sredstev za majhne izboljšave ni na voljo, vodje oddelkov pa se ne želijo izpostavljati.

Pomemben vir predlogov so tudi opažanja in vprašanja strank. Banka bi morala na osnovi predlogov, sugestij in vprašanj vzpostaviti evidenco potencialnih sprememb, ki bi strankam olajšale delo in jih poskušati realizirati v čimkrajšem času. Prav tako bi bilo potrebno vzpostaviti programsko opremo, ki bi dovoljevala strankam, da delovanje bančnega produkta prilagodijo svojim potrebam.

Določene specifične funkcionalnosti npr. množična plačila uporablja samo ozek krog uporabnikom, na voljo pa je vsem. Prilagoditev izpiskov prometa na poslovnem računu, po katerih je precejšnje povpraševanje pa ni realizirana. Banke se morajo zavedati, da je vska stranka »posebna« in ima svoje zahteve. Spremembe, ki se vsakodnevno dogajajo bodo banke prisilile, da se bodo morale ukvarjati z vsakim komitentom posebej in mu omogočiti razpolaganje s podatki v obliki kakršni bo želel.

Banke bodo morale poenostaviti postopke za odpiranje in zapiranje poslovnih in osebnih transakcijskih računov. Prav tako bo potrebno poenostaviti postopke kontrole izvajanja gotovinskih plačilnih storitev komitentov, ki jih zahteva regulator. Tu mislim predvsem na kontrolo poslovanja z vidika preprečevanja pranja denarja in poročanje sumljivih transakcij. Meja za poročanje gotovinskih transakcij je postavljena zelo nizko, banka pa za poročanje porabi veliko časa in ostalih resursov.

Banke morajo spremembe obravnavati učinkovito, prepoznati kaj je zares treba spremeniti in ponuditi storitve, ki bodo komitentom in banki prinašale maksimalne koristi. Za pravne osebe pomeni to avtomatizacijo poslovanja, za fizične osebe, npr. upokojence pa prijazen bančnik, ki jim bo v osebnem stiku podal vse informacije.

2 OBVLADOVANJE TVEGANJ V BANČNEM OKOLJU

2.1 Tveganja v bančnem okolju

Vstop Republike Slovenije v Evropsko unijo dne 1. 5. 2004 in tri leta kasneje v Evropsko monetarno unijo, dne l. 1. 2007, je prinesel tudi spremembe in začetek prilagajanja načinov in postopkov obvladovanja vseh vrst tveganj (sistemska, likvidnostna, kreditna, obrestna, operativna in druga) v slovenskem bančnem okolju evropskim standardom.

Glede na to, da je bila prilagoditev na področju obvladovanja bančnih tveganj nujna, je bilo potrebno v slovenskem bančnem okolju sprejeti evropske smernice za obvladovanje operativnih tveganj. Še posebej pomembna so operativna tveganja na področju posameznih bančnih produktov (plačilni promet, kartično poslovanje, spletno bančništvo).

Tveganj v bančnem okolju je najmanj toliko, kolikor je poslovnih procesov. Tveganja in "pomembnost" tveganj (uteži), ki so sicer različna po bankah, so prikazana kot vzorčni primer na sliki 5, težava pa nastane, če se uprava ne zaveda oz. ignorira obstoj operativnih tveganj.

Basel III v primerjavi z Basel II prinaša pomembne doponitve v smislu odgovornosti uprav za obvladovanje tveganj in tudi vrsto potrebnih javnih razkritij bank (Štiblar, 2010, str. 183).

Prav vsako izvajanje poslovnega procesa je izpostavljeno tveganjem in širša kot je paleta poslovnih procesov oz. storitev, večja je možnost, da bo poslovni proces moten. Seveda obstajajo operativna določena tveganja, ki so skupna vsem informacijsko podprtim poslovnim procesom npr. izpad komunikacijskih povezav ali električne energije.

Tveganje je torej verjetnost, da se bo poslovni proces izvajal napačno, kar pomeni, da dobljeni rezultati ne bodo v skladu z dogovorjenimi, s tem se bo zmanjšala verjetnost in možnost organizacije, da doseže svoje zastavljene cilje. Tveganja lahko povzročijo izgubo denarja in premoženja ali izgubo ugleda in dobrega imena. V obeh primerih pa gre za izgube, ki so rezultat prepletenih dejavnikov, kateri sestavljajo poslovna tveganja, in pojav ene vrste tveganja povzroči možnost pojava druge vrste tveganja. Glede na to, da so informacijski sistemi vse bolj kompleksni, so tudi tveganja večja, saj je možnost, da se pojavi napaka zaradi večjega števila informacijskih komponent, vedno večja. Različni

avtorji različno kategorizirajo bančna tveganja. Bančna tveganja delimo na (Greuning, 2003, str. 3):

- finančna tveganja (struktura bilance stanja, prihodkovno, kapitalsko, kreditno, likvidnostno, tržno in valutno tveganje),
- operativna tveganja (notranje prevare, zunanje prevare, kadrovska politika, varnost del. mesta, stranke, produkti in poslovne storitve, okvare delovnih sredstev, tehnološko tveganje, procesno upravljanje),
- poslovna tveganja (makro politika, finančna infrastruktura, pravna infrastruktura, pravne obveznosti, usklajenost s predpisi, tveganje ugleda, deželno tveganje),
- tveganja okolja (politično tveganje, tveganje okužbe, bančne krize, druga zunanja tveganja).

Kapitalski sporazum Basel II je kot najpomembnejša izpostavil kreditna, finančna in operativna tveganja, Basel III pa v Direktivi 2013/36/EU tveganja v bančnem okolju deli na :

- kreditno tveganje in tveganje nasprotne stranke,
- tveganje koncentracije,
- tveganje listinjenja,
- tržno tveganje,
- tveganje spremembe obrestne mere, ki je posledica dejavnosti iz netrgovalne knjige,
- operativno tveganje,
- likvidnostno tveganje,
- Tveganje prevelikega finančnega vzvod.,

V letu 2014 je bil z Uredbo št. 468/2014 vzpostavljen mehanizem enotnega bančnega nadzornika (angl. *Single Supervisory Mechanisem - SSM*), namenjen nadzoru pomembnih bank, ki sodelujejo v stresnih testih. V stresnih testih je običajno poudarek na kreditnih tveganjih, testira pa se tudi nabor tržnih tveganj, deželnega tveganja, stroške financiranja in neto obrestni prihodki. V testih so zajeta tudi operativna tveganja z vidika kapitalskih zahtev, uporabljen je enostaven pristop.

Za primer reševanja in prisilnega prenehanja bank je Evropski parlament izdal Direktivo 2014/59/EU, ki vzpostavlja okvir za reševanje kreditnih institucij in investicijskih podjetij. V slovensko zakonodajo je bila Direktiva imlementirana v okviru Zakona o reševanju in prisilnem prenehanju bank.

Direktiva omogoča pripravo in preprečevanje bančnih kriz, zgodnje posredovanje v primeru, da se banka znajde v težavah in njeno reševanje, če se kljub vsemu znajde v težavah in je ogrožen njen obstoj (Banka Slovenije, 2016).

2.2 Operativno tveganje

2.2.1 Metodologije upravljanja operativnih tveganj

Metodologija upravljanja in obvladovanja tveganj je prepuščena bankam, ki se tega področja lotevajo na različne načine in izbirajo različne pristope. Pred uvedbo baselskega kapitalskega sporazuma leta 2007 imenovanega Basel II, je bilo upravljanje operativnega tveganja v domeni oddelkov informacijske tehnologije oz. informacijske podpore, v zadnjih letih pa v okviru oddelkov za upravljanje s tveganji.

Vsako tveganje potencialno zmanjšuje dobiček in prav zato je aktivno upravljanje s tveganji ključna bančna funkcija, ki ji lahko prinese konkurenčno prednost. Nova ljubljanska banka že v letnem poročilu za leto 2004 omenja obvladovanje tveganj ko navaja, da so bile sprejete pomembne odločitve povezane z razvojno strategijo na področju informacijske tehnologije z namenom boljšega obvladovanja tveganj, povezanih z informacijsko tehnologijo. Operativno tveganje se pojavlja na dveh ravneh, na tehničnem nivoju, ki zajema informacijski sistem z merjenjem oz. oceno tveganj (lahko je nepopolno oz. pomanjkljivo), in na organizacijskem nivoju, ki zajema poročanje in nadzor tveganja ter vsa pravila in politike v zvezi s tem (Besis, 1998, str. 12).

Obvladovanje sprememb in tveganj je potrebno gledati tudi skozi prizmo stroškovne učinkovitosti. Stroški namenjeni obvladovanju sprememb in tveganj naj ne bi presegali morebitnih (potencialnih) izgub banke iz naslova obvladovanja tveganj.

Izgube v bankah nastajajo tudi iz naslova neobvladovanja operativnih tveganj, v javnosti najbolj znan primer je projekt Sigma, ki je zaradi neobvladovanja sprememb in identifikacije operativnih tveganj zašel v težave.

Pomembno je, da ima vsaka banka izdelane podrobne plane za obvladovanje sprememb (v tehnološkem okolju npr. zamenjava programske ali strojne opreme, izguba ključnih kadrov, varovanje informacij), s katerimi bodo zmanjšale tudi operativna tveganja. Žal so v večini bank plani za upravljanje s spremembami omejeni na oddelek informacijske tehnologije.

Po Baselskem odboru za bančni nadzor je operativno tveganje opredeljeno kot "tveganje izgube zaradi neustreznih ali neuspešnih notranjih postopkov, ljudi in sistemov ali zaradi zunanjih dogodkov" in ga tako sestavljajo tveganja na področju poslovnih procesov, organizacije, kadrov in informacijske tehnologije.

Za merjenje operativnega tveganja po Basel III lahko uporabljamo naslednje pristope:

- enostaven pristop (angl. *Basic Indicator Approach*),

- standardiziran pristop (angl. *Standardised Approach*),
- napreden pristop (angl. *Advanced Measurement Approaches*).

Zakaj nastanejo tveganja ? Tveganja na področju organizacije nastanejo zaradi slabega razumevanja in poznavanja poslovnih procesov, neupoštevanja notranjih in zunanjih pravnih regulativ, nezadostnega in pomanjkljivega strateškega in operativnega načrtovanja, neustreznega upravljanja s kadri, pomanjkljivega vodstvenega nadzora.

Tveganja na področju informacijske tehnologije pa lahko nastanejo zaradi neustrezne podpore poslovnim procesom, nedorečenih poslovnih pravil, odpovedi posameznih komponent, ki sestavljajo informacijski sistem (sistemska in uporabniška programska oprema, podatkovne baze, komunikacijska oprema in strojna oprema), nedelovanja svetovnega spleta, pomanjkanja ustrezne zaščite pred računalniškimi virusi.

Tveganja, ki jih povzročijo ljudje (zaposleni) nastanejo najpogosteje zaradi nepoznavanja postopkov, neupoštevanja navodil, preobremenitve na delovnem mestu.

Tveganja, ki jih povzročijo zunanji dejavniki, lahko nastanejo zaradi nezanesljivosti najetih zunanjih storitev in nezadostne podpore zunanjih partnerjev in vzdrževalcev.

Tveganja na področju kadrov nastanejo zaradi nezadostnega števila zaposlenih na določenem področju, nezadostne usposobljenosti (študenti in pripravniki), napak pri izvajanju poslovnega procesa, kraje zaupnih in drugih podatkov.

Možna operativna tveganja pri uvajanju novega poslovnega procesa so nezainteresiranost zaposlenih (problem motivacije, uvedba »neprijetnih« sprememb v poslovnem procesu), nepoznavanje informacijske tehnologije, nezadostno in pomanjkljivo izobraževanje, tehnološki komunikacijski problemi, zagotavljanje varnosti in zaščite, elektronska nepovezanost zaposlenih, problemi na pravnem področju.

Oddelki za upravljanje operativnih tveganj se ukvarjajo z vsemi vrstami tveganj na nivoju banke, operativnim tveganjem na posameznih področjih pa ponavadi ne namenjajo dovolj pozornosti, ne komunicirajo s posameznimi oddelki in ne delujejo proaktivno.

Druga težava, ki sem jo zaznal pri obravnavanju operativnih tveganj je, da so le-ta pomembna in upravljana samo v oddelku informacijske tehnologije. Odeelek informacijske tehnologije je zelo pomemben, če ne eden najpomembnejših oddelkov banke in možnost, da se bo morebitna grožnja pojavila zaradi pomankljive varnosti v tehnoloških komponentah je velika.

Komunikacija zaposlenih v banki z zunanjimi partnerji poteka preko različnih komunikacijskih poti (spletne aplikacije, elektronska pošta, omrežja za prenos plačilnih

sporočil, faks, telefon, dopis, osebni sestanek) in vsaka od teh poti predstavlja potencialno grožnjo. Vsak oddelek ima faks, zaposleni uporabljajo elektronsko pošto, kar pomeni, da je praktično vsak zaposleni možna tarča napada.

Lažna elektronska pošta zaposlenim, ki jim naloži klik na določeno spletno stran, lahko posledično omogoči vdor v informacijski sistem banke.

Banke se morajo soočiti z vsemi potencialnimi grožnjami, ki se prav tako izpopolnjujejo in povzročajo potencialna operativnega tveganja. Tarče v dobi globalizacije niso samo bančni sistemi, ampak vsi zaposleni. Zaposleni imajo dostop do zaupnih podatkov komitentov in jih morajo v skladu z bančnim kodeksom varovati. Zelo težko je preprečiti »uhajanje« informacij ali napake pri izvajanju delovnih postopkov, če so zaposleni nezadovoljni z delom, z osebnimi prejemki, z obremenitvami na delovnem mestu.

Vse našteto predstavlja vir in vzrok, da se operativna tveganja pojavljajo, njihovo omejevanje pa zahteva aktivnosti na področju ureditve organiziranosti banke, na kadrovskem področju (nagrajevanje in druge spodbude), na področju vključevanja zaposlenih v širše delovanje banke in na področju osebnega izobraževanja ter napredovanja.

Problem v bankah je, da so zaposleni na istem delovnem mestu tudi dest in več let in ves čas prejemajo enak dohodek. Osebnih izzivov jim banka ne ponudi, izobraževanja so skrčena na minimum oz. potekajo samo v ozkem krogu za določeno vrsto opravila, dodatna znanja niso ovrednotena.

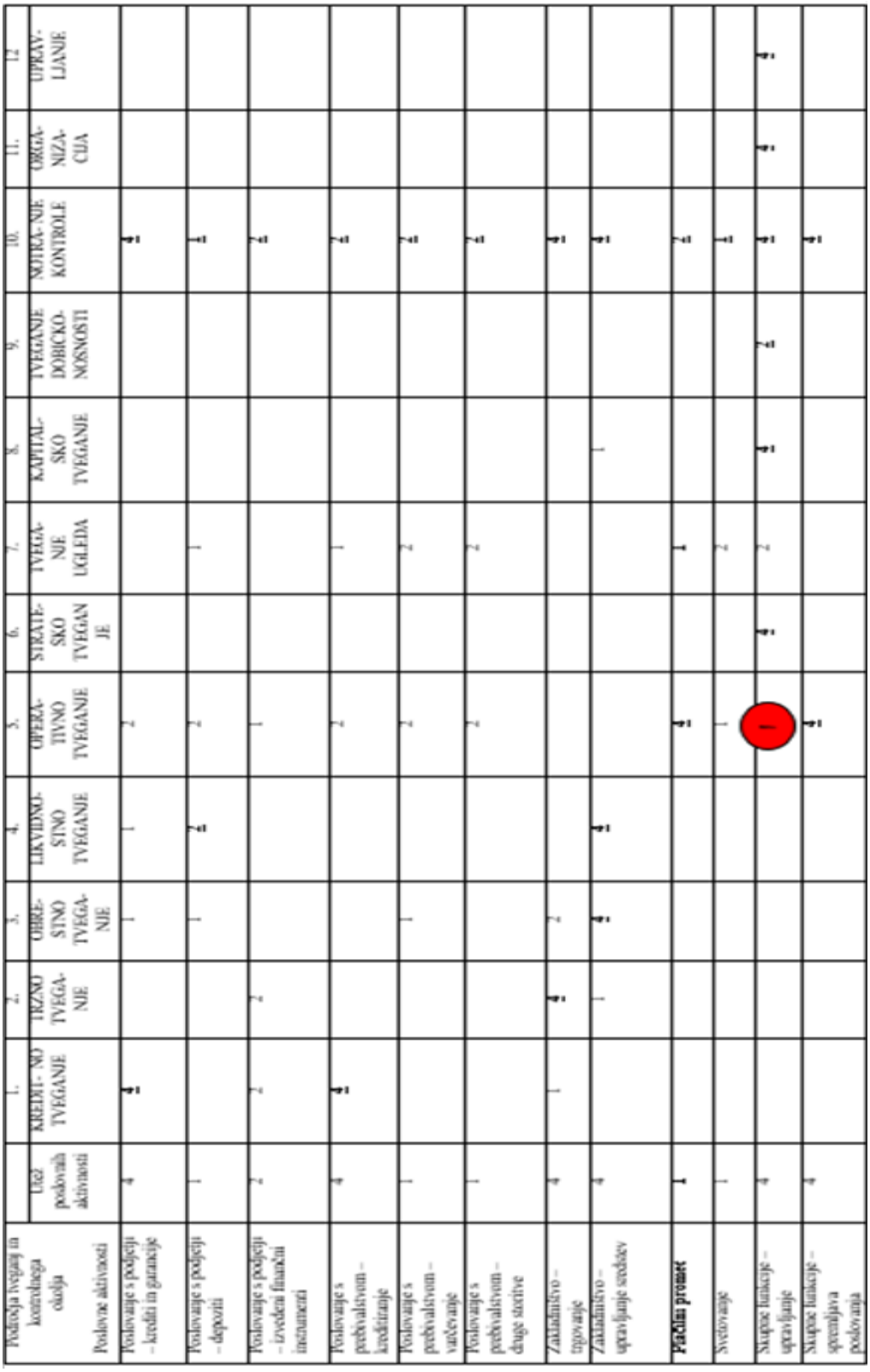
Enostavni pristop uporabimo, če banka nima vzpostavljenega sistema za upravljanje operativnih tveganj ali v primeru, da banka posluje manj kot tri leta in nima zgodovine beleženja dogodkov operativnega tveganja.

Standardiziran pristop vključuje kvalitativne standarde in kvantitativne standarde, ki vključujejo v nadzor nad upravljanjem operativnih tveganj tudi Upravo banke.

V okviru naprednega pristopa lahko uporabimo model na podlagi scenarijev v katerem vnaprej ocenjujemo operativna tveganja banke, kar pomeni, da definiramo ranljivost banke glede na npr. strokovno znanje zaposlenih, kontrole na področju dodeljenih pooblastil, nenamerne napake, namerne napake, neupoštevanje internih aktov, zakonske zahteve (Rotovnik, 2005, str. 36).

Informacije, ki jih pridobimo lahko ocenjujemo na podlagi odgovorov kaj se zgodi v primeru, da ni strokovnega znanja, ni dokumentiranih postopkov, ni odgovornih oseb, ni pooblastil za delo, odpovedi centralnega strežnika, prekinitve komunikacijske povezave, izvedbe aktivnost izven predvidenega urnika.

Slika 5: Matrika tveganj v bančnem okolju



Vir: Banka Slovenije, Proces ocenjevanja tveganj, 2007, str. 15.

Pri nalogah ocenjevanja operativnega tveganja gre predvsem za izvedbo pregledov z

namenom pridobitve mnenja o obsegu obvladovanja ustreznih poslovnih in informacijskih kontrol ter z vzpostavitvijo baze dogodkov operativnih izgub za pripravo poročil vodstvu organizacije o pomanjkljivostih v poslovnem in informacijskem sistemu ter za pripravo priporočil za odpravo tveganj.

2.2.2 Merjenje in ocenjevanje operativnih tveganj

Tveganja in grožnje je treba pravočasno odkriti in oceniti. Pri tem nam je lahko v pomoč programska oprema za upravljanje in oceno poslovnih procesov (angl. *Business Process Management Systems,* v nadaljevanju BPMS) oz. različna orodja za analizo procesov, kot so npr. Process Survey Tool, CRAMM, s katerimi lahko banka analizira poslovne procese in odkrije slabosti pri organiziranju le-teh.

Merjenje operativnih tveganj običajno temelji na analizah preteklih dogodkov, še bolj pomembno pa je, da lahko identificiramo bodoča tveganja.

Podatki škodnega dogodka, ki ga povzroči operativno tveganje, so pomembni za izogibanje enakim dogodkom v bodočnosti. Podatke je potrebno zapisati v bazo dogodkov in določiti potrebne aktivnosti za odpravo morebitne škode in aktivnosti, ki bodo odpravile vzrok za nastanek škodnega dogodka.

Podatki, ki so pomembni za evidenco škodnih dogodkov, so datum izdelave poročila, poročevalec, delovno mesto, organizacijska enota, datum začetka dogodka, datum konca dogodka, trajanje dogodka, povzročitelj dogodka, aktivnost – postopek, kategorija dogodka, opis dogodka, ocena dejanske škode, ocena potencialne škode, obrazložitev dejanske in potencialne škode, predlagani ukrepi.

Ena prvih slovenskih bank je že v letu 2008 v okviru obvladovanja tveganj vzpostavila sistem zbiranja škodnih dogodkov ter identifikacije in ocenjevanja operativnih tveganj. Za merjenje potencialnih izgub pa je v banki potekala tudi identifikacija in ocenjevanje tveganj.

Nadzor nad pregledom obvladovanja operativnih tveganj je v pristojnosti centralne banke, ki v svojih pregledih »obdela« aktivnosti spremljanja določenih sistemov, ocenjuje njihove usklajenosti s cilji centralne banke oz. določenih standardov.

Centralne banke se pojavljajo v vlogi preglednikov predvsem zaradi naslednjih razlogov (Banka Slovenije, 2007):

- pregledov v povezavi z osnovnimi funkcijami banke, predvsem glede varnosti, učinkovitosti in zagotavljanja finančne stabilnosti,

- izkušenj, ki jih imajo z nudenjem poravnalnih računov in kot operaterji plačilnih sistemov,
- učinkovitosti, ki izhaja iz njihove nepristranskosti in pravne moči,
- izkušenj s plačilnimi in poravnalnimi sistemi.

Vsak večji operativni problem poravnalnih sistemov ali bank ima za posledico likvidnostne težave v plačilnih sistemih in lahko privede do sistemskega tveganja.

Težave v delovanju plačilnih in poravnalnih sistemov vplivajo na (Banka Slovenije, 2007):

- nemoteno izvajanje monetarne politike,
- tekoče delovanje plačilnih sistemov,
- zmanjšanje stabilnosti celotnega finančnega sistema

Poravnalni sistemi so oblikovani tako, da lahko banke obvladujejo poravnalno tveganje in da se problemi ene banke ne širijo na druge. V skladu s tem centralne banke na področju poravnalnih sistemov pri upravljavcih izvajajo redne aktivnosti pregledov.

2.2.3 Spremljanje operativnih tveganj

Operativna tveganja na področju plačilnih sistemov spremljamo z beleženjem vseh odklonov, ki nastajajo med izvajanjem poslovnega procesa. Problem, ki nastaja pri spremljanju dogodkov operativnega tveganja, je že v sami naravi poslovnega procesa, ki se v banki izvaja skozi več organizacijskih enot oz. oddelkov.

Gre za odklone na vseh področjih in oddelkih, kjer se pojavljajo operativna tveganja. Beležiti je potrebno vse napake, ki izvirajo iz delovanja zaposlenih (ročni vnosi, avtorizacije, monitoring), iz delovanja aplikacij (napake v programih, bazi podatkov), iz delovanja strojne opreme (prekinitve delovanja strežnikov, diskovnih enot) in iz delovanja komunikacijske opreme (nedelovanje omrežja, elektronske pošte). Odklone in težave spremljamo in beležimo dnevno.

2.2.4 Metodologije obvladovanja operativnih tveganj

Banka Slovenije je leta 2007 bankam v obliki priporočila izdala dokument Metodologija imenovana Proces ocenjevanja tveganj, ki, vsebuje naslednje elemente (Banka Slovenije, 2007):

- identifikacija tveganj po Baslu II,
- identifikacija tveganj v organizaciji,
- ocenjevanje in razvrščanje tveganj:
  - samoocenjevanje,

    - razvrščanje tveganj,
    - kriteriji za razvrščanje tveganj v organizaciji,
    - definiranje kazalnikov tveganja,
    - merjenje tveganja,
- spremljanje operativnega tveganja:
    - zbiranje podatkov o dogodkih operativnega tveganja,
    - vrednotenje dogodkov operativnega tveganja,
    - opredelitev rokov za poročanje o dogodku OT,
    - opredelitev nabora podatkov za poročanje o dogodku operativnega tveganja,
    - obdelava podatkov operativnega tveganja,
    - interno poročanje,
- obvladovanje operativnega tveganja:
    - ključna dokumentacija za obvladovanje OT,
    - možnosti za obvladanje tveganja,
    - sprejem tveganja,
    - zmanjšanje in prenos tveganja,
    - izognitev tveganju,
- kontrole pri obvladovanju operativnih tveganj:
    - sistem notranjih kontrol,
    - notranja revizija,
    - zagotavljanje skladnosti s predpisi in internimi akti.

Metodologija za obvladovanje operativnih tveganj na vseh področjih temelji na aktivnostih s katerimi analiziramo, merimo, ocenjujemo in obvladujemo tveganja. Pri identifikaciji tveganj so upoštevani notranji in zunanji dejavniki, poslovna politika in strategija organizacije, katera vpliva na izpostavljenost organizacije operativnim tveganjem. Rezultat identifikacije je razvrščanje operativnih tveganj in pripadajočih škodnih dogodkov, na osnovi katerih se lahko pripravi obrazec škodnih dogodkov.

Z identifikacijo tveganj dobimo vrste in opredelitveh dogodkov iz naslova operativnih tveganj po Basel II (Banka Slovenije, 2007), ki so:

- notranja goljufija povzroči izgubo zaradi kraje, zaradi neupoštevanja zakonskih podlag ali internih aktov,
- zunanja goljufija povzroči izgubo zaradi kraje in poneverjanja,
- ravnanje v zvezi z zaposlovanjem in varnostjo pri delu povzroči izgubo zaradi neurejene skladnosti s pogodbami, ki urejajo zaposlovanje in varnost pri delu,
- negativna poslovna praksa povzroči izgubo zaradi neizpolnjevanja pogodbenih obveznosti do strank,
- škodni dogodek na premoženju, ki vključuje izgube, ki nastanejo zaradi uničenja premoženja in zaradi naravnih nesreč,
- izpadi sistemov vključujejo dogodke, ki povzročijo izgubo zaradi izpada sistemov,

Na osnovi identifikacije tveganj pa lahko škodne dogodke operativnega tveganja razvrstimo v več podkategorij:

- varnost informacijskega sistema, vdor v računalniški sistem,
- neustrezna ravnanja z zaposlenimi,
- napake kadrov pri izvajanju aktivnosti (zajem in obdelava podatkov),
- kraja podatkov in sredstev s strani zaposlenih,
- kraja podatkov in sredstev s strani zunanjega vdora,
- napake v sistemih (programi, obdelave, parametri, arhiviranje),
- napake pri poročanju nadzornikom, upravljavcem in državnim organom.

Pri beleženju škodnih dogodkov ocenimo dejansko oz. potencialno škodo, odgovornost za nastanek škodnega dogodka, vzrok nastanka in predlagamo ukrepe za odpravo operativnega tveganja.

Leta 2010 je zaradi gospodarske krize in pomanjkljivosti Basla II, v veljavo stopil nov Baselski sporazum, t.i. Basel III, ki zajema tri stebre, in sicer minimalne kapitalske zahteve, regulatorni nadzor in tržna disciplina. Glede na sporazum Basel II krepi pokrivanje kreditnih in drugih tveganj, uvaja dodatne kapitalske zahteve in finančni vzvod, krepi pokrivanje tveganj ter zaostuje standarde za nadzor.

Basel III uvaja javna razkritja tveganj in določa minimalne standarde za izboljšanje likvidnostne odpornosti bank na stres, največji poudarek je na kreditnem tveganju in razširitvi regulatornega nadzora v smislu nadzora tveganja na ravni banke in obvladovanju specifičnih vrst tveganj (tveganje izgube poslovnega ugleda banke).

Na podlagi Basel III je sta Evropski parlament in svet sprejela Direktivo o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij (Direktiva 2013/36/EU) in Uredbo o bonitetnih zahtevah za banke in investicijska podjetja (Uredba EU št. 575/2013).

Uredba o bonitetnih zahtevah banke opredeljuje naslednje metodologije za merjenje učinkov operativnih tveganj, s poudarkom na izpostavljenosti tveganjem v stresnih situacijah:

- enostavni pristop,
- standardiziran pristop,
- napreden pristop:
    - kvalitativni standardi,
    - kvantitativni standardi

Kapitalska zahteva za operativno tveganje je enaka 15% triletnega povprečja relevantnega kazalnika. V kazalnik so vključeni z vsoto (z negativnim ali pozitivnim predznakom) naslednji elementi : prihodki iz obresti, odhodki za obresti, Prihodki od delnic in vrednostnih papirjev, prejete opravnine/provizije, dane opravnine/provizije, čisti dobiček ali čista izguba iz finančnih poslov in drugi poslovni prihodki). EBA bo osnutek regulativnih tehničnih standardov za določitev metodologije za izračun relevantnega kazalnika pripravila do 31. 12.2017.

Merila za uporabo standardiziranega pristopa zahtevajo, da ima banka vzpostavljen dobro dokumentiran sistem ocenjevanja operativnega tveganja in njegovega obvladovanja z jasnimi odgovornostmi. Nadalje zahtevajo, da banka vključi izdelan sistem v procese upravljanja tveganj banke in je predmet rednega neodvisnega pregledovanja. Banka mora uvesti sistem poročanja višjemu vodstvu, vzpostavljene mora imeti tudi postopke za ustrezno ukrepanje.

Kvalitativni standardi zahtevajo, da ima banka neodvisno funkcijo za upravljanje operativnega tveganja, da so podatkovni toki in procesi, ki so povezani s sistemom banke za merjenje tveganj pregledni in dostopni.

Kvantitativni standardi vključujejo standarde, ki so povezani s procesom, notranjimi podatki, zunanjimi podatki, analizami scenarijev, poslovnim okoljem in dejavniki notranjih kontrol.

2.3 Tveganja na področju plačilnih sistemov

Menim, da operativnemu tveganju ni dan zadosti velik poudarek, saj se večina sprememb nanša na kreditna tveganja in kapitalske zahteve v zvezi s kreditnimi tveganji. V zvezi z operativnimi tveganji se v Direktivi navaja, da nadzorni organi zagotovijo, da bodo banke izvajale tako politiko in procese za ovrednotenje in upravljanje izpostavljenosti operativnemu tveganju, ki bodo omogočili čim manjšo stopnjo operativnega tveganja. Od bank se zahteva da pripravijo krizne načrte v primeru pandemij in načrte neprekinjenega poslovanja kot je bilo že v Basel II.

V plačilnih sistemih se pojavljajo poravnalna in likvidnostna tveganja, ki nastanejo, če banka odobri sredstva komitentom na transakcijskem računu ob prejemu obvestila o plačilnem sporočilu še preden s strani upravitelja plačilnega sistema prejme obvestilo o dokončnosti poravnave (Anko, 2010).

Kreditno tveganje nastane, ko eden ali več udeležencev v plačilnem sistemu ne more izpolniti svojih obveznosti. Te vrste tveganja zmanjšujejo z jamstvenimi shemami vzpostavljenimi pri upravitelju plačilnih sistemov, ki opredeljujejo prispevek posamezne banke v poravnalni jamstveni shemi glede na višino plačilne udeležbe v plačilnih sistemih.

Sistemsko tveganje predstavlja alarmantno tveganje v plačilnih sistemih. Zgodi se takrat ko nezmožnost enega udeleženca v plačilnih sistemih, ki ne more poravnati svojih obveznosti, povzroči, da svojih obveznosti ne morejo poravnati tudi ostali udeleženci. To povzroči t. i. domino efekt.

Operativna tveganja v plačilnem sistemu so povezana z nenamernimi dogodki in ravnanji, kot je npr. izpad strojne opreme, izpad programske opreme, neučinkovito planiranje uvedbe novih sistemov in postopkov za primere izpadov in nesreč.

Med operativna tveganja, ki so zaznana v bančnem okolju, sodijo npr. tveganja, ki izhajajo iz (Bankart, 2013):

- delovanja infrastrukture (strojna, programska in komunikacijska oprema),
- delovanja zaposlenih (znanja, veščine, motivacija, zamenljivost kadra),
- delovanja procesov (ustreznost procesov in kontrol, postavitev ciljev, sestava in jasnost procesov),
- delovanja sistemov (varnost, razpoložljivost, primernost informacijske tehnologije in prostorov),
- delovanja okolja (nezaželene ali nepričakovane spremembe, kriminal, nesreče, izredni dogodki),
- pravnih tveganj (kršenje ali nepravilno upoštevanje zakonov, podzakonskih aktov, navodil, priporočil in sklenjenih pogodb).

Operativno tehnološka tveganja se lahko učinkovito zmanjšuje oziroma odpravlja na različne načine – npr. poleg primarnega sistema vzpostavimo še sekundarni sistem in še dodatni rezervni center, podvajanje ostalih tehnoloških komponent sistema ipd. Verjetno najtežje odpravljivo pa je operativno tveganje, ki ga vnaša t. i. človeški faktor.

Tovrstno tveganje se lahko omeji z največjo možno stopnjo avtomatizacije vseh postopkov v okviru plačilnega sistema.

Tveganja goljufij in zlorab so povezana z namernimi ravnanji in so lahko posledica notranjega ali zunanjega delovanja. Notranje goljufije in zlorabe se poskuša preprečevati z večstopenjskim sistemom odgovornosti, v katerem noben posameznik ne more izvršiti škodljivega dejanja ali posega v sistem.

Problem zunanjih zlorab pa predstavlja predvsem nepooblaščen dostop do informacij, ki se prenašajo v okviru plačilnih sistemov, njihovo spreminjanje ipd. Tovrstne zlorabe se poskuša preprečiti z uporabo ločenih komunikacijskih omrežij, varnostnih algoritmov za kriptiranje podatkov in procedur za identifikacijo udeležencev plačilnih sistemov.
Možnosti za obvladovanje tveganj so (Vaughan, 1997, str.18):

- sprejem tveganja,

- zmanjševanje tveganja,
- prenos tveganja,
- izognitev tveganju,
- deljenje tveganja.

Katero možnost bo banka izbrala, je seveda odvisno od nje same, najpogosteje pa gre za obvladovanje tveganja z uporabo vseh petih možnosti. Če gre za manjša tveganja, ki bi zahtevala prevelik vložek, se taka tveganja sprejme in poskuša obvladovati na druge načine.

Zmanjševanje tveganja doseže banka tudi s spremembo poslovnih procesov, spremembo postopkov, spremembo poslovnih pravil, prenosom tveganja ali z večjim naborom uporabljenih kontrol. Prenos tveganja na drug oddelek je neprimeren, posebej, če gre za dogovorjene postopke znotraj enega oddelka, ki niso prenosljivi na druge.

S kontrolami obvladovanja tveganj je potrebno skrbeti za redno spremljanje operativnih tveganj in redno poročanje oddelku za operativna tveganja. Kontrolo nad obvladovanjem tveganj se zagotavlja z nadzorom sprememb postopkov in posodobitvijo dokumentacije, ki se nanaša na uvedbo novih ali spremembo obstoječih postopkov.

Redno je potrebno izvajati notranje in zunanje kontrole za obvladovanje operativnih tveganj (notranja in zunanja revizija). Pomembno je, da banka v okviru in neodvisno od razpoložljivih resursov deluje predvsem na zmanjševanju tveganj na čim manjšo možno raven.

Ocena tveganja obvladovanja informacijske tehnologije se običajno sestoji iz ocene naslednjih informacijskih komponent: procesi in podatki, osebje in prostori, komunikacijska infrastruktura, strojna oprema, programska oprema, informacije v elektronski obliki, papirni dokumenti ter ocene groženj in klasificiranje škodnih dogodkov, ki bi potencialno lahko škodile informacijskim komponentam organizacije banke ter ogrozile zaupnost, razpoložljivost, celovitost, kot so interni kriminal, eksterni kriminal, postopki in aktivnosti zaposlenih, komitenti, storitve, dobra poslovna praksa, odpoved ali zaustavitev sistemov, upravljanje sistemov, ocena verjetnosti uresničitve groženj.

Z oceno verjetnosti, da se bo dogodek zgodil, banka ugotavlja, kakšna je verjetnost, da se bo dogodek zgodil. Majhna verjetnost je, če gre za dogodek, za katerega je malo verjetno, da se bo zgodil, srednja verjetnost je, če gre za dogodek, ki se redko zgodi, in visoka verjetnost je, če gre za zelo verjeten dogodek.

Z oceno škode, ki bi jo grožnja lahko povzročila, in stopnje posledic na poslovanje banka ugotavlja, kakšna škoda in posledice bi lahko nastale zaradi dogodka. Škoda je majhna, če

je stopnja posledic manj resna, škoda je srednja, če je stopnja posledic resna, in škoda je visoka, če je stopnja posledic kritična.

Z oceno stopnje izpostavljenosti je banki omogočeno, da ugotovi, katerim grožnjam je najbolj izpostavljena. Ocena stopnje izpostavljenosti se prikazuje s tabelaričnim prikazom odvisnosti verjetnosti uresničitve groženj od stopnje posledic uresničene grožnje

Oceno tveganja določimo z oceno stopnje ranljivosti (majhna, srednja, velika) in oceno učinkovitosti protiukrepov (majhna, srednja, velika).

Škodni dogodki, ki so se pojavili so banki x povzočili minimalno poslovno škodo, bolj pomembno pa je, da škodni dogodki pokažejo ranljivosti, ki jim je banka izpostavljena ter na podlagi analize dogodkov te ranljivosti odpravi. Grožnje katerim je banka izpostavljena so raznovrstne, namerne in nenamerne. Primer grožnje, ki jo je težko vnaprej predvideti je poizvedovanje zunanjih deležnikov (sodišča, odvetniki, stečajni upravitelji) o podatkih komitentov.

Določene podatke o komitentih banka posreduje na osnovi zakonskih podlag. Zunanji deležniki običajno povprašujejo po podatkih na podlagi zakonskih določil, zelo redko pa se zgodi, da namerno povprašujejo po podatkih do katerih niso upravičeni. Banka mora zato dejansko vedno preveriti upravičenost zahtevkov in jih v primeru, da gre za zavajajočo poizvedbo tudi zavrniti.

Obvladovanje tveganj v bankah se v prvi vrsti po veliki krizi v preteklih letih nanaša na kreditna tveganja. Vsa izobraževanja, dodatne kontrole regulatorja, direktive EU so namenjene zmanjševanju kreditnega tveganja v bankah.

Vir kreditnih tveganj v bankah izhaja iz nezmožnosti kreditojemlca, da redno odplačuje kreditne obveznosti. Za odobravanje kreditov je v bankah odgovorna kreditna komisija, dokončno potrditev odobritve odobri uprava banke.

Menim, da je kreditnim tveganjem v banki namenjena prevelika pozornost, napačne odločitve pri odobravanju kreditov ne povzročijo nobenih posledic. Čeprav je za obe vrsti tveganj v banki na voljo kapital za pokrivanjeizgub iz tega naslova, pa je bistvena razlika med operativnim in kreditnim tveganjem v evidentiranju dogodkov in posledicah, ki jih posameznik nosi, če se izkaže, da je povzročil škodni dogodek ali malomarno opravil svojo nalogo.

Dogodek operativnega tveganja lahko povzroči dejansko ali potencialno škodo, ki je vidna tudi komitentom in drugim uporabnikom bančnih storite, medtem ko dogodek iz naslova kreditnega tveganja ni deležen pozornosti izven banke (izjema so seveda velike sistemske banke v državni lasti).

Potencialni škodni dogodki kažejo na nepravilnosti v bankah in njihovo razkritje ostane v domeni bank, ki lahko na podlagi dogodka sprejemejo ustrezne ukrepe. Ocenjujem, da se večina dogodkov operativnega tveganja zgodi zaradi neustrezne oraginiranosti banke, neustrezne organizacije dela v poslovnih enotah in zaradi obremenjenosti zaposlenih z večimi opravili, ki jih morajo opraviti v kratkem času.

Menim, da bi morale biti zadolžitve zaposlenih v poslovnih enotah razporejene tako, da zaposleni opravlja naloge v zaporedju in v okviru urnika. Škodni dogodek, ki sicer ni povzročil izgube banki, je pa povzročil slabo voljo med komitenti in drugimi uporabniki, se nanaša na polnjenje bankomatov, ki se nahajajo v poslovni enoti.

Zaposlen, ki je bil zadolžen za polnjenje bankomata z gotovino, je tisti dan opravljal delo na blagajni in obseg dela s strankami je bil na tisti datum (30. v mesecu) nadpovprečno velik zaradi dviga pokojnin. Istega dne je bilo na bankomatu opravljeno nadpovrečno veliko gotovinskih dvigov kar je povzročilo minimalno stanje gotovine v bankomatu.

Naslednji dan je bil praznik in bankomat se je že zjutraj izpraznil. Ker ni izdelanega sistema za obveščanje, ki bi zaposlene takoj opozoril, da je se bankomat prazni, zaposleni ni naročil gotovine za polnjenje bankomata.

V naslednjih dneh je do uprave prispela pritožba stranke, da ni mogla dvigniti denarja ker je bil bankomat prazen. Pritožba je seveda povzročila iskanje krivca in vzroka zakaj bankomat ni bil napolnjen in zakaj ni bila naročena gotovina.

Izkazalo se je, da je bil krivec za stanje zaposleni, ki je bil nadpovprečno obremenejn z drugimi aktivnostmi v banki, vendar bi kljub temu moral še poskrbeti za gotovino v bankomatu. Zaposleni je bil opozorjen, da naj delo opravlja bolj vestno, neposredna škoda iz tega naslova ni nastala, nastalo pa je potencialno tveganje izgube ugleda banke.

Menim, da je tak pristop k upravljanju z operativnimi tveganji popolnoma napačen. Zaposleni, ki ves dan vestno opravlja delo na blagajni, potem pa »pozabi«, »spregleda« polnjenje bankomata, sploh ne bi bil smel biti zadolžen za tako aktivnost. Aktivnosti bi bilo potrebno razporejati v skladu z razpoložljivim časom in že zjutraj izdelati seznam dnevnih zadolžitev in njihovo izvajanje preverjati vsako uro.

Primer kaže pojav operativnega tveganja katerega pri identifikaciji tveganj nismo predvideli. Pomembno je dejstvo, da se dogodek lahko zgodi kljub večjemu številu zaposlenih v poslovni enoti. Zaposleni, ki bi naj aktivnost izvajal ni bil nadzorovan s strani vodje poslovne enote, prav tako ni bil določen dodatni zaposleni, ki bi aktivnost opravil v primeru, da do določene ure, aktivnost ne bi bila opravljena.

Vse to kaže na pomembnost upravljanja s spremembami še posebej na področju odnosov

med zaposlenimi, saj pomanjkanje komunikacije in neustrezno razporejanje dela lahko povzroči dogodke operativnega tveganja.

3 INFORMACIJSKI SISTEM

3.1 Koncept informacijskega sistema

Koncept informacijskega sistema lahko v ožjem smislu opredelimo kot urejen sistem podatkov, informacij in znanja. Kriteriji, po katerih lahko razvrstimo informacijske sisteme, so: vrsta organizacijske strukture (sektorski oz. oddelčni informacijski sistem, medorganizacijski, raziskovalni), funkcionalna področja (računovodstvo, finance, kadri), vrsta podpore, ki jo zagotavlja (sistem za procesiranje transakcij, upravljavski sistem, sistem za podporo odločanju, sistem za avtomatizacijo pisarniških opravil).

Gradnike informacijskih sistemov lahko razdelimo na (Gradišar et.al., 2005, str.41-42) trde, ki so povezani s tehnologijo, in mehke, ki so povezani z ljudmi, postopki in procesi. Tehnološki del IS poimenujemo informacijska tehnologija, omogoča pa uporabo, zajemanje, shranjevanje, prenašanje in obdelovanje podatkov ter informacij:

- računalniška strojna oprema,
- računalniška programska oprema,
- baze podatkov,
- komunikacijska tehnologija.

Mehki gradniki so:

- ljudje, zaposleni, ki informacijski sistem uporabljajo,
- aktivnosti, postopki in procesi managementa informacij.

Za izvajanje potrebnih aktivnosti je potrebno v informacijskem sistemu v plačilnem prometu učinkovito usklajevati kadrovske, tehnološke in organizacijske vire.

Zmogljivejša informacijska tehnologija, konkurenčna naravnanost okolja in nova znanja zaposlenih postavljajo pred organizacije zahtevo po kakovostnejših načinih upravljanja sprememb in obvladovanja oz. upravljanja tveganj.

Pri zagotavljanju novih in novih zahtev, novega in novega razvoja so ravno zaposleni najšibkejši člen, če govorimo o vlogi ljudi kot vzroku nastajanja operativnih tveganj v informacijskem sistemu. Spopadati se morajo z novimi strokovnimi dejstvi, z intenzivnim sodelovanjem v skupini ali v timu (konflikti), pri tem pa slediti smernicam vodstva in lastnikov, kar vse predstavlja velike pritiske in stresne situacije.

Hiter razvoj informacijskih sistemov od zaposlenih zahteva visoko stopnjo začetne izobrazbe, kasneje pa permanentno izobraževanje. Zaposleni na tem področju so nenehno izpostavljeni velikim spremembam in velikim tveganjem, ki jih prinaša razvoj informatike in strokovnega področja, zato se morajo neprestano prilagajati novim razmeram.

Napake, ki se lahko pojavijo, so namerne ali nenamerne, za vse pa je potrebno predvideti njihovo reševanje in zagotavljanje neprekinjenega poslovanja. Možnost dolgoročnega preživetja bodo imele le tiste banke, ki bodo uspele prilagoditi svoje poslovanje spremembam in pri tem še učinkovito obvladovale operativna tveganja in obenem zagotavljale neprekinjeno poslovanje.

Ena najpomembnejših faz je projektiranje informacijskega sistema. S projektiranjem razumemo vse dejavnosti, ki jih je treba izpeljati, da bi omogočili fizično izvedbo informacijskega sistema na računalniku. Že pri projektiranju informacijskega sistema moramo identificirati ključne dejavnike prenove poslovnih procesov in opredeliti vidike upravljanja s spremembami in posledično identifikacijo in obvladovanje operativnih tveganj.

Ko je nova oz. prenovljena programska rešitev v produkciji, je potrebno zagotoviti njeno neprekinjeno poslovanje.

Na konkurenčnem trgu bodo preživele le tiste banke, ki bodo zagotovile najbolj učinkovito in sistematično obvladovanje tveganj, kar pa bodo dosegle le, če bodo uspele doseči celovito obvladovanje sprememb. To pomembno področje, ki vpliva na ugled domačih bank in zadovoljstvo njenih komitentov, je potrebno obravnavati z vidika celovitosti in upoštevati vse vidike, ki vplivajo na uspešno upravljanje, saj je od uspešnosti slovenskega bančništva odvisna uspešnost celotne družbe.

3.2 Banka kot organizacija

Poleg storitev, ki jih banke ponujajo svojim komitentom in predstavljajo ključne oz. temeljne poslovne procese (kreditiranje, sprejemanje depozitov, zakladništvo), se v banki izvajajo še podporni procesi (npr. oddelki plačilni promet, informacijska tehnologija, reklamacije, podpora uporabnikom), ki so nujni za zagotavljanje ustrezne podpore temeljnim procesom in upravljalski poslovni procesi, katerih izvajanje se nanaša na načrtovanje in nadziranje temeljnih in podpornih procesov. Vodstvo banke mora poskrbeti za ustrezno informacijsko podporo vsem navedenim poslovnim procesom. Integracija procesov, ki daje nova znanja na organizacijskem nivoju za drugačno delovanje (Myers, Hulks & Wiggins, 2012).

Pri tem je pomembno, da ima banka poslovni sistem podprt z ustrezno sodobno informacijsko tehnologijo, ki je prilagodljiva, zagotavlja varnost poslovanja in je

zanesljiva. Prilagodljivost in možnost razširitve sistema je pomembna zaradi nenehnih sprememb v banki in okolju ter razvoja novih bančnih produktov, ki jih je potrebno implementirati. Banka je izpostavljena mnogim spremembam, ki jih lahko delimo glede na to, ali so »sprožene« iz zunanjega okolja ali s strani banke same, na pomembne in manj pomembne, majhne in velike, nujne in manj nujne, ali vplivajo na poslovanje celotne banke ali samo na posamezne oddelke.

Zahteve po spremembah prejema banka od nadzornika bančnega poslovanja Banke Slovenije, upravljalca plačilnih sistemov Bankarta, Združenja bank Slovenije, Zakonodajalca (Ministrstva in drugi državni organi) in zunanjih partnerjev. Določena obvestila o spremembah tehnoloških komponent, ki so široko uporabljana, mora banka poiskati sama, npr. kompatibilnost podpisnih komponent s posameznimi brskalniki ali pojav novih vrst digitalnih potrdil s strani izdajateljev digitalnih potrdil, ki jih uporabljajo komitenti banke.

Področje oz. funkcija opravljanja plačilnega prometa je prav tako kot druge funkcije v bankah neločljivo povezana z informacijsko podporo. Standardi procesiranja plačil so postavljeni tako, da je vloga posameznika pri procesiranju minimalna.

V času hitrih sprememb v poslovanju bank ter pritiskov konkurence, trga in regulative se banke in finančne institucije soočajo z izzivom uvajanja novih storitev, novih poslovnih procesov in novih tehnologij, s katerimi lahko izboljšujejo svojo konkurenčnost na trgu in zadostijo zahtevam regulatorjev (zakonodaja, zahteve centralne banke).

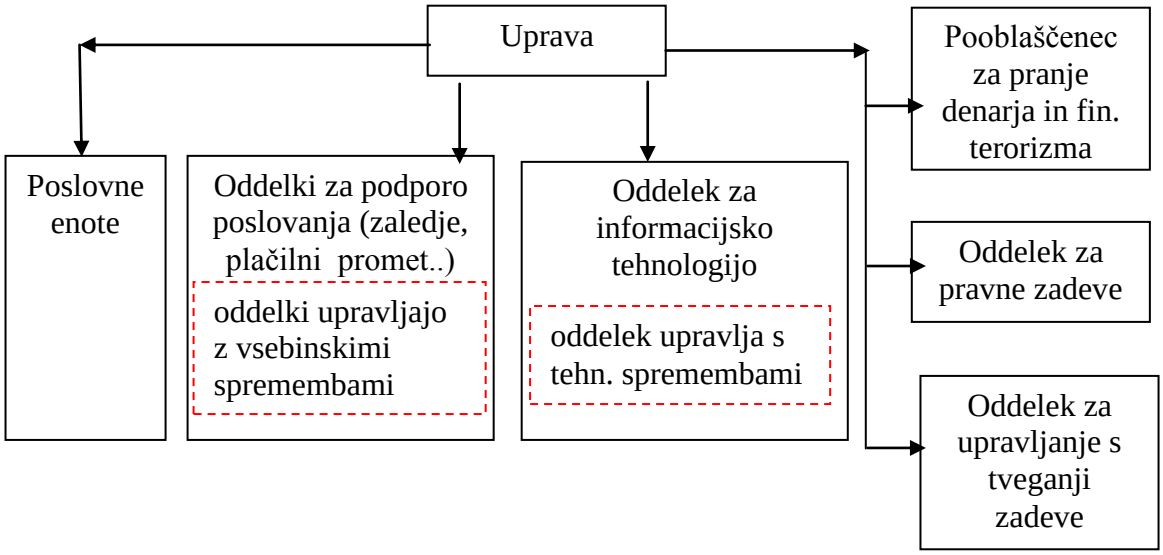
Organizacijska struktura v bankah je običajno prilagojena bančnim produktom in zaposlenim v posameznem oddelku, kar lahko pri načrtovanju procesov in lastnikov procesov povzroči nemalo težav. Pomembno vprašanje, ki se pojavi, je, kdo je lastnik poslovnega procesa plačilni promet, saj se njegove aktivnosti pojavljajo praktično v vseh bančnih produktih in v vseh oddelkih.

Zgoraj naštete vrste sprememb na področju plačilnega prometa se v bankah preko uprave distribuirajo lastnikom poslovnih procesov. Spremembe lahko prejmejo s strani zunanjega okolja formalni lastniki poslovnih procesov. Ker obstaja za poslovni proces plačilnega prometa več skrbnikov oz. lastnikov, ki se nahajajo po posameznih oddelkih, preko katerih se izvaja proces, ni jasna razmejitev odgovornosti in pooblastil za učinkovito upravljanje spremembe.

Glede na to, da so poslovni procesi tehnološko podprti, je ponavadi potrebna sprememba tehnoloških komponent (baza podatkov, programi). Na sliki 6 je prikazana trenutna umestitev področja upravljanja sprememb v banki X.

Upravljanje sprememb ni organizirano centralno, ampak parcialno po oddelkih, kar povzroča nejasnosti pri delegiranju spremembe lastniku poslovnega procesa (komu vse se delegira spremembo) in zadolžitev za njeno implementacijo. Spremembe v banki X niso celovito obravnavane in ni dokumentov, ki bi definirali, na katere aktivnosti in tehnološke komponente sprememba vpliva. Konkurenčna prednost v obliki obvladovanja sprememb in obvladovanja tveganj, banki X zagotavlja več komitentov, večji dohodek in dobiček.

Slika 6: Organiziranost banke



Vir: Banka X, Organizacijska shema banke, 2010.

Konkurenčno prednost banke zagotovijo z izboljšanjem zagotavljanja kvalitete storitev (dosegljivost, razpoložljivost, hitrost, varnost), nižjimi cenami produktov, obsegom ponudbe storitev, krepitvijo zaupanja v banke. Banke lahko povečajo učinkovitost poslovanja s prihranki na področju poslovanja, večjim pregledom nad poslovanjem, hitrejšim in varnim poslovanjem, z razširjeno ponudbo storitev in ponudbo neomejenega časovnega in krajevnega dostopa do storitev.

Tehnološka podpora mora v bankah zadostiti nekaterim osnovnim pogojem, ki zagotavljajo učinkovito upravljanje sprememb in nizko stopnjo tveganja v delovanju podpore. Nanašajo se na enostavnost uporabe, povezljivost modulov (produktov), sistem mora delovati na različnih platformah, zagotavljati mora parametrizacijo vseh pomembnih spremenljivk, zagotavljati mora povečevanje obsega uporabnikov, modulov ter redno in preprosto nadgradnjo sistema.

Za nemoteno delovanje informacijskega sistema pa je potrebno, da banke s strani vzdrževalca posameznih tehnoloških komponent, ki jih uporablja (programi, strojna in

komunikacijska oprema, baza podatkov), zagotovijo še ostale storitve, ki zagotavljajo nemoteno delovanje sistema in s tem tudi poslovanja.

Med te storitve štejemo izobraževanje in usposabljanja uporabnikov, svetovanje pri načrtovanju sprememb in integracijo le-teh v obstoječe module, oblikovanje in vzdrževanje spletnih strani, svetovanje in izvajanje prenosa podatkov iz produkcijskih baz podatkov v testne ali arhivske, izobraževanje na področju spletnih bank in dokumentiranje programskih rešitev kot zelo pomembna storitev, ki zmanjšuje operativna tveganja.

Tehnološka podpora sama po sebi ne zagotavlja učinkovitega in varnega poslovanja banke. Pomembni so zaposleni v tako v oddelkih kot na oddaljenih poslovnih enotah, ki s svojim strokovnim znanjem uporabljajo informacijski sistem in zaposleni v informacijski podpori, ki zagotavljajo učinkovito tehnološko podporo. Visoka stopnja informatizacije mora zagotoviti kvalitetne informacije za komitente, za vodstvo, za zaposlene, za lastnike, za nadzornike, pri tem pa čimbolj omejiti (onemogočiti) človeške napake in napake pri delovanju informacijskega sistema, s tem pa zmanjšati tveganja na čim manjšo mero. Iz navedenega lahko povzamemo, da gre pri informacijskem sistemu za izredno širok nabor poslovnih procesov oz. bančnih storitev, ki zahtevajo kompleksno obravnavo na področju upravljanja, usklajevanja, nadzorovanja in obvladovanja sprememb in tveganj.

3.3 Tehnološke komponente

3.3.1 Opredelitev tehnoloških komponent

Tehnološke komponente, ki jih upravlja oddelek informacijske tehnologije, imajo pri široki uporabi naprednih tehnologij velik vpliv na delovanje informacijskega sistema. Težava je v tem, da se pojavljajo vedno nove in boljše tehnološke rešitve (poslovanje v oblaku, e-bančništvo na mobilnih napravah – telefoni, tablice), ki zahtevajo nove varnostne mehanizme pri prenosu podatkov in dostopov do spletnih bank ter »nosijo« v sebi nova potencialna tveganja. Tehnološke komponente v bankah sestavljajo programska, strojna in komunikacijska oprema ter baze podatkov.

Vloga informacijske tehnologije oz. tehnološkega okolja je seveda mnogo širša, saj obsega še izobraževanje in svetovanja zaposlenim, dobavo novih tehnoloških komponent, testiranja komponent, vsakodnevni monitoring delovanja sistema itd.

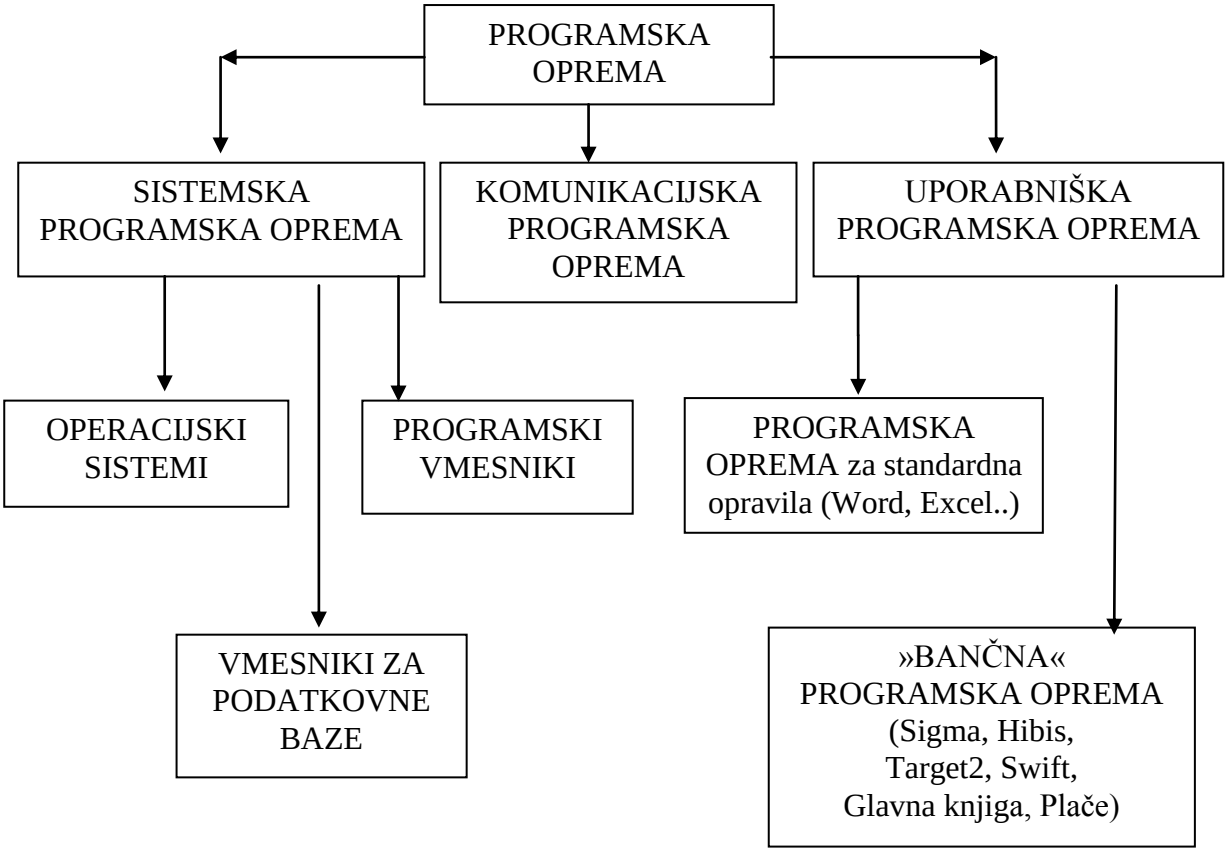
3.3.2 Programska oprema

Običajno programska oprema v bankah zajema najmanj: uporabniške programe, sistemske programe (operacijski sistem ter razni servisni programi) in orodja za izdelavo lastnih enostavnih programov za končne uporabnike kar je prikazano na sliki 7. Najpomembnejša je bančna programska oprema, ki jih banke uporabljajo pri podpori poslovnim procesom.

Ponavadi gre za en centralni program oz. aplikacijo, ki ga banka kupi na tržišču in ki skrbi za podporo kar največ bančnim produktom.

Poleg centralnega programa, ki je prilagojen za izvajanje bančnega poslovanja, pa banka uporablja še uporabniške programe, ki so namenjeni specifičnim zahtevam uporabnikov (kadrovski, računovodski) ter programe, ki omogočajo komuniciranje med zaposlenimi in navzven (programi za upravljanje s telefonskimi klici, programi za upravljanje s sistemskimi sporočili), splošno uporabne programe za izdelavo preglednic in poročil ter programe za podporo poročanja upravi in podporo spletnemu poslovanju.

Slika 7: Programska oprema v bankah



3.3.3 Strojna oprema

Strojna oprema v bančnem okolju zajema poleg standardnih komponent kot so osebni računalniki, strežniki, diskovne enote, tiskalniki, monitorji, optične enote, enote za arhiviranje podatkov, še druge »bančne« komponente (Banka X, 2011):

- bankomati, ki jih delimo na notranje, zunanje, mini-bankomate, več-funkcijske bankomate, bankomate, ki omogočajo tako imenovani zaprti denarni krog,
- POS terminali v lasti bank,

- bančni tiskalniki (tiskalniki za bančna okenca, večnamenski tiskalniki),
- informacijsko-transakcijski kioski,
- avtomati za štetje gotovine,
- naprave za preverjanje pristnosti in primernosti gotovine,
- e-kioski,
- informacijski prikazovalniki (veliki ekrani v banki, ki prikazujejo najpomembnejše informacije o ponudbi banke).

Raznolikost in obseg strojne opreme v bankah sta odvisna od velikosti banke in ponudbe različnih vrst storitev oz. produktov. V času novih tehnoloških komponent (tablice, pametni telefoni), preko katerih je možen dostop do bančnih produktov, se zahteva dodatne ukrepe na področju uvajanja sprememb in obvladovanja operativnega tveganja.

E-kiosk zagotavlja izvajanje določenih storitev brez prisotnosti bančnega delavca. Stranka lahko dviguje ali polaga gotovino, lahko izvrši plačilo iz osebnega transakcijskega računa na druge račune, lahko sklene varčevanje ali pa si izpiše izpisek iz računa. Na e-kiosku so dostopne tudi vse informacije o produktih, ki jih banka ponuja, njihovih posebnostih in cenah.

E-kiosk omogoča tudi oddajanje vlog za povišanje limita, za pridobitev kreditne kartice ali za izvajanje plačil preko trajnega naloga. Storitve, ki jih ponuja e-kiosk so raznovrstne, banka pa s tem omogoča 24-urno dostopnost do storitev banke. E-kiosk je primeren predvsem za redko poseljena in oddaljena območja kjer nima možnosti odprtja poslovnih enot.

Uporaba e-kioskov je v slovenskem prostoru razmeroma redka, banke se raje odločajo za postavitev bankomatov z razširjeno ponudbo kot je polog gotovine in predlaganje plačil v papirni obliki v izvršitev.

V storitvah e-kioskov so združene storitve bankomatov in informacijskih prikazovalnikov, ki jih banke uporabljajo za obveščanje strank o svoji ponudbi produktov, akcijah, deviznih tečajih, odpiralnih časih, pasivnih in aktivnih obrestnih merah.

3.3.4 Baza podatkov

Podatkovna baza je strukturirana zbirka medsebojno povezanih podatkov, ki je shranjena na računalniškem nosilcu podatkov. V podatkovnih bazah so shranjeni podatki o entitetah, ki so povezane s poslovanjem banke in povezavah med entitetami (Gradišar, 2005, str. 90)

V bazi podatkov so torej na urejen, organiziran in varen način shranjeni podatki o strankah, kakor tudi vsi dogodki, ki so povezani s poslovanjem strank, seveda pa tudi vsi drugi

podatki, ki so potrebni za nemoteno poslovanje banke (tarife, obrestne mere, obdelana in knjižena plačila).

V bazi se lahko nahajajo tudi nestrukturirani podatki, ki so predstavljeni kot naslovi spletnih strani, naslovi dokumentov, elektronska pošta in tudi podatki iz okolja. Z razvojem strojne opreme, predvsem kapacitete diskov, je omogočena širitev baze podatkov v giga in tera byte in s tem shranjevanje ogromnih količin podatkov.

Baza podatkov je torej namenjena hranjenju podatkov in zagotavljanju kvalitetnih podatkov in informacij vsem zaposlenim: operativnim uporabnikom, uporabnikom, ki uporabljajo podatke v analitične namene, in vodstvu, ki uporablja podatke za spremljanje poslovanja, preverjanje doseganja načrtov, za planiranje in odločanje.

3.3.5 Komunikacijska oprema

Komunikacijska oprema omogoča povezovanje s svojimi zaposlenimi, z uporabniki storitev, uporabniki storitev banke in z zunanjim svetom.

V komunikacijsko opremo štejemo komunikacijske strežnike, programe za šifriranje in prenos podatkov, strežniška digitalna potrdila, usmerjevalnike (routerji), podatkovne kanale in drugo opremo, ki omogoča vključitev banke v lokalna računalniška omrežja, t. j. povezava med računalniki na različnih lokacijah banke – LAN, vključitev v široka računalniška omrežja – WAN, ki vključujejo tudi posamezna krajevna omrežja, vključitev v zaprta medbančna omrežja, ki zagotavljajo šifrirano izmenjavo finančnih podatkov (omrežje B-Net, Swift) in vključitev v internetno omrežje (omrežje omrežij).

Razlika med LAN in WAN omrežjem je geografska oddaljenost računalnikov, uporaba javnih oz. privatnih telekomunikacijskih vodov (poti) in hitrost prenosov podatkov. Dostopi do informacijskega sistema so omogočeni preko lokalnega omrežja ali preko svetovnega omrežja, preko žičnih ali brezžičnih omrežij na varen način (digitalna potrdila, pametne kartice).

Kljub novim možnostim za dostop do produktov banke preko spleta, je za komitente zelo pomembno vprašanje, ali so se pripravljeni odreči osebnemu stiku z bančnikom (Glogovšek, 2008, str. 269). Osebno bančništvo je za komitente zelo pomembno, saj se na ta način vzdržuje zapupanje, ki ga imajo komitenti do banke, storitve se opravijo hitro in brez nepotrebnih dodatnih vprašanj in informacij.

3.4 Ljudje

Zaposleni v banki predstavljajo ključni dejavnik delovanja informacijskega sistema. Skrbijo za opravljanje poslovnih aktivnosti banke, za uvajanje, testiranje in vzdrževanje

tehnoloških komponent informacijskega sistema. Pomembno je tudi, da zaposleni spremljajo razvoj novih tehnologij ter da je zagotovljeno nenehno izobraževanje vseh zaposlenih. Zaposleni v oddelkih, še posebej pa zaposleni v poslovnih enotah morajo dobro poznati vse bančne produkte in njihove lastnosti (obrestne mere, pogoje), ki se prav tako hitro menjajo. Vodje oddelkov morajo imeti sposobnosti avtentičnega vodje (Dimovski, V., Penger, S., Peterlin, J., Uhan, M., Černe, M. & Marič M., 2013), ki so sposobni razvijanja odnosov z ljudmi in vzpodbujanja osebne rasti.

Zunanji poslovni partnerji, ki sodelujejo pri zagotavljaju delovanja tehnoloških kompnent bančnega sistema, so pomemben del samega informacijskega sistema banke, po drugi strani pa je banka zaradi njih izpostavljena dodatnim tveganjem na katere nima vpliva. Zelo pomembno je, da ima banka z zunanjimi partnerji vzpostavljene dobre komunikacijske kanale, osebne stike in vzpostavljene pogodbe, ki natančno opredeljujejo vse medsebojne obveznosti.

3.5 Poslovni procesi v banki

Poslovni proces je poenostavljeno v literaturi največkrat opredeljen kot pretvorba inputov v outpute z dodano vrednostjo. Poslovni proces sestavljajo strukturirane množice aktivnosti, ki predstavljajo zaključeno celoto za zagotavljanje določenega izhoda, rezultata, proizvoda ali storitve, ki ima določeno vrednost na trgu. Za poslovni proces je značilna transformacija vhodov v izhode. Proces se sestoji iz več postopkov, postopki pa iz več aktivnosti (Davenport, 1993, str. 5–7).

Poslovni proces v bankah zaradi poenostavitve, običajno kar enačimo s pojmom bančni produkt. Trditev ni korektna saj se določeni poslovni procesi izvajajo v več bančnih produktih.

Poslovni proces opredeljujemo kot sestavo logično povezanih izvajalskih in nadzornih postopkov in aktivnosti, katerih posledica oziroma izid je načrtovani izdelek ali storitev (Kovačič & Bosilj Vukšič, 2005, str. 29).

Pri poslovnih procesih digitalizacija vodi k preoblikovanju ročnih postopkov oz. ročno podprtih poslovnih procesov v avtomatizirane. Digitalizirane procese je precej lažje obvladovati, saj se lahko načrtujejo, izvajajo in izboljšujejo z uporabo informacijskih orodij, npr. sistemi za upravljanje poslovnih procesov BPMS.

V bančnem okolju se pojem poslovni proces prekriva s pojmom bančna storitev ali bančni produkt in se odvija skozi več oddelkov oz. sektorjev v banki. Ponudba bančnih storitev je odvisna od velikosti oz. specializiranosti posamezne banke, običajno pa obsega storitve, ki so zajete v treh sklopih (Banka X, 2010):

- Poslovanje s podjetji oz. pravnimi osebami:

- odpiranje in vodenje poslovnih računov,
- poslovne plačilne debetne in kreditne kartice,
- depozitni in krediti posli,
- investicijsko bančništvo,
- naložbe v vrednostne papirje,
- zavarovanje poslovanja,
- ostale storitve (factoring, leasing …),
- opravljanje plačilnega prometa,
    - za komitente (plačila preko Blagajne, preko spletnega bančništva, preko mobilnega bančništva),
    - za nekomitente (plačila samo preko Blagajne,

- Poslovanje s fizičnimi osebami:
    - odpiranje in vodenje osebnih računov,
    - osebne plačilne debetne in kreditne kartice,
    - depozitni in kreditni posli,
    - bančno zavarovalništvo,
    - osebno bančništvo in individualno upravljanje s premoženjem oz. portfeljem, naložbe v vrednostne papirje, trgovanje z vrednostnimi papirji, vzajemni in drugi investicijski skladi,
    - ostale storitve (sefi in depoji, menjalnica),
    - opravljanje plačilnega prometa,
        - za komitente (plačila preko Blagajne, preko spletnega bančništva, preko mobilnega bančništva, čeki),
        - za nekomitente (plačila samo preko Blagajne)
- Poslovanje z drugimi finančnimi institucijami:
    - medbančno kreditiranje,
        - poslovni odnos z drugimi bankami,
        - poslovni odnos s centralno banko
    - nakup in prodaja vrednostnih papirjev (obveznice, delnice).

Poslovni proces plačilnega prometa sestavljajo naslednji elementi (Gradišar, 2005, str. 118):

- dobavitelj: plačnik oz. nalogodajalec, iniciator plačilnega naloga,
- vhod: plačilni nalog, ki ga predloži plačnik preko različnih bančnih poti (elektronsko bančništvo, mobilno bančništvo, telefonsko bančništvo, papirni nalog, …),
- oskrbovalci: udeleženci poslovnega procesa so zaposleni na blagajni (“šalter“), ki plačilne naloge vnesejo in kontrolirajo, in zaposleni v oddelku za plačilni promet, ki naloge opremijo z dodatnimi podatki, jih avtorizirajo in pošljejo v plačilni sistem,
- izhod: plačilni nalog namenjen prejemniku plačila,
- odjemalec: prejemnik plačilnega naloga oz. plačila,

- preoblikovanje: gre za informacijsko preoblikovanje plačilnega naloga iz papirne v elektronsko obliko z dodanimi podatki za pravilno usmerjanje in pošiljanje plačilnega naloga v ustrezen plačilni sistem glede na podatke, ki jih plačilni nalog vsebuje oz. glede na dodatne podatke s katerimi oddelek plačilega prometa opremi plačilni nalog,
- zahteva: pričakovan "proizvod" za plačnika je izvršitev plačila čim hitreje in čim ceneje, za prejemnika pa odobritev njegovega transakcijskega računa na osnovi pogodbe ali sporazuma, iz katerega izhaja, da mora nalogodajalec izvršiti plačilo za dobavljen proizvod ali storitev, ki mu ga je/bo posredoval prejemnik plačila,
- povratna informacija: je informacija, ki jo prejme nalogodajalec v zvezi z izvršitvijo plačila, npr. izpiski opravljenega prometa na transakcijskem računu, iz katerih je razvidno, da je bil račun nalogodajalca bremenjen. V primeru neizvršitve plačila je nalogodajalec obveščen o razlogu zavrnitve plačila,
- meje poslovnega procesa: so naloge, aktivnosti in postopki, ki jih vsebuje poslovni proces. Na vhodu je omejen z nalogodajalcem, na izhodu pa s prejemnikom plačilnega naloga,
- lastnik poslovnega procesa: oseba, ki je pooblaščena in odgovorna za izvajanje in izboljšavo poslovnega procesa. Običajno je lastnik poslovnega procesa plačilni promet direktor oddelka za plačilni promet.

Elementi poslovnega procesa plačilni promet nastopajo v različnih bančnih produktih in funkcijah. Kot plačnik lahko nastopa banka, plačilo tako nastane v kreditnem modulu, modulu za podporo pravnim osebam, modulu za podporo fizičnim osebam, modulu plačilnega prometa, deviznem modulu, računovodskem modulu.

Komitent oz. nekomitent lahko plačilo posreduje banki v papirni obliki, v preteklosti je bila možnost predlaganja plačil banki na magnetnem oz. prenosnem mediju, ali preko spletnega bančništva. V zadnjih letih se je razširila možnost predlaganja plačil preko mobilne bančne aplikacije. Mobilna aplikacija nudi poleg plačevanja tudi ostale storitve, sklepanje varčevanj, vpogled v promet, vpogled v izvajanje direktnih obremenitev in trajnikov, plačevanje e-računov.

Če komitent plačilo predloži na blagajni banke in podatke plačila vnese blagajnik govorimo o papirnem nalogu. Značilnost univerzalnega plačinega naloga (v nadaljevanju UPN) je, da so podatki zapisani v skladu s SEPA standardi in v točno določenem formatu.

V kolikor podatke izpolni prejemnik plačila lahko na UPN obrazec zapiše tudi t.i. optično berljiva vrstica *(*angl. *Optical Character Recognition - OCR*) vrstico, ki je določena v skladu z ISO standardi. Omogoča avtomatski zajem podatkov, za plačila te vrste pa banke običajno zaračunajo nižje nadomestilo za opravljeno storitev.

Prejemnik plačila je lahko druga banka, proračunski uporabnik, pravna oseba ali fizična oseba, ki ima odprt osebni transakcijski račun pri drugi ali isti banki. Za plačila katerih

prejemnik je proračunski uporabnik, je na UPN obrazcu zahtevana referenca v točno določeni obliki. V kolikor plačnik reference ne navede v ustrezni obliki, se plačilo zavrne.

V kolikor imata plačnik in prejemnik odprt transakcijski račun v isti banki, govorimo o internem plačilu. Za izvršitev internega plačila banke običajno ne zaračunajo nadomestila za opravljeno storitev.

Izvršitev plačila se realizira v skladu s podatki navedenimi na plačilu, na podlagi katerih se posreduje ob določenem času v določen plačilni sistem. Kriteriji za usmeritev plačila so datum plačila (tekoči datum ali datum vnaprej), nujnost plačila (nujno ali nenujno plačilo), SEPA ali devizno plačilo, valuta (evro ali neevro valuta) in znesek.

Povratno informacijo o uspešnosti izvršitve plačila banka prejme od upravljalca plačilnega sistema in jo posreduje plačniku. Informacija je v obliki dnevnega ali mesečnega izpiska, uspešnost izvršitve plačila pa komitent vidi tudi v arhivu prometa. V primeru zavrnitve plačila s strani upravljalca ali prejemnika, je komitent obveščen z dopisom v katerem je naveden tudi razlog zavrnitve ali vračila.

Meje poslovnega procesa plačilni promet so v vsaki banki določene drugače. Meje so odvisne od organiziranosti banke in od razpoložljivih kadrovskih resursov s potrebnim znanjem plačilnega prometa in plačilnih sistemov. Običajno je zajem podatkov plačil omejen na blagajniški modul, ki poskrbi za vnos in avtorizacijo plačil.

Izven meja poslovnega procesa plačilni promet je tudi modul spletnega bančništva, ki je v okviru bank umeščen v različne oddelke, zajema pa poleg storitev plačilnega prometa tudi druge storitve.

Podatki se iz vseh modulov posredujejo modulu plačilni promet, ki se nahaja v oddelku plačilni promet in ki poskrbi za izvršitev plačila v medbančnem okolju in poskrbi za distribucijo povratnih informacij drugim modulom.

Lastništvo poslovnega procesa plačilni promet je prav tako odvisno od organiziranosti banke in razpoložljivih kadrov. Priporočljivo je, da ima oseba, ki je lastnik poslovnega procesa pridobljeno licenco Banke Slovenije, ki dokazuje usposobljenost osebe za delo v plačilnem prometu in dobro pozna plačilne sisteme. Prav tako mora lastnik poslovnega procesa zelo dobro poznati druge module v banki, povezljivost modulov in samo delovanje procesiranja plačil v različnih modulih.

Ponavadi je v bankah lastnik poslovnega procesa plačilni promet direktor oddelka za plačilni promet, poslovni proces pa zajema samo procesiranje plačil, ki se izvaja v oddelku. Takšna organiziranost terja veliko usklajevanja z lastniki ostalih poslovnih procesov, ki imajo v svojih modulih možnost oddaje in prejema plačil.

Tukaj je potrebno zelo dobro sodelovanje zaposlenih iz različnih oddelkov, ki izvajajo aktivnosti v različnih modulih. Storitve plačilnega prometa morajo biti poenotene na nivoju banke in zagotavljati enake kontrole pri vnašanju podatkov v aplikacijo. Ker programsko opremo zagotavlja zunanji izvajalec, in njegovi zaposleni programirajo posamezne module, se zgodi, da programska oprema ni poenotena. Problem, ki se pojavlja je, kdo bo zunanjemu izvajalcu posredoval zahtevek za spremembo ali dopolnitev določenega atributa v plačilu.

Praksa v banki kaže, da vsak lastnik poslovnega procesa v banki ločeno oddaja zahtevke zunanjemu izvajalcu, tudi če gre za enake spremembe. To pomeni, da se mora praktično vsak lastnik poslovnega procesa ukvarjati s plačilnim prometom in spremembami, ki jih to področje prinaša. V kolikor lastniki poslovnih procesov niso usklajeni, pride do zamika pri testiranju in uvedbi spremembe v produkcijo, posledično enake zadeve v različnih modulih delujejo različno.

V izogib takšnim situacijam je potrebno v bankah sistematično in premišljeno določiti lastnike poslovnih procesov in njihove zadolžitve in jih v primeru kadrovskih menjav nemudoma tudi ažurirati. Oddelek upravljanja s spremembami bi bil namenjen poenotenju delovanja banke navzven in bi preprečil morebitna podvajanja posredovanih zahtevkov.

Menim, da bi moral biti lastnik poslovnega procesa plačilni promet odgovoren za celotni poslovni proces, ki ne bi bil omejen na oddelek plačilnega prometa. Meja poslovnega procesa je na vhodu pri vnosu plačila po katerikoli poti, na izhodu pa s kreiranjem izpiskov za komitente banke. S tem bi odgovornost za procesiranje plačil bila točno določena in ne bi prihajalo do konflikotov s smislu, za neizvršitev plačila je krivda pri tebi in ne pri meni.

4 PLAČILNI SISTEMI

4.1 Medbančni plačilni sistemi v Sloveniji

V Sloveniji plačilno infrastrukturo za procesiranje plačil predstavljajo plačilni sistemi SEPA, ki jih upravlja Bankart in plačilni sistem Target2, ki ga upravlja Banka Slovenije.

Upravljavec Bankart v okviru SIMP infrastrukture upravlja naslednje plačilne sisteme, ki so namenjeni procesiranju plačil v evro valuti (Bankart, 2011):

- Interna kreditna plačila,
- Eksterna kreditna plačila,
- Eksterne direktne bremenitve po osnovni shemi,
- Eksterne direktne bremenitve po medpodjetniški shemi,
- Interne direktne bremenitve po osnovni shemi,
- Interne direktne bremenitve po medpodjetniški shemi.

Sistem Target2 je namenjen procesiranju nujnih plačil in plačil velikih vrednosti za domači in čezmejni plačilni promet ter za procesiranje neto poravnav v evro valuti. Sistem Target2 je sistem, ki deluje na enotni skupni platformi sistema Target2 in vključuje veliko število bank v evro območju, banke s sedežem v R Sloveniji, ki so vključene v Target2 pa so pravno formalno pod nadzorom Banke Slovenije.

S svojim delovanjem je Target2 sistem pričel v novembru 2007 (Banka Slovenije, 2007).

Sistem SEPA IKP je namenjen izvrševanju medbančnih plačilnih nalogov malih vrednosti (plačila malih vrednosti v višini do vključno 50.000,00 EUR) med udeleženkami in med komitenti bank v domačem SEPA okolju. Plačilni sistem SEPA EKP pa je namenjen izvrševanju medbančnih plačilnih nalogov malih vrednosti (plačila malih vrednosti v višini do vključno 50.000,00 EUR) med udeleženkami samimi in med komitenti bank v čezmejnem SEPA okolju.

Preko sistema se izvršujejo tudi poravnave obveznosti iz naslova multilateralnih klirinških shem, za katere je Banka Slovenije poravnalni agent.

Pri upravljanju sistemov SEPA nastopa v vlogi klirinškega agenta (izvedba kliringa) podjetje Bankart d.o.o. in v vlogi poravnalnega agenta Banka Slovenije, ki izvrši poravnavo neto obveznosti in terjatev udeleženk preko njihovih računov odprtih pri njej.

Plačilni sistem kreditnih plačil SEPA je bil omogočen 28. januarja 2008, ko je bilo ponudnikom plačilnih storitev prvič omogočeno plačevanje čezmejnih plačil. S tem je projekt SEPA prešel v fazo prehoda vseh kreditnih plačil v SEPAokolje. Dne 4. marca 2009 je bil vzpostavljen plačilni sistem SEPA, namenjen izvrševanju malih kreditnih plačil SEPA med slovenskimi bankami (domača plačila). Procesiranje čezmejnih direktnih obremenitev SEPA je bilo omogočeno novembra 2010, procesiranje direktnih obremenitev znotraj države pa je bilo omogočeno v začetku 2011 (Bakart, 2013).

4.2 Značilnosti plačilnih sistemov

Plačilni sistemi predstavljajo enega pomembnejših elementov, ki so potrebni za delovanje gospodarstva. Denarnim sredstvom omogočajo njihovo vlogo menjalnega sredstva ter s svojim učinkovitim in zanesljivim delovanjem zmanjšujejo stroške in tveganja, povezana s poravnavo med udeleženci (realnih in finančnih) trgov (Evropska centralna banka, 2012, str. 90).

Plačilne sisteme v najširšem smislu torej predstavljajo institucije, pravila, postopki, instrumenti in tehnologija, ki omogočajo prenos denarnih sredstev za najširši krog uporabnikov v ožjem smislu pa gre za izmenjavo informacij o plačilih in prenos sredstev iz

naslova plačil med bankami kot izvajalci storitev plačilnega prometa, ki sta potrebna v primeru, ko plačnik in prejemnik nista komitenta iste banke (Banka Slovenije, 2007).

Plačilni sistemi so zakonsko urejni z Zakonom o bančništvu, Zakonom o Banki Slovenije in z Zakonom o plačilnih sistemih in storitvah, prenos in izmenjava podatkov v plačilnih sistemih upošteva tudi določila Zakona o elektronskem poslovanju in elektronskem podpisu.

Zakoni urejajo vlogo Banke Slovenije na področju plačilnih sistemov ter določajo njene pristojnosti in odgovornosti za upravljanje in urejanje delovanja le-teh. Poleg tega je potrebno upoštevati Direktive in Uredbe EU, ki so implementirane v slovensko zakonodajo.

Pomembnejša funkcija centralne banke nadzor in pregled nad delovanjem plačilnih sistemov (angl. *Payment Systems Oversight*), kar zagotavlja varnost in učinkovitost plačilnih sistemov v bankah.

Značilnosti SEPA plačilnih sistemov (Združenje bank Slovenije, 2008) so:

- plačila se procesirajo preko klirinških hiš,
- enotni standardi plačilnih sporočil v državah EU,
- popolna identifikacija nalogodajalca, banka nalogodajalka in banka, prejemnica razpolagata z vsemi podatki plačilnega naloga,
- XML enoten standard zapisa plačil,
- enotno plačevanje v EU,
- popolna avtomatika procesiranja plačilnih nalogov (STP):
    - SWIFT BIC,
    - IBAN nalogodajalca in prejemnika plačila,
    - oznaka stroškov SHA,
    - znesek do vključno 50.000,00 EUR,
    - valuta samo EUR,
- uporaba identifikacijskih podatkov plačnika in nalogodajalca v dogovoru med prejemnikom in nalogodajalcem,
- izvedba dveh ali več poravnalnih presekov na dan,
- cena elektronskega bančništva je izenačena za domača in čezmejna plačila.

Glede na to, da v Sloveniji ni obstajala klirinška hiša, je plačila malih vrednosti do uvedbe klirinške hiše v upravljanju Bankart, procesirala Banka Slovenije. Da bi se plačilni sistem prilagodili evropskim standardom, je bilo potrebno najprej vzpostaviti klirinško hišo, nato pa v sistem vključiti banke.

Na nacionalnem nivoju je bila sprejeta odločitev, da bo upravljavec klirinške hiše Bankart, v sistem pa se bodo vključile vse slovenske banke. Za procesiranje plačil je Bankart vzpostavil tehnološko infrastukturo imenovano SIMP, preko katere se procesirajo domača in čezmejna plačila malih vrednosti in domače in čezmejne direktne bremenitve.

SEPA interna kreditna plačila so plačila, kjer sta banka plačnika in banka prejemnika udeleženki sistema SEPA (Banka Slovenije, 2007). Po usklajevanju na nacionalnem nivoju in razpoložljivosti udeležencev za pripravo potrebne dokumentacije za dejanski zagon in implementacijo projekta je Bankart pripravil časovni načrt projekta migracije kreditnih plačil majhne vrednosti iz sistema Žiro kliring v sistem SEPA.

4.3 Pravni okvir uvedbe SEPA plačil

Začetek SEPA sega v leto 2002, ko so banke v okviru EBA objavile Belo knjigo, v kateri so objavile deklaracijo, v kateri opredeljujejo, da so plačila v evro območju domača plačila.

Iniciativo za vzpostavitev SEPA območja je podala Evropska komisija. Marca 2007 je Evropski parlament sprejel Direktivo o plačilnih storitvah (angl. *Payment Services Directive* - PSD), z namenom da poenoti in odstrani pravne ovire za plačila v Evropski uniji. Direktiva o plačilnih storitvah je dejansko omogočila nastanek enotnega območja plačil v evrih v EU.

Vstop Republike Slovenije v Evropsko unijo (1. 5. 2004) in tri leta kasneje v Evropsko monetarno unijo (l. 1. 2007) je prinesel tudi spremembe in začetek prilagajanja domačih plačilnih sistemov SEPA pravilom, prav tako je bilo potrebno prilagoditi načine in postopke obvladovanja vseh vrst tveganj (sistemska, likvidnostna, kreditna, obrestna, operativna) evropskim standardom.

Glede na to, da je bila prilagoditev na področju obvladovanja bančnih tveganj nujna, je bilo potrebno sprejeti evropske smernice za obvladovanje operativnih tveganj. Še posebej pomembna so operativna tveganja na področju informacijskih sistemov in na področju posameznih bančnih storitev oz. produktov (plačilni promet, kartično poslovanje, spletno bančništvo).

Na nacionalni ravni vodi in usmerja projekt SEPA Združenje bank Slovenije. Cilj SEPA je vzpostaviti domača in čezmejna kreditna plačila in plačila s kreditnimi karticami, elektronskimi bančnimi prenosi, direktnimi obremenitvami in drugimi plačilnimi sredstvi enostavno, poceni in varno.

Časovna razporeditev za implementacijo projekta SEPA (Združenje bank Slovenije, 2007) je bila načrtovana v časovnem obdobju od 2005 do 2010 in naprej in je potekala v treh stopnjah:

- prva stopnja, ki je vključevala projektiranje dveh novih shem za elektronske prenose in za kartice,
- druga stopnja, ki je vključevala implementacijo in poskusno delovanje za obe novi shemi,
- tretja stopnja, ki je vključevala prehod v novi shemi

V okviru projekta SEPA še vedno potekajo nadgradnje plačilnih shem (npr. uvajanje elektronskih mandatov oz. pooblastil v shemi SEPA direktne bremenitve, uvajanje dodatnih zaščitnih elementov v okviru kartičnih in gotovinskih shem)

Storitve plačilnega prometa, ki zagotavljajo nemoten prenos sredstev med komitenti bank v negotovinski obliki, se izvajajo preko SEPA infrastrukture za mala plačila (SIMP). Informacijsko podporo oz. tehnološko okolje (programsko opremo in upravljanje baze podatkov) zagotavlja zunanji izvajalec, oddelek informacijske tehnologije v banki pa skrbi za komunikacijo z zunanjim izvajalcem in redno posodabljanje informacijske podpore.

Banka je vključena v plačilni sistem za procesiranje domačih kreditnih plačil malih vrednosti, v plačilni sistem za procesiranje čezmejnih kreditnih plačil malih vrednosti, procesiranje domačih debetnih plačil in procesiranje čezmejnih debetnih plačil.

Za procesiranje plačil velikih vrednosti in nujnih plačil ter plačil za poravnavo neto obveznosti iz naslova SEPA plačilnih sistemov, je banka vključena v plačilni sistem Target2.

Devizna oz. mednarodna plačila v tuji valuti banka izvršuje preko kontokorentne banke.

V okviru banke deluje kot eden od vitalnih delov v t. i. »back office« poslih Sektor plačilnega prometa. Najpomembnejše naloge sektorja so zagotavljanje hitrega, varnega in zanesljivega izvajanja plačilnih storitev in opravljanje vseh aktivnosti, ki tako izvajanje plačilnih storitev omogočajo.

V letu 2009 se je v skladu z Direktivo EU v slovenskem bančnem okolju izvedel prehod izvrševanja plačil malih vrednosti iz plačilnega sistema Žiro kliring v plačilni sistem SEPA IKP. V nadaljevanju bom opisal in analiziral prehod, ki smo ga izvedli tudi v banki in s katerim smo zagotovili procesiranje domačih plačil malih vrednosti v skladu s SEPA standardi. V decembru 2015 je bila objavljena v uradnem listu EU Direktiva 2015/2366 o plačilnih storitvah na notranjem trgu t.i. PSD2. Direktiva razširja obseg plačilnih storitev in

uvaja napredne varnostne zahteve za spletna plačila. Države članice morajo implementirati zahteve PSD2 v svojo zakonodajo do 13. januarja 2018.

4.4 Modeli poravnave v plačilnih sistemih

Obstajata dva modela sistemov izvajanja medbančnih plačil. V prvem modelu se vsak plačilni nalog poravna takoj, ko pride v sistem, in sicer v celotnem (bruto) znesku – bruto poravnava v realnem času (Target2 sistem). Poravnalne sisteme ponavadi upravljajo centralne banke, pri katerih imajo poslovne banke odprte poravnalne račune (Banka Slovenije, 2007)

Plačilni nalog, ki ga v breme svojega računa pošlje prva banka, se obdela takoj in če so na njenem računu pri centralni banki zadostna sredstva, se njen račun bremeni in odobri račun druge banke (Banka Slovenije, 2007). Tak postopek velja za vsako plačilo posebej. V teh sistemih se poravnavajo plačila iz naslova monetarnih operacij, poravnava obveznosti in terjatev drugih podsistemov, prenos likvidnostnih sredstev (npr. medbančni krediti) in tudi nujna plačila strank.

Drugi model pa deluje po načelu pobota, kar pomeni, da se plačilni nalogi v breme računov udeleženk zbirajo določen čas, nato pa se npr. na dve uri, na podlagi posredovanih in prejetih nalogov za posamezno udeleženko izračunajo neto pozicije.

Pobot pomeni preoblikovanje obveznosti in terjatev, ki izvirajo iz medsebojnega plačevanja med udeleženkami v sistemu, v eno ali več neto terjatev ali obveznosti, ki jih mora udeleženka dobiti ali pa plačati. Multilateralna neto pozicija oziroma posamezne bilateralne pozicije med udeleženkami se nato ponavadi poravnajo s prenosom sredstev preko računov pri centralni banki. (Banka Slovenije, 2007).

Drugi model je namenjen poravnavi velikega obsega plačil majhnih vrednosti, in sicer gre za plačila za medsebojno plačevanje fizičnih oseb in podjetij in za plačila iz naslova plačevanja storitev z direktno obremenitvijo.

Glavna prednost neto poravnalnih sistemov je nižja zahtevana likvidnost, ki jo banke potrebujejo za poravnavo določene vrednosti plačilnih transakcij ker se s prenosom sredstev poravna samo neto razlika med odlivnimi in prilivnimi nalogi posamezne banke in banke postanejo neto upnice oz. neto dolžnice.

Neto poravnalni sistemi so učinkovitejši z vidika uporabljenih komunikacijskih in procesnih zmogljivosti, kar vpliva na nizko ceno transakcij preko njih. (Banka Slovenije, 2007).

V primeru, da neto dolžnica ne bi zmogla pokriti svoje obveznosti, bi se aktivirala poravnalna jamstvena shema, v katero sredstva prispevajo vse udeleženke glede na obseg prometa.

Naslednja delitev plačilnih sistemov je geografska. Domači medbančni plačilni sistemi omogočajo izmenjavo plačil in njihovo poravnavo med bankami kot izvajalci storitev plačilnega prometa znotraj države, pri čezmejnih plačilih pa gre za plačila, pri katerih izvajalec storitev plačilnega prometa upnika in dolžnika nista iz iste države, sta pa člana SEPA območja.Pri deviznih plačilih gre za plačila, katerih znesek ni v evro valuti oz. upnik in dolžnik nista iz držav SEPA območja (tretje države).

5 UVEDBA SPREMEMB POSLOVNEGA PROCESA IN VPLIV NA OPERATIVNA TVEGANJA V PLAČILNEM PROMETU

5.1 Obvladovanje sprememb

Upravljanje in obvladovanje sprememb v banki X je organizirano na nivoju posameznih oddelkov. V primeru velikih sprememb npr. vključitev v plačilne sisteme se po sklepu uprave formira projektna skupina, ki skrbi za izvedbo in uspešno dokončanje projekta. Za spremljanje projekta se uporabljajo preglednice, ki vsebujejo opis aktivnosti, potrebni resursi za izvedbo aktivnosti, rok dokončanja aktivnosti in nosilci, zadolženi za izvedbo aktivnosti. Upravljanje in ovbladovanje sprememb v banki X je bilo pomanjkljivo in nezadostno.

5.2 Obvladovanje tveganj

Banka X upravljanju in obvladovanju tveganj namenja pozornost v skladu s smernicami nadzornika bančnega poslovanja in izvaja vse potrebne aktivnosti za njihovo obvladovanje. Najpomembnejša identificirana tveganja v banki X so: likvidnostno, kreditno (posebej zaradi izpostavljenosti do posameznega komitenta), obrestno in operativno.

Banka X izvaja aktivnosti za razvoj in dograjevanje informacijske tehnologije ter integracijo informacijskega sistema. Prav tako po metodi najboljše prakse dograjuje kontrolne mehanizme, katerih izvajanje omogoča obdržati visoko stopnjo kakovosti informacijskih storitev. Varnostna politika se nadgrajuje tudi v skladu s standardom ISO17799:2005 ter ISO27001:2006 z namenom zagotavljanja večje zanesljivosti, sledljivosti in varnosti informacijskega sistema, ki je temelj učinkovitega izvajanja bančnih storitev.

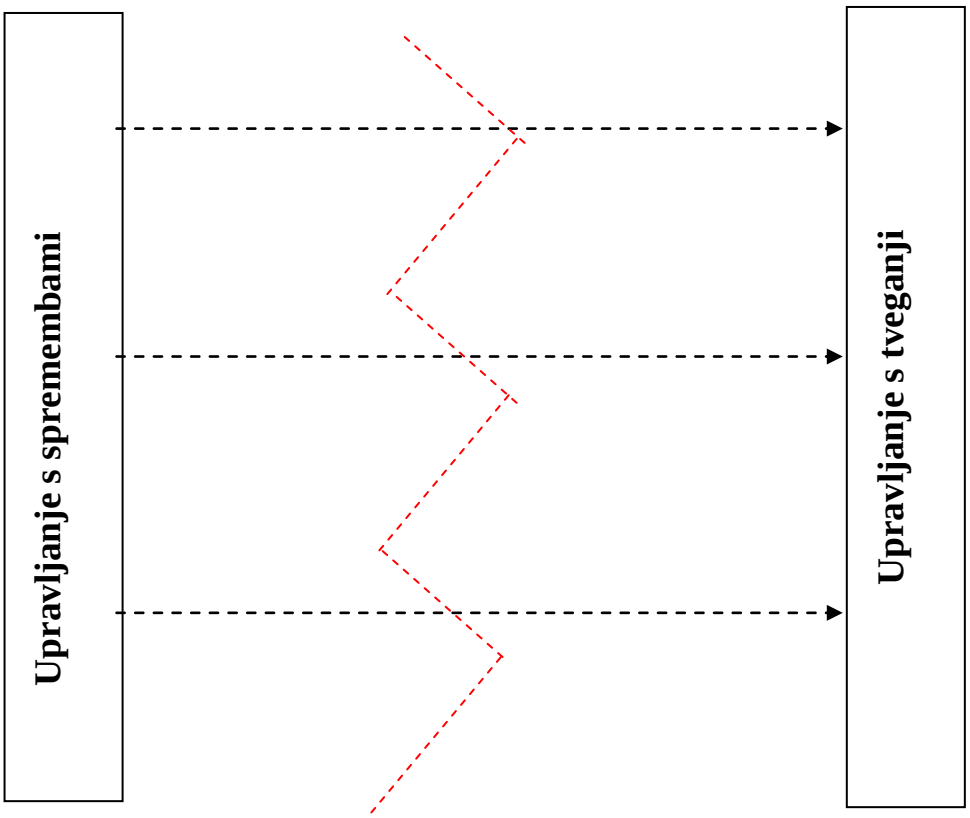
5.3 Operativno tveganje na področju plačilnega prometa

V oddelku Plačilni promet je bila posebna pozornost namenjena operativnim in finančnim tveganjem iz naslova poravnave plačilnih sistemov. Obvladovanje najpomembnejših in

identificiranih operativnih tveganj dosegamo predvsem z nenehnim delovanjem na aktivnostih, ki zagotavljajo neprekinjeno poslovanje oz. poslovanje v izrednih razmerah in na izobraževanju zaposlenih. Glede na to, da gre v plačilnih sistemih za visoko stopnjo avtomatiziranosti postopkov (angl. *Straight Through Processing - STP),* ki pomeni popolno avtomatizacijo procesiranja plačilnega naloga oz. podatkov plačilnega naloga od plačnika do prejemnika) in zahteva popolno podporo tehnološkega okolja. Aktivnosti so usmerjene predvsem v zagotavljanje tehnološke podpore za neprekinjeno poslovanje in v zvezi s tem tudi zagotavljanje rezervnih zmogljivosti, ki omogočajo neprekinjeno poslovanje. Rezervne zmogljivosti se nanašajo na vse resurse (kadrovske, tehnološke, prostorske in komunikacijske).

V plačilnem prometu smo v obstoječem plačilnem sistemu Žiro kliring obvladovali tveganja s predpisanimi postopki in notranjimi kontrolami. Na spremembo plačilnega sistema smo se odzvali z vzpostavijo projekta, ki je zajel vse bistvene spremembe na določenih aktivnostih, v projekt smo vključili tudi rok za dokončanje posamezne aktivnosti in njihove nosilce, ki so odgovorni za izvedbo posameznih aktivnosti. Poslovni proces plačilnega prometa kot eden najpomembnejših poslovnih procesov v banki X ima običajno vgrajeno visoko oz. srednje tveganje, ki ga lahko s sistematičnim pristopom pri vzpostavitvi in vzdrževanju obvladujemo tako, da naj bi se zagotavljalo nizka operativna tveganja.

Slika 8: Povezanost upravljanja sprememb z upravljanjem s tveganji



Upravljanje s spremembami in upravljanje operativnega tveganja sta v korelaciji predvsem pri identifikaciji in odpravljanju potencialnih nevarnostih in tveganjih, ki se pojavljajo ob spremembah (vsaka sprememba nosi v sebi tveganje).

Vzroki za potencialna tveganja se v večini primerov nahajajo v kadrovski podhranjenosti, nezadostni in pomanjkljivi dokumentaciji, nezadostnem izobraževanju in posledično pojavljanje napak pri izvedbi potrebnih aktivnostih zaposlenih. Tveganjem nedelovanja tehnoloških komponent se izognemo z rezervnimi zmogljivostmi in preklopom na rezervne lokacije tako na strani banke kot tudi na strani upravljavca plačilnih sistemov.

V banki X se upravljanje sprememb na področju plačilnega prometa izvaja neodvisno od upravljanja s tveganji. Upravljanje tveganj je omejeno na tehnološko podporo in delovanje tehnoloških komponent. Tveganja se identificira naknadno po vzpostavitvi spremembe. Na sliki 8 je prikazano trenutno stanje v banki X na področju povezanosti obeh sistemov upravljanja.

Nepovezanost področij povzroča težave pri poslovanju, ki nastanejo v primeru izrednih situacij, ob odkritju napak v programih, napak pri vnesenih podatkih in je težavo potrebno odpraviti takoj. Vsaka najmanjša sprememba, kot je npr. sprememba stroška nadomestila za določeno plačilno storitev, povzroči spremembe na različnih področjih bančnega poslovanja, spremembo je potrebno objaviti na spletnih straneh banke X, v pisnem in elektronskem dokumentu, ki predpisuje tarife in nadomestila za opravljanje plačilnih storitev.

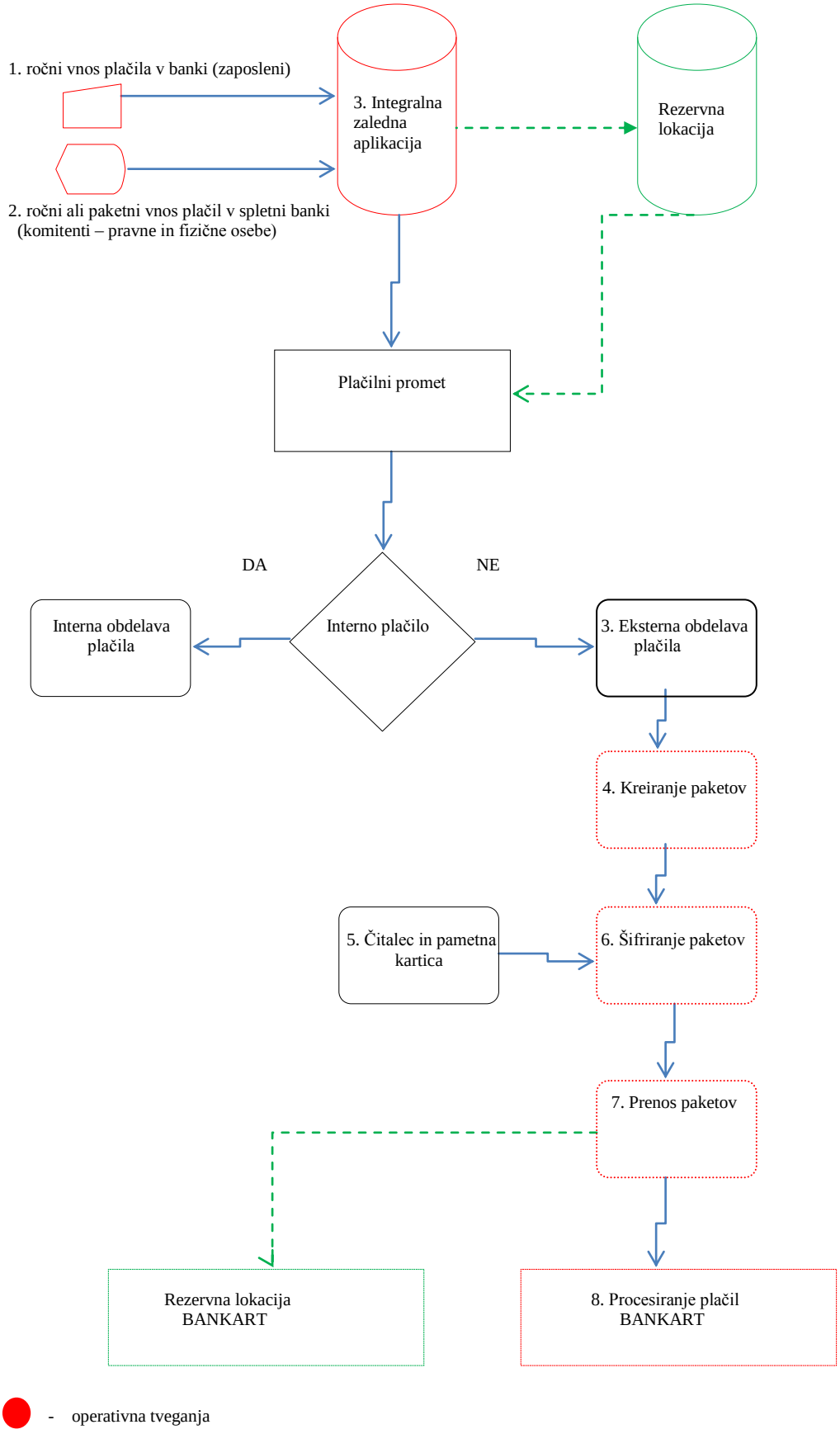
Spremembo je potrebno javiti oz. ažurirati na spletni strani Banke Slovenije (nadomestila plačilnih storitev za potrošnike), spremembo je potrebno ažurirati v centralni zaledni aplikaciji banke in javiti zunanjim izvajalcem, ki skrbijo za objave na zaslonih v poslovnih enotah.

Pri uvedbi spremembe je udeleženih najmanj pet ljudi iz različnih oddelkov, ki o spremembi niso istočasno obveščeni in če kdorkoli ne izvrši spremembe, lahko povzroči nastanek škodnega dogodka iz naslova operativnih tveganj.

Na sliki 9 so prikazana mesta nastanka operativnih tveganj v procesu izvrševanja medbančnega nenujnega plačila. Vidimo, da je potrebno vsako aktivnost obravnavati posebej in zagotoviti njeno neprekinjeno delovanje ter identificirati možne napake v delovanju.

Vzpostaviti je potrebno dokument, ki bo za vsako tehnološko komponentno opredelil ravnanje v primeru izrednega dogodka (odpoved, nedelovanje). Dokument mora biti ažurno dopolnjevan z novimi možnostmi delovanja v izrednih razmerah, za njegov razvoj in posodobitev pa mora biti določen točno določen nosilec.

Slika 9: Operativna tveganja pri procesiranju nenujnih plačil v banki X



- operativna tveganja

Plačilni nalogi (plačila) nastanejo na podlagi vnosa podatkov UPN obrazca v zaledno aplikacijo v banki X, lahko pa podatke vnese komitent sam preko spletnega bančništva. V obeh primerih se lahko pojavi nedelovanje sistema ali nepravilna uporaba programske opreme. V primeru nedelovanja sistema je potrebno preiti na rezervne postopke.

Ko je plačilo vnešeno in avtorizirano se vnese v centralno bazo podatkov in nadaljnjo obdelavo prevzame oddelek plačilnega prometa, ki plačilo obdela v skladu s plačilnimi instrukcijami. V kolikor so v plačilu prisotne napake se le-to zavrne, podatke o zavrnitvi se pošlje plačniku. V primeru, da so podatki plačila pravilni, se pošlje v plačilni sistem, ki se določi na podlagi podatkov plačila (nenujno, nujno, plačilo male vrednosti, plačilo velike vrednosti, valuta). V kolikor pride do odpovedi posameznih komponent se uporabijo rezervne zmogljivosti. Zaposleni morajo biti seznanjeni in usposobljeni za izvajanje vseh rezervnih postopkov.

Najpomembnejše je, da se vzpostavijo interna navodila z natančnim opisom delovnega postopka (workflow), opredeli možne situacije in predpiše ravnanje v primeru pojava neobičajnih in potencialno škodnih dogodkov.

5.4 Operativna tveganja v povezavi s prehodom v nov plačilni sistem

Projekt je bil načrtovan in voden s strani Banke Slovenije, pri usklajevanju in vzpostavitvi sistema pa sta bila udeležena ZBS in Bankart, ki sta bankam posredovala vse potrebne pravne podlage, informacije, scenarije testiranja in potrebne časovnice. Programsko podporo je izvajalo zunanje podjetje, ki je pripravljalo zaledno podporo istočasno za več slovenskih bank, ki so implementirale nov sistem.

Iz zgoraj navedenega izhaja, da so pomembna potencialna tveganja na strani upravljavca plačilnega sistema, ki bi lahko nastala pri prehodu na plačilni sistem SEPA (Bankart, 2009), in sicer zamuda pri pripravi internih vsebinskih scenarijev za testiranja, zamuda pri izdelavi novih načrtov za delovanje v izrednih razmerah, zamuda pri načrtovanju prehoda na nov plačilni sistem in zamuda pri izdelavi dokumentacije za upravljanja tveganja ob času prehoda.

5.5 Projekt prehoda v plačilni sistem SEPA

5.5.1 Vključitev v projekt SEPA

V skladu z nacionalnim planom prilagoditve domačega plačilnega sistema za procesiranje plačil malih vrednosti (Žiro kliring), plačilnim sistemom za procesiranje čezmejnih plačil, se je banka v letu 2008 vključila v projekt migracije domačega plačilnega sistema Žiro kliring v plačilni sistem SEPA, ki je bil načrtovan na nacionalnem nivoju že leta 2007, implementiran pa v marcu 2009.

Banka X se je v skladu z nacionalnim programom SEPA, ki ga je pripravilo ZBS, v januarju 2008 vključila v čezmejni plačilni sistem SEPA, ki je bil kot prvi enotni plačilni sistem uveden na področju SEPA območja in je vseboval enotna pravila in standarde za procesiranje plačil malih vrednosti za vse vključene udeležence.

Metodo mehkega prehoda uvedbe postopnih sprememb smo izbrali zaradi razširjenosti v slovenskem bančnem prostoru in zaradi internega akta, ki predpisuje, da se spremembe, ki bistveno vplivajo na potek poslovnih procesov, uvajajo v obliki projekta, ki ga izvaja projektna skupina.

Metoda je bila izbrana tudi zaradi narave poslovnega procesa, ki zahteva vključevanje kadrovskih virov iz različnih organizacijskih enot. Projekt je vodil direktor oddelka za plačilni promet, člani projektne skupine so bili direktor oddelka informacijske tehnologije in direktor oddelka podpore za pravne osebe.

5.5.2 Vzpostavitev projekta

V banki X je bil za namen vzpostavitve nove rešitve vzpostavljen projekt imenovan Migracija SEPA internih kreditnih plačil. Za izvedbo projekta je bila imenovana projektna skupina, katere naloga je bila priprava in usklajevanje vseh aktivnosti, ki so bile potrebne, da se izvede migracija na nov sistem. Delovna ali projektna skupina pomeni, da je na čelu skupine en človek, ki je zadolžen za posredovanje sprememb zunanjim partnerjev in drugim delom organizacije (Cameron & Green, 20102, str. 74). Projekt je odobrila uprava banke X.

Za načrtovanje, spremljanje in implementacijo migracije (prehoda) je bila izbrana metoda mehkega prehoda, ki se uporablja tudi za uvajanje sprememb na drugih področjih v banki X prav tako je ta metoda najbolj razširjena v slovenskem bančnem prostoru.

Akcijski načrt priprav je obsegal:

- vzpostavitev interne organizacije za uvedbo SEPA,
- prilagoditve na pravnem področju (v sodelovanju z Banko Slovenije in Bankartom),
- prilagoditve informacijske tehnologije (nosilec banka in zunanji izvajalec),
- komunikacijo z udeleženci v plačilnem prometu (v sodelovanju z ZBS in Bankartom).

Vzpostavitev interne organizacije je določila potrebne kadrovske in tehnološke vire, ki bodo omogočili realizacijo projekta. V projekt so bili vključeni oddelki za katere se je ocenilo, da bo projekt povzročil največ sprememb. Vodje teh oddelkov so bili zadolženi za implementacijo sprememb v njihovem poslovnem modulu. Težava je nastala ker je sprememba vključevala praktično vse oddelke, nekateri od njih pa niso bili vključeni oz. so bili vključeni naknadno.

Za prilagoditev na pravnem področju je bila zadolžena uprava, ki je vse pravne zahteve izpolnila v roku. Prav tako ni bilo težav pri vključevanju v nove plačilne sisteme SEPA in TARGET2.

Tehnološko prilagoditev programske in sistemske opreme je izvedel oddelek informacijske tehnologije, ki je bil zadolžen tudi za vzpostavitev ustreznih komunikacijskih poti, ki so omogočila vključitev v domača, čezmejna in svetovna omrežja za prenos plačilnih sporočil.

Za komunikacijo z udeleženci v plačilnem prometu je bil zadolžen oddelek za plačilni promet, ki je tudi koordiniral vse aktivnosti povezane z načrtovanjem, organizacijo, izvedbo, testiranjem in prehodom novega plačilnega sistema v produkcijsko delovanje. Komunikacija z udeleženci je obsegala izmenjavo elektronskih sporočil z zunanjim izvajalcem, izdelavo predlogov in pripomb pri izdelavi programske opreme, testiranje programske opreme, izdelava poročil na podlagi testiranj, testiranje popravkov programske opreme in vključitev programske opreme v produkcijsko delovanje.

Sledilo je preverjanje delovanja programske opreme v produkciji, nastavitve potrebnih programskih parametrov, določitev pravic uporabnikov in izdelava osnovne dokumentacije za ostale uporabnike. Dokumentacija, ki bi opisovala delovanje programske opreme skozi več oddelkov ni bila pripravljena.

Tveganja lahko nastanejo zaradi neustreznih in nepravočasnih internih in integralnih testiranj, zaradi napak pri programski opremi, napak pri izvajanju novih avtomatiziranih in ročnih postopkih za procesiranje plačilnih sporočil in napačnih nastavitev parametrov za izvajanje poslovnega procesa (dnevni maksimalni znesek oddanih plačil v plačilni sistem, poti za oddajanje in sprejemanje datotek, čas oddaje plačil).

Izvedba vseh potrebnih internih in eksternih testiranj je odvisna od razpoložljivih kadrov in obremenitve kadrov z drugimi aktivnostmi. Napačna nastavitev parametrov v zalednih aplikacijah je lahko posledica nekvalitetne dokumentacije, neznanja ali nepripravljenosti na izobraževanje.

Uvajanje sprememb s kombinacijo mehkih metod prenove poslovanja je vplivalo na zmanjševanje tveganja realizacije projekta predvsem v identifikaciji in odpravljanju potencialnih nevarnosti, ki se pojavljajo ob uvedbi sprememb (»vsaka sprememba nosi v sebi tveganje«).

Banka je na podlagi scenarijev prehoda na nov plačilni sistem SEPA, ki jih je pripravil upravljavec sistema, identificirala lastna tveganja, ki bi lahko nastala pri prehodu:

- zamuda pri načrtovanju prehoda na nov plačilni sistem,
- zamuda pri pripravi internih vsebinskih scenarijev za testiranja,

- neustrezna izvedba internih in integralnih testiranj,
- nepravočasna izvedba internih in integralnih testiranj,
- napake na novi programski opremi za interno podporo izvajanja plačilnega prometa,
- napake pri programski opremi za podporo šifriranja odlivnih in prilivnih plačilnih sporočil,
- napake pri vzpostavljanju komunikacijske povezave z novimi strežniki,
- napake pri izvajanju novih postopkov za procesiranje plačilnih sporočil,
- zamuda pri izdelavi novih načrtov za delovanje v izrednih razmerah,
- zamuda pri izdelavi upravljanja tveganja ob času prehoda,
- napačna nastavitev parametrov za izvajanje poslovnega procesa (določitev mejnega zneska plačila, ki se oddaja v sistem, določitev strežniških poti za oddajanje in sprejemanje datotek, čas oddaje plačil),
- organizacija izobraževanj za zaposlene v zvezi z novostmi, ki jih prinaša prehod na nov plačilni sistem.

Zamude pri pripravi dokumentacije nastajajo zaradi kadrovskih omejitev ali neznanja, redkeje zaradi nerazpoložljivih informacij o projektu, izvedba testiranj je odvisna od razpoložljivih kadrov in obremenitve kadrov z drugimi aktivnostmi, napačna nastavitev parametrov je lahko posledica neznanja ali nepripravljenosti na izobraževanje.

V projektu je bilo potrebno predvideti razpoložljive in dejansko potrebne kadrovske vire ter dejansko potreben čas za izvedbo posameznih aktivnosti in v skladu z razpoložljivimi kadri in časom načrtovati projekt. Kot se je kasneje izkazalo, so škodni dogodki iz naslova operativnih tveganj nastali ravno zaradi naštetih pomanjkljivosti pri izvedbi projekta.

Projekt je bil izveden v sodelovanju z Združenjem bank Slovenije, Banko Slovenije, Bankartom ter z zunanjim izvajalcem za izdelavo tehnološke podpore.

Prilagoditve na pravnem področju so vključevale nove pogodbe iz naslova prenosa poslov procesiranja plačil malih vrednosti od klirinškega agenta Banke Slovenije na klirinškega agenta Bankart, kot poravnalni agent pa je poravnavo izvajala Banka Slovenije (Bankart, 2007):

- pogodba o procesiranju internih kreditnih plačil v SIMP (med upravljavcem in bankami udeleženkami),
- pogodba o izvajanju poravnave internih kreditnih plačil (med upravljavcem in poravnalnim agentom),
- pogodba o posredovanju in procesiranju eksternih kreditnih plačil (upravljavcem, poravnalnim agentom in bankami udeleženkami).

Na pogodbene odnose s komitenti uvedba novega plačilnega sistema ni vplivala. Potrebno je bilo spremeniti oz. dopolniti določene interne akte in splošne pogoje vodenja računov, dodatno se je uvedlo poročanje Banki Slovenije.

Najobsežnejše so bile predvidene prilagoditve informacijske tehnologije. Potrebno je bilo identificirati vse potrebne prilagoditve informacijskega sistema (lastnih in najetih), izvesti potrebne spremembe, jih interno in integralno testirati in pripraviti načrt prehoda na nov plačilni sistem.

Komuniciranje z udeleženci v plačilnem prometu (pravne in fizične osebe) je potekalo v skladu z nacionalnim planom, ki ga je pripravilo ZBS in je predvideval obveščanje komitentov z obvestili na bančnih izpiskih, z brošurami in letaki na bančnih okencih in s povabili velikih podjetij na predstavitve novega plačilnega sistema.

Vzpostavitev novega plačilnega sistema je imela vpliv na vse ostale poslovne procese, kreditno poslovanje, računovodstvo, največji vpliv pa na poslovanje s pravnimi in fizičnimi osebami na področju izvajanja plačilnega prometa v banki X, tako na področju blagajniškega poslovanja kot tudi na področju poslovanja pravnih in fizičnih oseb preko spletnega bančništva.

Spletno bančništvo je bilo v domeni oddelka informacijske tehnologije, kar je zaradi kadrovskega manjka povzročilo dodatne obremenitve zaposlenih.

5.5.3 Opis ciljev projekta

Projektna skupina je za najpomembnejše cilje projekta določila (Banka X, 2008):

- pripravo in organizacijo aktivnosti, ki so potrebne za delovanje plačilnega sistema v novi SEPA shemi,
- koordinacijo in nadzor vseh aktivnosti potrebnih za implementacijo novega plačilnega sistema.

Izdelava analize vpliva uvedbe novega plačilnega sistema na povečanje/zmanjšanje operativnega tveganja, v banki X ni bila izvedena.

Naloga skupine je bila tudi opredelitev vseh področij v banki X, ki jih je sprememba plačilnega sistema zajela, prav tako je pripravila seznam vseh sprememb, ki so bile potrebne za delovanje novega sistema in izdelavo analize in ocene stopnje operativnih tveganj informacijskega sistema.

Evidentirane spremembe so se nanašale na module, ki so vključevali vnos podatkov plačil v novem SEPA formatu in jih je bilo potrebno spremeniti.

Med izvajanjem projekta je projektna skupina z vsemi potrebnimi informacijami oskrbovala zunanjega izvajalca, ki je skrbel za izdelavo sprememb programske in sistemske podpore.

BankaX je med vzpostavitvijo novega plačilnega sistema z obstoječimi kadri (trije zaposleni v plačilnem prometu) zagotavljala nemoteno delovanja starega plačilnega sistema in »mehak« prehod na delovanje novega plačilnega sistema.

V projekt ni bila vključena ocena vpliva implementiranih sprememb na oceno operativnega tveganja v plačilnem sistemu SEPA IKP. Razlog za nevključitev ocene sta bili kadrovska podhranjenost in nepovezanost oddelkov.

5.5.4 Težave pri izvedbi projekta

Težave pri izvedbi projekta so se pojavljale zaradi manjših zamud pri izdelavi funkcijskih specifikacij s strani upravljavca plačilnih sistemov in posledično tudi pri izdelavi sprememb programske opreme. Nekoliko zamude je bilo pri vzpostavitvi ustreznega testnega okolja, saj je bilo potrebno vzpostaviti novo testno bazo z novimi atributi na tabelah.

Največjo težavo pri izvedbi projekta so predstavljale kadrovske omejitve v banki X in razpoložljivost strokovnega osebja informacijske tehnologije, ki skrbi za nemoteno delovanje informacijskega sistema za vse poslovne enote, skrbi za nameščanje informacijskega okolja v novih poslovnih enotah in skrbi pomoč uporabnikom na področju spletnega bančništva.

Učinkovitost upravljanja s spremembami z vidika zadovoljstva zaposlenih ocenjujem kot dobro, zaposleni so seznanjeni s spremembami in aktivno vključeni v projekt izvedbe projekta. Z vidika komuniciranja med oddelki ocenjujem učinkovitost kot nezadostno, saj niso jasno določene pristojnosti in pooblastila vodje projekta, zaposleni v drugih oddelkih ne sodelujejo pri uvajanju sprememb na svojih oddelkih.

Kot pomanjkljivost se je pokazala tudi odločitev Uprave, da kadrovsko ne okrepi oddelka za plačilni promet, čeprav je bilo to nujno potrebno. S tem so bili direktor in zaposleni v oddelku plačilni promet izpostavljeni velikim delovnim obremenitvam in možnost pojava škodnega dogodka se je zelo povečala.

Kot se je izkazalo kasneje so se škodni dogodki dejansko pojavili, odgovornost za posledice pa je namesto Uprave, moral prevzeti direktor oddelka, ki škodnih dogodkov ni mogel preprečiti zaradi povečanega obsega dela na operativnih poslih. Škodni dogodek je povzročil spremembe internih aktov in navodilo zaposlenim, da pri svojem delu upoštevajo pisna navodila.

Z vidika povečevanja baze znanja v banki X pa le-tega na podlagi opravljenih razgovorov z zaposlenimi ocenjujem zelo dobro, saj je projekt prinesel nova znanja s področja upravljanja sprememb in strokovna znanja s področja plačilnih sistemov v EU in Sloveniji.

5.5.5 Realizacija projekta

Stroški projekta so bili realizirani v predvidenem okviru, vključeni so bili stroški nabave dodatne strojne in komunikacijske opreme ter stroški komunikacije s komitenti (nabava brošur). Dodatnih stroškov dela ni bilo, saj so zaposleni sodelovali v projektu v okviru svojih rednih delovnih nalog. Stroški niso bistveno odstopali od planiranih stroškov.

Projekt je bil praktično voden s strani upravljavca plačilnega sistema (Bankart), v banki X smo dejansko vzpostavili aktivnosti, ki so zagotavljale nemoten način vključevanja v nove plačilne sisteme (migracija obstoječih v nove plačilne sisteme) z jasno zastavljenim ciljem (prilagoditev plačilnega sistema SEPA shemi).

Rok za dokončanje projekta je bil dosežen, saj se je banka X med prvimi uspešno v celoti vključila v migriran plačilni sistem. Sodelovanje z zunanjimi deležniki, ki so projekt migracije vzpostavili in dejansko tudi vodili (Banka Slovenije, Združenje bank Slovenije, Bankart, zunanji izvajalec za podporo informacijski tehnologiji), je bilo zadovoljivo, tako pri sodelovanju v zvezi z izdelavo funkcijskih specifikacij, pri izmenjavi ostale dokumentacije kot na področju testiranja in same migracije.

Uspešne in intenzivne so bile komunikacija in pomoč (način, odzivnost, izobraževanja) ter izmenjava drugih potrebnih podatkov in informacij v okviru projekta. Fleksibilnost oz. sprotno prilagajanje projekta razpoložljivim resursom je bila sicer realizirana, saj smo imeli v banki X dovolj dolg rok za implementacijo in testiranje sistema, tako da zaradi manjših zamud pri izvedbi določenih aktivnosti projekt ni bil ogrožen.

Dejavniki, ki so vplivali na povečanje operativnih tveganj:

- premajhno število zaposlenih - trije zaposleni (direktor in dva sodelavca na področju plačilnih sistemov),
- prekomerna obremenitev zaposlenih v plačilnem prometu z rednimi rutinskimi postopki in uvajanjem dodatnih zadolžitev (vodenje gotovinskega poslovanja),
- izvedba dodatnih aktivnosti na področju uvajanja novih plačilnih sistemov (sočasen prehod iz domačega BPRČ v Target2 in domačega Žiro kliringa v SEPA plačilne sisteme),
- širitev banke X z novimi podružnicami in posledično opdpiranjem velikega števila transakcijskih računov ter posledično povečevanje obsega dela v plačilnem prometu,
- nepoznavanje informacijske tehnologije,
- nezadostno in pomanjkljivo izobraževanje,

- elektronska nepovezanost zaposlenih,
- problemi na pravnem področju (ni bilo pravnega oddelka)

V projektu so bila definirana operativna tveganja naknadno, torej po implementaciji novega plačilnega sistema. Tveganja smo v banki X naknadno dopolnili s tveganji, ki so se pokazala v teku projekta in za katera smo predvidevali, da se lahko zgodijo. Kot se je pokazalo kasneje, določenih potencialnih tveganj, ki so povzročila škodne dogodke, nismo predvideli.

Realizacijo sprememb v obliki projekta lahko ocenimo kot uspešno, saj je migracija prehoda bila izvedena, uporabe določenih dodatnih funkcionalnosti, ki jih nudi nova plačilna shema, pa so bile implementirane naknadno.

Projekt je bil uspešno izveden zaradi zunanjega »pritiska«, ključni faktorji za uspešno izvedbo projekta v banki X so bili zagotovljeni (razpoložljiva sredstva za izvedbo projekta, podpora uprave, razpoložljiva informacijska podpora, problem je bil v kadrovski podhranjenosti).

»Ozko grlo« pri razpoložljivosti kadrov smo želeli obvladovati s prerazporeditvami zaposlenih in sprostitvijo ključnih kadrov za dokončanje projekta, vendar je bila zaradi pomanjkanja časa zaradi drugih zadolžitev komunikacija slaba in nezadostna. Časovni vidik za dokončanje aktivnosti je vseboval dovolj rezerve, da se je projekt kljub določenim manjšim zamudam zaključil pravočasno.

Uporabniki in komitenti banke X so bili pravočasno seznanjeni z uvedbo novega plačilnega sistema, tako s strani same banke kot s strani Združenja bank slovenije. V banki X so bila plačila procesirana enako hitro, varno in cenovno ugodno kot pred uvedbo novega sistema. Strošek procesiranja čezmejnih plačil, ki se je prej izvrševal kot devizno plačilo in s temu primerno ceno, se je z uvedbo plačilnega sistema za čezmejna plačila bistveno znižal.

Projektna dokumentacija je bila izdelana pred začetkom izvedbe projekta, v teku projekta je bila v glavnem sproti ažurirana, zaradi kadrovskih omejitev pa se po zaključku projekta ni dokončno zaključila oz. ažurirala.

Za potrebe vodenja in upravljanja sprememb in operativnih tveganj smo izdelali tabelo, ki vsebuje kritične faktorje uspešnosti izvedbe projekta in ocenjene vrednosti doseganja uspešnosti realizacije projekta ter oceno vzpostavitve operativnih tveganj.

Pridobljeni podatki kažejo, da je za uspešno upravljanje sprememb potrebno organizirati oddelek, ki bo sprejemal in vodil uvajanje vseh sprememb, ki nastajajo v banki X, kar zaenkrat še v banki X ni realizirano, po posameznih oddelkih pa je potrebno zagotoviti

dovolj strokovno usposobljenih kadrov, ki bodo te spremembe sposobni realizirati in upravljati.

Banka X izvaja aktivnosti za razvoj in dograjevanje informacijske tehnologije ter integracijo informacijskega sistema. Prav tako po metodi najboljše prakse dograjuje kontrolne mehanizme, katerih izvajanje omogoča obdržati visoko stopnjo kakovosti informacijskih storitev. Varnostna politika se nadgrajuje tudi v skladu z ISO standardom ISO17799:2005 ter ISO27001:2006 z namenom zagotavljanja večje zanesljivosti, sledljivosti in varnosti informacijskega sistema, ki je temelj učinkovitega izvajanja bančnih storitev.

Razlika med merjenjem tveganj in ocenjevanjem tveganj je v velikosti statistične napake. Z merjenjem tveganj, ki jih izvedemo na podlagi večjega števila primerov oz. vzorca, dobimo bolj natančne rezultate, z ocenjevanjem tveganj na podlagi mehkih informacij in opisnih kazalcev pa dobimo približne rezultate.

V nalogi sem v analizi zajel področje plačilnega prometa in zaradi pomanjkanja "zgodovinskih" podatkov o škodnih dogodkih operativnega tveganja uporabil oceno operativnega tveganja, ki temelji na majhni količini škodnih dogodkov.

5.5.6 Ugotovitve in predlogi

Trenutno stanje kaže na odsotnost upravljanja sprememb na področjih identifikacije, ocenjevanja, spremljanja in obvladovanja operativnega tveganja, pomanjkanja nadzora in revizije na področju upravljanja sprememb, identifikacije potencialnih prevar znotraj in zunaj podjetja (npr. v tujini), neustreznega dokumentiranja in arhiviranja podatkov je delovanje novega plačilnega sistema izpostavljeno povečanemu operativnemu tveganju.

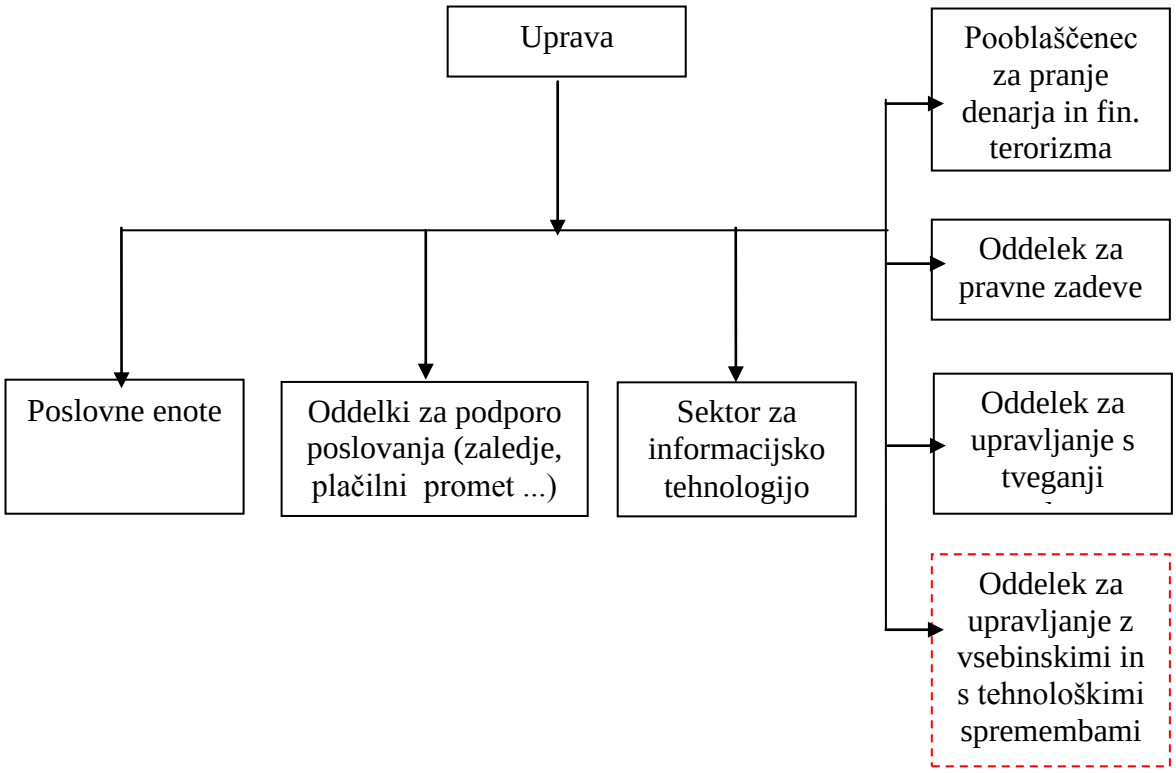
Po uvedbi projekta je zaradi nezadostnih kadrovskih resursov, pomanjkljivih internih navodil, ne-upravljanja s spremembami in pojavom "novega" dogodka, prišlo do naslednjih operativnih tveganj:

- prepis produkcijske baze podatkov v testno z vsemi atributi produkcijskega okolja,
- daljše nedelovanje spletne banke in pritožba stranke,
- vdora v spletno banko fizične osebe v tujini in izvršitev nakazila na transakcijski račun pravne osebe v Sloveniji. Stranka je dvignila sredstva z računa kljub temu, da ji niso pripadala

Bodoče stanje mora zagotavljati transparentno vodenje sprememb, zato predlagam vzpostavitev oddelka za upravljanje s spremembami, ki vplivajo na poslovanje banke (slika 10), kateri bo skrbel za identifikacijo sprememb, razvrstitev sprememb kot je razvidno iz priloge 2, delegiranje sprememb pooblaščenim osebam, poskrbel za koordinacijo in nadzor

izvedbe sprememb in ocenjeval učinkovitost realiziranih sprememb ter bo neposredno odgovoren upravi. Oddelek mora biti pri svojem delovanju visoko profesionalen in strokoven, zaposleni morajo poznati celotno bančno poslovanje.

Slika 10: Predlagana organiziranost banke X



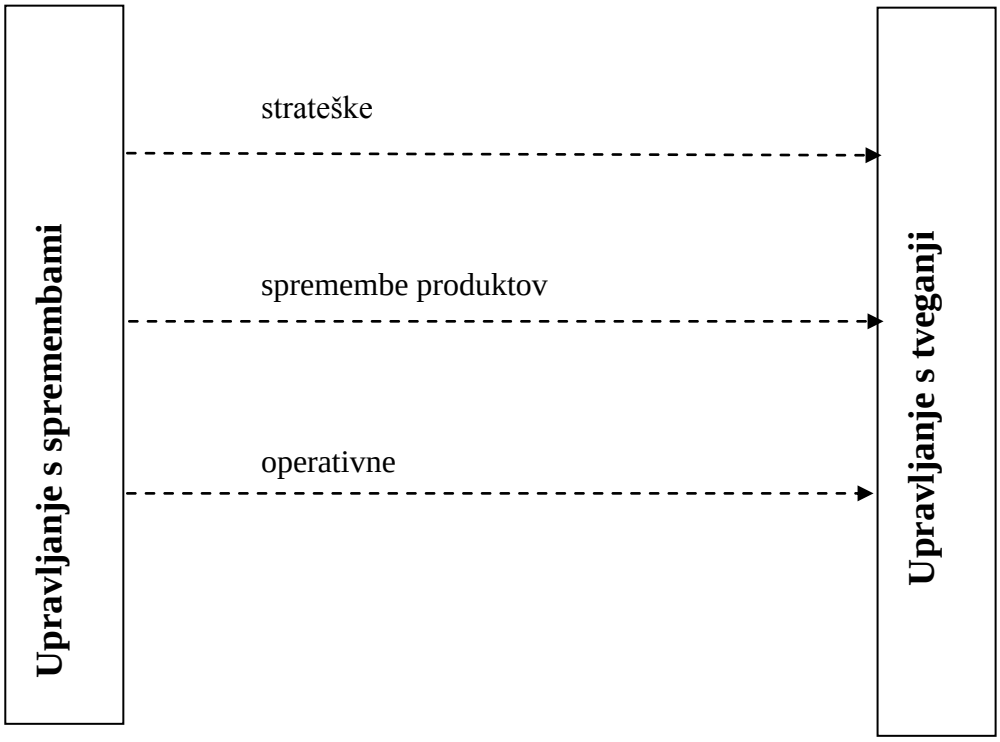
Predlagam, da se spremembe evidentira, kot je navedeno na Obrazcu za evidentiranje sprememb v prilogi 3.

Uprava bi morala zagotoviti poleg organizacijskih, tehnoloških in finančnih resursov tudi kadrovske, ki bi bili sposobni definirati in upravljati »svoje« poslovne procese od začetka do konca. Še enkrat se je pokazalo, da zaposleni niso samo eden od resursov, ki zagotavlja nemoteno delovanje banke, ampak je potrebno, da je zaposlenih dovolj, da imajo potrebna pooblastila, znanja in da delovne obremenitve niso tako velike, da bi lahko prihajalo do škodnih dogodkov bodisi zaradi utrujenosti bodisi zaradi nedefiniranih in nejasnih poslovnih pravil ter posledično zaradi »poenostavitve« delovnih postopkov s strani zaposlenih (zapisano je eno, v praksi se na podlagi ustnih navodil dogaja drugo).

Upravljanje operativnega tveganja je v banki X sicer urejeno, vendar ostaja na ravni poročanja operativnih dogodkov oddelku za upravljanje tveganj, ki poroča upravi, ni pa ustreznega proaktivnega reševanja morebitnih incidentov. Potencialna tveganja je potrebno prepoznati in identificirati, ne pa reševati in odpravljati takrat, ko nastanejo. Tveganja so v

različnih oddelkih različna, zato mora vsak vodja oz. direktor izdelati seznam potencialnih tveganj, ki so možna v oddelku.

Slika 11: Predlagana povezava področij upravljanja sprememb in upravljanja tveganj



Predlagam, da se vzpostavi povezava področja upravljanja s spremembami s področjem upravljanja s tveganji, kot je prikazano na sliki 11. Oddelek za obvladovanje tveganj mora oddelkom pojasniti možne škodne dogodke, oddelki pa določijo, kateri škodni dogodki so za njih najpomembnejši.

Pojav škodnih dogodkov in postopke za njihovo preprečitev in odpravo je potrebno vnesti v vsa interna navodila vseh oddelkov. Za implementacijo se zadolži vodje oz. direktorje oddelkov, z morebitnimi grožnjami in potencialnimi nevarnostmi pa se morajo seznaniti vsi zaposleni v oddelku.

Grožnje so v bančnem okolju vedno pogostejše. Globalizacija je omogočila, da so tudi majhne banke ogrožene in tarča napadov. Banke morajo zato nenehno izboljševati varnostno opremo, izobraževati zaposlene in se od kulture banke, ki je usmerjena k stranki, usmeriti v kulturo zagotavljanja varnosti tehnološke opreme in v kulturo, ki bo usmerjena v zaposlene.

Zaposleni, ki so »ogroženi« s strani komitentov in zunanjih groženj, hkrati pa nimajo podpore svojih nadrejenih, niso zadovoljni zaposleni. V pogojih delovanja pod pritiskom

so možnosti za napake večje, poveča se bolniška odsotnost, pomanjkanje kadra pa zopet vodi k večji možnosti operativnega tveganja.

Upravljanje s spremembami je potrebno voditi po načelu »od zgoraj navzdol«. Potencialna zahteva po spremembi se mora v banki X pojaviti na enem mestu. Dosedanja praksa kaže, da zunanji partnerji (npr. Združenje bank Slovenije ali Banka Slovenije) informacije, ki so pomembne za banko, pošiljajo upravi, vodjem ali celotnim oddelkom. Informacije glede novih zahtevanih funkcionalnostih produktov pošiljajo naslovnikom na podlagi informacij, ki so jih dobili od bank kar pomeni, da so si banke same ustvarile več virov informacij. Težava nastane ko zaposleni v banki X niso usklajeni glede realizacije in v primeru, da sprememba zahteva poseg v različne produkte oz. poslovne procese.

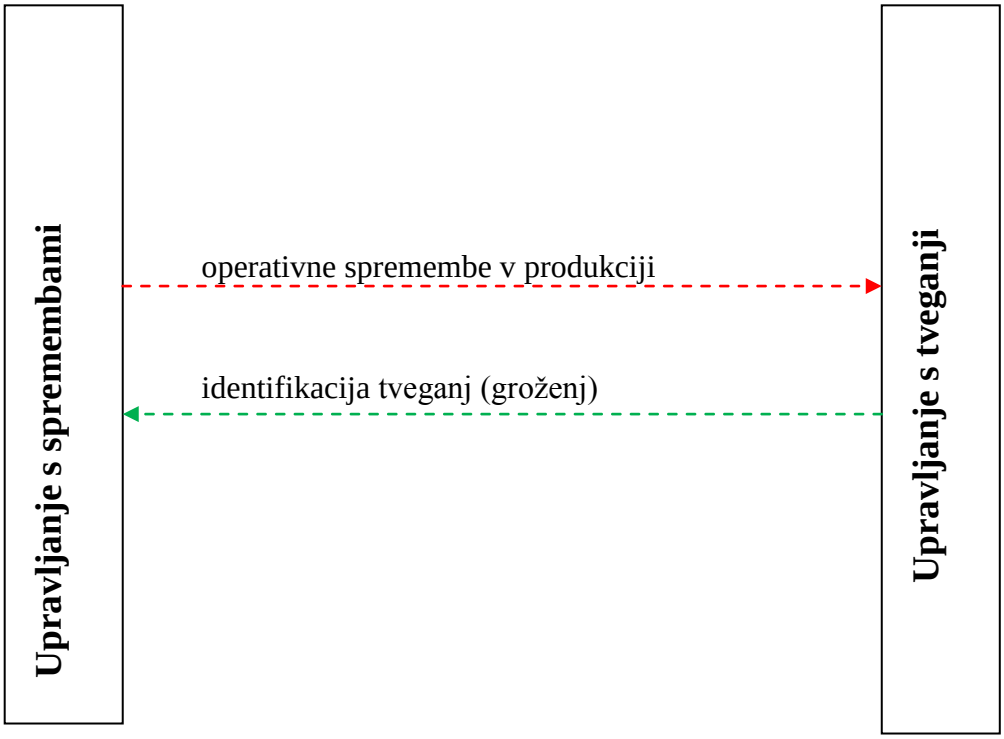
Uprava v banki X po prejemu zahteve po spremembi le-to posreduje vodji oddelka na katerega naj bi se ta sprememba nanašala in ga zadolži za realizacijo. Načrtnega spremljanja poteka realizacije prejetih sprememb ni. Druga težava v banki X je najem programske opreme za izvedbo bančnih poslov pri zunanjem izvajalcu. Banka X je odvisna od kadrovskih in tehnoloških resursov zunanjega izvajalca, kar po mojem mnenju ni sprejemljivo.

Določenih nujnih aktivnosti banka ne more prepustiti zunanjim izvajalcem. Primer je npr. realizacija nujnega popravka programske opreme, dogovor banke X z zunanjim izvajalcem pa predvideva minimalni čas za implementacijo spremembe npr. deset dni. Zunanji izvajalec bi moral dosledno skrbeti za ažurno dokumentacijo delujoče programske opreme in sledlljivost sprememb v programski opremi. V kolikor to ne bi bilo izvedljivo, bi to nalogo prevzel nov oddelek upravljanja s spremembami. Poudarek je na poznavanju produkcijske programske opreme, delovanju posameznih modulov in povezljivost med njimi. Vsi zaposleni bi morali poznati funkcionalnosti programske opreme, ki je v produkciji in jih uporabljajo pri svojem delu.

Oddelek za upravljanje s spremembami bi predlagal nove storitve in nova programska orodja za podporo odločanju. Uprava bi morala dobiti vpogled v analize podatkov in nova poročila o poslovanju na osnovi podatkovnega rudarjenja, ki bi ga omogočilo podatkovno skladišče. V oddelku bi poskrbeli tudi za izvajanje lastnih poizvedb v podatkovnih bazah z orodji, ki omogočajo dostop do podatkovnih baz in omogočajo izdelavo poročil.

V magistrskem delu je pokazano, da učinkovito upravljanje s spremembami pomembno vpliva na upravljanje operativnih tveganj. V banki X so se rezultati neučinkovitega upravljanja oz. neupravljanja s spremembami pokazali šele v delovanju sistema v produkciji, ko se zaradi določenih neobičajnih in izrednih dogodkov, ki niso bili identificirani in zapisani v internih navodilih kot potencialna tveganja, pojavili škodni dogodki.

Slika 12: Opravtivne spremembe in identifikacija tveganj v plačilnem prometu



Večina operativnih sprememb, ki se v oddelku plačilni promet dogajajo vsakodnevno, se izvaja rutinsko in ne terjajo posebne obravnave. V primeru, da oddelek plačilni promet prejme informacijo, ki ni običajna in ni evidentirana kot morebitna grožnja, bi moral zaposleni v oddelku takoj kontaktirati oddelek upravljanja s spremembami, le-ta pa bi moral pojav novega dogodka oceniti in ga posredovati oddelku upravljanju s tveganji.

Oddelek s tveganji bi dogodek preveril v evidenci oz. seznamu možnih škodnih dogodkov in sporočil povratno informacijo oddelku za upravljanje s spremembami kot je prikazano na sliki 12. Oddelek upravljanja s tveganji bi v primeru, da takšnega dogodka v banki X še ni bilo, dogodek dodal v seznam potencialnih škodnih dogodkov in o tem obvestil vse oddelke v banki X, prav tako tudi poslovne enote.

Na ta način bi se dopolnjeval seznam groženj banki X in bi se naslednjič venakem primeru takoj ustrezno odzvala. Vsi zaposleni bi imeli možnost pravilnega ravnanja v primeru izrednega dogodka. V bankah se potencialna tveganja in tveganja katerim je bila banka izpostavljena običajno obravnavajo interno, saj bi sicer informacije prišle v javnost.

Prevzemanje tveganj je neločljivo povezano z bančništvom, pomanjkljivo zavedanje in upravljanje s tveganji pa lahko vodi v izgubo in ogrozi varnost bančnih vlog. Zaradi pomembne vloge v nacionalni ekonomiji in zaupanja, ki ga imajo vlagatelji v banke, morajo te poslovati skrbno in varno ter vzdrževati primeren nivo kapitala in rezervacij za

zaščito pred morebitnimi tveganji, ki izhajajo iz poslovanja. Vse banke so v ta namen podvržene nadzoru s strani države za to pooblaščenih institucij.

SKLEP

V zadnjih letih je finančni sektor doživel mnogo sprememb. Današnji bančni sistem zaznamuje predvsem razvoj novih finančnih instrumentov, zagotavljanje neprekinjene razpoložljivosti, krepitev odnosov z najpomembnejšimi strankami in pa velika odvisnost od informacijske tehnologije. Seveda ne gre pozabiti še vse bolj zahtevne zakonodaje na področju bančnega poslovanja.

Banke so zadnja leta izvedle pomembne investicije v razvoj novih metodologij, procedur in kontrol z namenom boljšega identificiranja, merjenja in upravljanja tveganj. Banka mora imeti vzpostavljen takšen sistem upravljanja sprememb in tveganj, da bo pravočasno zaznaval spremembe v posamezni vrsti tveganja in temu ustrezno tudi prilagajal obseg kontrol in aktivnosti za njegovo zmanjševanje.

Interne politike in procedure morajo postati strateški element upravljanja s tveganjem, pri čemer je potrebno doseči, da se bodo dosledno izvajale in ne bodo same sebi namen (Branda, 2009). V bankah so tveganja prepoznana kot strateški element, interne politike pa se ne izvajajo v celoti in so pogosto same sebi namen.

Banke so že v letu 2004 v okviru Združenja bank Slovenije pripravile dokument Metodologija analize in upravljanja informacijskih tveganj v bankah. Ta dokument je postal neke vrste smernica za obvladovanje omenjenih tveganj v poslovnih bankah.

Ker banke niso bile eksplicitno in formalno prisiljene v izvajanje potrebnih aktivnosti za upravljanje tveganj, se je šele z uvajanjem načel Basel II pričelo z beleženje incidentov oz. škodnih dogodkov, kar lahko bankam služi kot izhodišče, na osnovi katerega bo možno podati oceno o kvaliteti upravljanja s tveganji in oceno o potrebnem kapitalu za pokrivanje operativnih tveganj.

Banka Slovenije je pripravila raziskavo QStudy (anketa, analiza bank) glede nameravanega izbora načinov obvladovanja OpRisk v slovenskih bankah. Standardni in napredni pristop zahtevata za pripravo ustrezne informacijske podpore več resursov (finančnih, kadrovskih in tehnoloških), zato je večina manjših slovenskih bank izbrala enostavni pristop.

Ker se operativnim in drugim tveganjem namenja vse več pozornosti in banke že dalj časa evidentirajo dogodke se predvideva, da bi slovenske banke postopno prešle na standardiziran pristop. Do leta 2007 je bilo upravljanje in obvladovanje tveganj prepuščeno intuitivnemu načinu zaznavanja in odpravljanja v bankah, po uveljavitvi Basla II pa se banke intenzivno ukvarjajo s sistematičnim upravljanjem tveganj.

Z uvedbo Basel III so se kapitalske zahteve še povečale, kar pa lahko vodi v zmanjševanje dobička ali povečanje izgube. Če bi se globalna kriza ponovila, lahko pričakujemo še Basel IV in naprej. Zato je pomembno, da banke resnično z zagotavljanjem potrebnih dodatnih resursev zmanjšajo možnost tveganja na najnižjo možno raven.

Plačilni sistemi so kompleksni in sestavljeni iz celega niza med seboj povezanih organizacijskih, kadrovskih in tehnoloških komponent. Obvladovanje tveganj, še posebej operativnih, zahteva celovit pristop na nivoju organizacije. V obvladovanje tveganj so vključeni zaposleni na front-office kot na back-office.

Zaposleni na blagajnah, v zaledju in v plačilnem prometu sodelujejo pri obvladovanju tveganj iz naslova izvajanja postopkov na svojem področju, zaposleni v informacijski tehnologiji pa pri obvladovanju tveganj iz naslova skrbi za nemoteno delovanje, delovanje v izrednih okoliščinah in nadgradnje tehnološke podpore.

Obvladovanje sprememb v banki X in v plačilnih sistemih se izvaja odvisno od hitrosti in obsega sprememb, ki so v plačilnih sistemih od uvedbe evra dalje, še posebej pa po prilagajanju plačilnih sistemov, kartičnem poslovanju, gotovinskem poslovanju, procesiranju novih plačilnih instrumentov evropskim SEPA shemam, zelo intenzivne, hitre in obsežne. Spremembe se dogajajo tako na plačilnih sistemih malih kot velikih vrednosti. Banka tem spremembam sledi in jih uvaja, ker so nujne in določene s strani zunanjih upravljavcev sistemov.

Permanentno se v banki X spremembe izvajajo na področju Target2 in na posodabljanju Swift komunikacijskega omrežja. Da bi te spremembe bile obvladljive in hkrati zagotavljale sprejemljivo raven tveganja, mora banka imeti na voljo dovolj kadrovskih resursov. Ti kadri morajo biti visoko usposobljeni, saj delo na plačilnih sistemih zahteva znanje tako bančnega kot informacijskega okolja.

Obvladovanje sprememb in obvladovanje tveganj sta neločljivo povezana, saj je operativna tveganja težko preprečevati, če se jih ne zavedamo že pri uvajanju sprememb. Vseh operativnih tveganj se seveda ne more preprečiti, lahko pa jih z načrtnim uvajanjem sprememb predvidimo in tako zmanjšamo njihov vpliv.

Banka X operativna tveganja na področju plačilnih sistemov obvladuje na dva načina. Oddelek za upravljanje s tveganji, v skladu z internimi akti (Pravilniki o spremljanju in poročanju operativnih tveganj) skrbi za redno nadgradnjo vseh aplikativnih informacijskih podpor in v skladu z razpoložljivimi resursi skrbi za izdelavo internih navodil za izvajanje postopkov, direktor oddelka plačilni promet pa izvede oceno ogroženosti plačilnih sistemov.

Zaradi preobsežnega operativnega obsega dela, ki ga izvajajo zaposleni, veliko pomembnih aktivnosti ni izvedenih kot npr.: izdelava natančnih internih navodil, izdelava internih aktov z natančnim popisom aktivnosti, ki se izvajajo v posameznem oddelku, niso določeni nosilci teh aktivnosti, ni medoddelčnih navodil.

Interna navodila sicer predpisujejo izvajanje postopkov in vgrajene kontrole, ki jih je potrebno redno izvajati, da se zagotovi pravilno in pravočasno izvajanje vseh potrebnih aktivnosti, kar je dovolj samo v primeru, da ni »neželenih« pojavov v obliki incidentov in škodnih dogodkov.

Podatki o številu in pogostosti incidentov v bankah, ki so posledica neučinkovitega upravljanja z operativnimi tveganji oz. slabega upravljanja s spremembami, ne obstajajo oz. niso dostopni za javnost. Javnost je ponavadi obveščena samo o najbolj odmevnih »negativnih« dogodkih v bankah.

V banki X si moramo odgovoriti na odprta vprašanja, kakšno je razmerje med centraliziran oddelek upravljanja s spremembami in upravljanjem z operativnim tveganjem na nivoju posameznih poslovnih področij in oddelkov in na nivoju banke, kdo je za kaj odgovoren, kdo so skrbniki poslovnih procesov in kje so prave meje poslovnih procesov.

Odgovornost za usklajevanje vseh poslovnih procesov in njihovo nemoteno delovanje v banki X nosi uprava banke. Uprava banke mora prepoznati pomembnost upravljanja s spremembami in pomembnost upravljanja z operativnimi tveganji.

Prav tako mora prepoznati kadrovske potrebe v podpornih oz. zalednih oddelkih, ki so močno odvisni od obsega produktov, obsega transakcij, obsega komitentov, obsega poslovnih enot. V času širjenja obsega poslovanja vodi nezmožnost prepoznavanja kadrovskih potreb, do povečevanje operativnih in tudi drugih tveganj.

Komitenti so lahko zadovoljni s storitvami, z nizkimi cenami plačilnih storitev, s troški odobritve kreditov, prijaznostjo bančnih uslužbencev, toda en sam potencialno škoden dogodek (nepravilna komunikacija, zaračunanje stroška o kateem komitent ni bil obveščen), lahko povzroči odhod komitenta k drugi banki, izgubo ugleda banke in posledično zmanjšanje prihodkov.

Vprašanje, ki se postavlja je, ali banka X takšen dogodek vidi kot možnost za izboljšanje, ali kot napako zaposlenega in napako tudi sancionira. Če bi dogodek obravnavali celovito in ne bi preverjali samo posledic ampak tudi vzroke, bi se na primerih lahko veliko naučili in izboljšali poslovanje. Evidentiranje dogodkov vsebuje tudi opis aktivnosti, ki jih bo banka izvedla, da se dogodek ne ponovi, ne vsebuje pa opisa dejanskega vzroka, ki je do dogodka privedel.

Nujno je, da banka vse spremembe skrbno načrtuje, določi realne roke za realizacijo, spremembam, ki jih je potrebno realizirati takoj in so nujne, pa je potrebno zagotoviti kadrovsko in tehnološko podporo.

Odprto vprašanje je tudi, kakšno naj bo sodelovanje med vzpostavljenim oddelkom za upravljanje sprememb v banki X, iniciativo na področju identifikacij operativnih tveganj v posameznih oddelkih in obstoječim oddelkom za upravljanje s tveganji ter ostalimi oddelki v banki X (interna revizija, oddelek za skladnost poslovanja, oddelek za pravne zadeve, oddelek za informacijsko tehnologijo).

Posebno vprašanje je upravljanje sprememb in operativnih tveganj v poslovnih enotah. Spremembe, ki nastajajo v okolju vplivajo tudi poslovanje poslovnih enot. Slabe gospodarske razmere v določeni regiji prinašajo povečana tveganja kraje premoženja banke, zato mora poslovna enota v sodelovanju z oddelkom za upravljanje s tveganji, izdelati svoj seznam groženj in morebitnih incidentov in določiti ravnanje zaposlenih v primeru incidenta.

V izobraževanje glede upravljanja in obvladovanja operativnih tveganj morajo biti vključeni vsi zaposleni. Ravnanje zaposlenih ob izrednih dogodkih mora biti vnaprej znano, določen mora biti sistem obveščanja in natančno definirane naloge vsakega zaposlenega. Izdelana morajo biti navodila, priporočila, na vidnem mestu v poslovalnici pa se morajo nahajati kontaktni podatki vseh odgovornih oseb.

Vse spremembe, ki se dogajajo v poslovni enoti in v regiji, morajo direktorji poslovnih enot nemudoma sporočiti oddelku za upravljanje sprememb. Oddelek oceni ali bo sprememba (npr. zaprtje več gospodarskih subjektov v regiji, povečevanje brezposelnosti v regiji) vplivala na poslovanje banke in z ugotovitvami seznani upravo. Uprava se nato odloči za ukrepe, ki bodo določeni poslovni enoti pomagali pri ohranitvi poslovnih rezultatov.

Z uvedbo novega oddelka za upravljanje s spremembami bi bilo potrebno določiti njene naloge in prenesti določene naloge iz drugih oddelkov. S tem bi se v drugih oddelkih sprostili resursi, ki bi jih lahko banka uporabila za izboljšanje poslovanja na tehnološkem področju, izboljšala bi se podpora poslovanju fizičnih in pravnih oseb, zaposlenim na blagajnah bi omogočili dodatna izobraževanja glede delovanja programskih modulov in rapoložljivih funkcionalnostih.

Oddelek za informacijsko tehnologijo bi lahko organiziral izobraževanja za napredno uporabo urejevalnikov besedil in preglednic. Zaposleni bi opravljali specializirane naloge.
Menim, da bi s specializacijo zaposlenih dosegli višjo raven poslovanja in boljše poslovne rezultate kot z univerzalnimi znanji.

Zaposleni v poslovnih enotah so usposobljeni za opravljanje vseh bančnih poslov, ki jih ni malo in vsak ima svoje posebnosti. Poudarek bi bilo potrebno dati izobraževanju na področju kreditnega poslovanja in področju izvajanja plačilnega prometa.

Tehnološki razvoj in splošna izobraženost uporabnikov bančnih storitev pred banke postavlja nove izzive. Ne samo, da so banke z dodatnimi kanali za dostop do podatkov, ki jih želijo komitenti, bolj ogrožene, skrbeti morajo za 24-urno razpoložljivost spletnih bank in v bodoče bodo morale zagotoviti tudi 24-urno tehnično pomoč uporabnikom.

Banke morajo zagotoviti dostopnost do bančnih storitev iz kateregakoli kraja. Predvsem za ljudi, ki veliko potujejo je to zelo pomembno, saj na ta način lahko poslujejo od koder koli.

Identifikacija stranke ne bo več možna samo z osebno prisotnostjo in s predložitvijo osebnega dokumenta, ampak se bo stranka identificirala z digitalnimi podatki (digitalno potrdilo, digitalni prstni odtis). Stranke nimajo časa čakati v vrsti, da se bodo lahko identificirale in odprle račun.

Banke bodo morale vzpostaviti povezave z drugimi razpoložljivimi registri v katerih se nahajajo podatki, ki so za bančno poslovanje s strankami potrebni. Predvsem gre za podatke o bonitetni oceni potencialnih strank, matičnih podatkih o strankah, premoženjskem stanju komitentov.

Povezljivost bank z zunanjimi deležniki je zelo pomembna, saj jim prinaša manj ročnega dela, ročnih postopkov in potencialne dobre komitente prepoznajo, še preden ti odprejo transakcijski račun. Brezpapirno poslovanje bankam praviloma prinese nižje stroške poslovanja in možnost avtomatiziranja postopkov. Proti takim spremembam so v bankah odpori, saj brezpapirno poslovanje prinaša prednosti (manj napak, manj tveganj, manj subjektivnih ocen določenega stanja) banki X, zaposlenim pa prinaša manj dela in dodatno izobraževanje.

Nove zakonodaje bodo v bodočnosti prinesle spremembe, ki se jih banke še niti ne zavedajo. Že danes lahko stranka izvrši plačilo v trafiki, v trgovini, na bencinskem servisu, na občini. Čeprav zaposleni na teh blagajnah nimajo znanja o plačilnih storitvah, le-te brez težav izvajajo. Zaposleni v bankah bodo morali graditi na zaupanju strank in jim ponuditi storitve, ki jih drugi udeleženci na trgu ne morejo.

Menim, da bi morale banke primarno skrbeti za kreditiranje gospodarskih subjektov in gospodinjstev in omogočiti privlačna varčevanja za vse starostne skupine. Pogoji pridobivanja sredstev morajo biti enostavni, hitri in učinkoviti. Banke morajo stopiti nasproti domačim gospodarskim subjektom, da bodo konkurenčni tujim na domačem trgu.

LITERATURA IN VIRI

1. Anko, S. (2010). Upravljanje projekta SEPA. *Bančni vestnik, 59*(9), 43-47.
2. Babič Kaligarič, K. (2012). *Učinki uvedbe SEPA kreditnih plačil in direktnih obremenitev na poslovne subjekte v Sloveniji* (magistrsko delo). Ljubljana: Ekonomska fakulteta.
3. Banka Slovenije. (2007). *Kaj je Basell II.* Najdeno 10. marca 2012 na spletnem naslovu http://www.bsi.si/html/basel2/02_kaj_je/Kaj_je_Basel_II.htm
4. Banka Slovenije. (2007). *Sepa v Sloveniji.* Najdeno 25. aprila 2014 na spletnem naslovu https://www.bsi.si/placilni-sistemi.asp?MapaId=1457
5. Banka Slovenije. (2007). *Proces ocenjevanja tveganj*. Najdeno 25. aprila 2012 na spletnem naslovu https://www.bsi.si/library/includes/datoteka.asp?DatotekaId=2437
6. Banka Slovenije. (2016). *Reševanje in prisilno prenehanje bank.* Najdeno 16. avgusta 2016 na spletnem naslovu https://www.bsi.si/sklad.asp?MapaId=1992&VsebinaId=19096
7. Banka X. (2010). *Organizacijska struktura banke* X. Ljubljana: Banka X.
8. Banka X. (2011). *Podpora poslovnim procesom v banki X*. Ljubljana: Banka X.
9. Bankart d.o.o. (2011). *Plačilni sistemi SEPA v okviru SIMP*. Najdeno 10. maja 2014 na spletnem naslovu strani http://www.bankart.si/si/ponudba/simp/
10. Bankart d.o.o. (2013. *Letno poročilo družbe Bankart d.o.o.* Najdeno 7. aprila 2015 na spletni naslovu http://www.bankart.si/assets/Uploads/Letna-porocila/Bankart-Letno-porocilo-2013.pdf/
11. Berk, A., Peterlin Jožko & Ribarič P. (2005). *Obvladovanje tveganja.* Ljubljana: GV Založba.
12. Besis, J. (1998). *Risk Management in Banking.* Chichester: John Wiley & Sons
13. Cameron, E. & Green, M. (2012). *Making sense of change management : A complete guide to the models, tools and techniques of organizational change*. London: Kogan Page
14. Davenport, T. (1993). *Reengineering Work throught Information Technology*. New York: McGraw-Hill.
15. Dimovski, V., Penger, S., Peterlin, J., Uhan, M., Černe, M. & Marič M. (2013). *Napredni management*. Ljubljana: Ekonomska fakulteta
16. Direktiva o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij. *Uradni list Evropske unije, št. 36/2013.*
17. Glogovšek, J. (2008). *Bančni menedžment*. Maribor: Založba Pivec.
18. Gomez-Mejia, L., Balkin, D., & Cardy, R. (2012). *Management : people, performance, change*. New York : Pearson.
19. Gradišar, M., Jurij, J., Talib, D., & Peter, B. (2005). *Osnove poslovne informatike*. Ljubljana: Ekonomska fakulteta.
20. Greuning, H. (2003). *Analyzing and managing banking risk.* Washington, DC : World Bank.

21. Kobayashi, I. (1995). *20 keys to workplace improvement*. New York : CRC Press.
22. Kovačič, A., & Vesna, B. (2005). *Management poslovnih procesov*. Ljubljana: GV Založba.
23. Možina, S. , Rozman, S., Tavčar, R., Pučko, D., Ivanko, Š., Lipičnik, B.,Gričar, J., Glas, M., Kralj, J., Tekavčič, M., Dimovski, V., & Kovač, B. (2002). *Management, nova znanja za uspeh*. Radovljica: Didakta.
24. Myers, P, Hulks, S., & Wiggins, L. (2012). *Organizational change: Perspectives on theory and practice.* Oxford : Oxford University.
25. Prosci Inc. (2014). *Change management.* Najdeno 5. maja 2016 na spletnem naslovu https://www.prosci.com/change-management/thought-leadership -library/measuring-change-management-effectiveness-with-metrics
26. Rotovnik, T. (2004). Problematika in kritika naprednih modelov za merjenje operativnega tveganja. *Bančni vestnik, (53)*12, 39
27. Rotovnik, T. (2005). Merjenje operativnega tveganja s pomočjo scenarijev. *Bančni vestnik, (54)*10, 36
28. International Organisation for Standardisation. (2015). *Quality management systems*. Najdeno 29. marca 2016 na spletnem naslovu https://www.iso.org/obp/ui/#iso:std:iso:9001
29. Štiblar, F. (2010). *Bančništvo kot hrbtenica samostojne Slovenije*. Ljubljana: ZRC SAZU
30. Tomisitch, J. (2010). Nekaj značilnosti operativnih škodnih dogodkov v slovenskem bančnem sistemu. *Bančni vestnik, (59)*10, 26
31. Uredba o bonitenih zahtevah za banke in investicijska podjetja. *Uradni list Evropske unije, št. 575/2013*.
32. Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). *Uradni list RS št. 98/2004*.
33. Zakon o bančništvu (ZBan-1). *Uradni list RS, št. 25/201.5*
34. Zakon o Banki Slovenije. *Uradni list RS, št. 72/2006, 59/2011*.
35. Zakon o plačilnih storitvah in sistemih (ZPlaSS). *Uradni list RS, št. 58/2009*.
36. Združenje bank Slovenije. (2007). *Uresničevanje projekta Sepa.* Najdeno 25. aprila 2014 na spletnem naslovu http://www.sepa.si/slo/sepa/
37. Združenje bank Slovenije. (2008). *Sepa v Sloveniji*. Najdeno 25. aprila 2014 na spletnem naslovu http://www.sepa.si/SloPrenova/Gradiva_Publikacije/Sepa_Zbs/

PRILOGE

KAZALO PRILOG

PRILOGA 1*:* Intervju z vodjem oddelka plačilnega prometa

Ali ste v oddelku plačilni promet do sedaj sistematično upravljali spremembe poslovnega procesa in kakšne težave ste imeli pri uvajanju sprememb?

Odgovor: Ne, žal smo do sedaj spremembe upravljali parcialno na nivoju oddelka. Težave, ki so se pojavljale, so bile posledica nezadostne dokumentacije o delovanju aplikacij in dokumentacije o izvajanju delovnih postopkov, prav tako ni bilo zadovoljivega komuniciranja med oddelki, na katere so spremembe vplivale, niti ni zadostne komunikacije med oddelkom informacijske tehnologije in oddelkom plačilnega prometa.

Ste mnenja, da bi proces upravljanja sprememb omogočil zmanjšanje možnosti za napake?

Odgovor: Mislim, da bi upravljanje sprememb, ki bi bile ustrezno obravnavane in dokumentirane, zmanjšalo možnost napak pri izvrševanju plačil in drugih aktivnosti v plačilnem prometu.

Kako mislite, da bi zaposleni sprejeli postopek upravljanja sprememb v oddelku?

Odgovor: Zaposleni v oddelku so mladi, željni znanja in bi upravljanje sprememb zagotovo sprejeli.

Sprejemate s strani zaposlenih predloge za izboljšave poslovnega procesa?

Odgovor: Z zaposlenimi imam odlično komunikacijo in lahko vedno predlagajo izboljšave poslovnega procesa.

Katere informacije želijo zaposleni v postopku upravljanja sprememb?

Odgovor: Najpogostejše informacije o obsegu spremembe, zakaj je potrebna in kako bo vplivala na njihova vsakodnevna opravila (zmanjšan obseg dela ali povečan obseg dela).

Ali bi se z uvedbo upravljanja sprememb zmanjšal odpor zaposlenih do uvedbe sprememb?

Odgovor: Da, na nivoju banke vsekakor, saj je zaradi kadrovske podhranjenosti vsaka sprememba sprejeta kot motnja in dodatno delo ter odgovornost, povzroči pa tudi možnost pojava napak.

Ali bi vzpostavljena dokumentacija upravljanja sprememb pripomogla k zmanjšanju napak in nepravilnosti zaposlenih pri izvajanju aktivnosti?

Odgovor: Menim, da bi se število napak zaposlenih pri izvajanju delovnih aktivnosti zmanjšalo.

Kako menite, da bo uprava banke sprejela predlog uvedbe upravljanja s spremembami?

Odgovor: Če bo Uprava banke spoznala, da je upravljanje s spremembami nujno in da bo pripomoglo k boljšim poslovnim rezultatom, bo predlog podprla.

Ali bo uvedba upravljanja s spremembami vplivala na poslovanje banke in kako?

Odgovor: V začetku bo uvedba upravljanja s spremembami zaradi povečanega obsega dela (izvajanje sprememb na podlagi prejetega dokumenta in obravnave sprememb) povzročila nekaj odpora predvsem pri srednjem managementu. Na dolgi rok se bo povečala baza znanja in nepotrebnih napak zaposlenih bo manj.

Bodo zaposleni z uvedbo upravljanja s spremembami razširili svoje znanje o bančnem poslovanju?

Odgovor: Vsekakor, upam, da bo upravljanje s spremembami doprineslo k boljšim poslovnim rezultatom banke, boljšemu komuniciranju med zaposlenimi in odpravilo ozka grla v poslovnih procesih, hkrati pa zaposleni ne bodo izpostavljeni tveganju, da naredijo napako, za katero sploh ne vedo, da se lahko pojavi.

PRILOGA 2: Razvrščanje sprememb

Spremembe bomo razvrstili glede na pomembnost, in sicer na spremembe, ki zahtevajo takojšnje ukrepanje t.i. nujne in take, katerih implememntacija lahko nekoliko počaka t.i. nenujne oz. rutinske spremembe.

Spremembe bomo razvrstili glede na obseg potrebnega dela za implementacijo, in sicer bomo definirali manjše spremembe, to bodo tiste, ki za realizacijo potrebujejo manjša sredstva (manj kot 1.000,00 EUR) in zahtevajo manj človeških resursov in večje spremembe, to bodo tiste, ki za realizacijo potrebujejo večja sredstva (več kot 1.000,00 EUR) in več človeških resursov.

Spremembe bomo razvrstili glede na velikost tveganja, in sicer na tiste, ki vključujejo manjša tveganja in tiste, ki vključujejo večja tveganja.

Spremembe bomo razvrstili glede na zahtevan rok izvedbe, in sicer na spremembe, ki morajo biti izvedene v manj kot enem mesecu in na spremembe, ki so lahko izvedene v obdobju po preteku enega meseca.

Spremembe bomo razvrstili glede na področje, in sicer na spremembe v vsebini (zakonske ali uporabniške zahteve), programski opremi, informacijski infrastrukturi.

Spremembe bomo razvrstili glede na bančni produkt /poslovni proces, in sicer ali se sprememba nanša na ključen produkt ali ne.

Spremembe bomo končno razvrstili tudi glede na poslovne funkcije t.j. oddelke v katerih bo potekala izvedba spremembe.

PRILOGA 3: Obrazec za uvedbo spremembe

Sprememba se v oddelku upravljanja sprememb identificira, razvrsti in zapiše v bazo prejetih sprememb. Po sprejemu odločitve, ali se bo sprememba izvedla in kako se bo izvedla, se v obliki obrazca posreduje upravi in pooblaščenim osebam za izvedbo spremembe.

Obrazec bo vseboval naslednje elemente:

- Datum prejema spremembe
- Šifra spremembe
- Naziv spremembe
- Pomembnost spremembe
- Obseg potrebnega dela
    - človeški resursi za izvedbo
- Stopnja tveganja
- Rok za dokončanje uvedbe spremembe
- Področje uvedbe
- Poslovni produkt
- Poslovna funkcija
- Pooblaščena oseba za izvedbo spremembe
- Sodelujoče osebe pri uvedbi spremembe
- Lastnik poslovnega procesa 1
- Lastnik poslovnega procesa 2
- Lastnik poslovnega procesa 3
- Identifikacija in opis možnih operativnih tveganj
- Odgovoren član uprave

V kratki dokumentaciji o spremembi se vpiše vse zgoraj naštete parametre, razloge za spremembo in cilj uvedene spremembe. Nakazati je potrebno možne rešitve ter izdelati načrt izvedbe uvajanja spremembe.

Najpomembnejše je, da se v zaključku dokumentacije navede vpliv na ostale poslovne procese in vključi opis potencialnih operativnih in drugih tveganj. S tem bomo v banki vzpostavili bazo potencialnih škodnih dogodkov v posameznih oddelkih.

PRILOGA 4: Seznam kratic

BANKART – upravljavec plačilne infrastrukture SIMP in upravljavec plačilnih sistemov sistemov **SEPA** v Republiki Sloveniji

BASEL II - kapitalski sporazum izdan s stani **BIS**, ki vsebuje priporočila za izdelavo politik za obvladovanje tveganj

BASEL III - nadgrajen kapitalski sporazum BASEL II, izdan s stani BIS, ki vsebuje dodatna priporočila za izdelavo politik za obvladovanje tveganj

BIC (angl. *Bank Identifier Code*) – identifikacijska oznaka banke (SWIFT)

BIS (angl. *Bank for International Settlements*) – Banka za mednarodne poravnave

BPR (angl. *Business Process Reengineering*) – popolna prenova poslovnih procesov

BS – Banka Slovenije

CRR (angl. *Capital Requirements Regulation*) - uredba o bonitetnih zahtevah za kreditne institucije in investicijska podjetja

CRD IV (angl. *Capital Requirements Directive IV***) -** direktiva o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij

CSM (angl. *Clearing and Settlement Mechanisms*) – klirinški in poravnalni mehanizmi

EBA (angl. *European Banking Association*) – evropsko bančno združenje je organizacija, ustanovljena po francoskem pravu, ki združuje banke s sedežem oziroma poslovno dejavnostjo, registrirano v državi članici EU, in katere cilj je sodelovanje pri uresničevanju skupnih interesov, zlasti na področju medbančnih plačil in prenosov denarnih sredstev. Z namenom uresničevanja skupnih ciljev svojih članic združenje EBA vzpostavlja plačilne sisteme, ki zagotavljajo učinkovit prenos denarnih sredstev med članicami (plačilni sistemi EBA).

EC (angl. *European Commission*) – evropska komisija

ECB (angl. *European Central Bank*) – evropska centralna banka

EPC (angl. *European Payments Council*) – evropski svet za plačila, zakonodajno telo za bančno industrijo na področju zadev v zvezi z evropskimi plačili

ESCB (angl. *European System of Central Banks***) –** evropski sistem centralnih bank

IBAN (angl. *International Bank Account Number*) – mednarodna bančna številka transakcijskega računa

KLIRING - postopek izračuna skupne neto denarne obveznosti oziroma skupne neto denarne terjatve posamezne neposredne udeleženke do ostalih neposrednih udeleženk plačilnega sistema

NCB (angl. *National Central Bank*) – nacionalna centralna banka

PJS – poravnalna jamstvena shema, mehanizem sodelovanja likvidnih udeležank pri kritju neporavnane skupne neto denarne obveznosti ene ali več udeležank, ki na poravnalnem računu nimajo zadosti sredstev za poravnavo svojih skupnih neto denarnih obveznosti iz naslova SEPA IKP

POS (angl. *Point of sale*) – terminal za sprejem plačilnih kartic na prodajnem mestu

PSD in PSD2 (angl. *Payment Services Directive*) – direktiva o plačilnih storitvah na notranjem trgu

SCT (angl. *SEPA Credit Transfer*) – kreditna plačila SEPA
SDD (angl. *SEPA Direct Debit)* – SEPA direktna obremenitev
SECA (angl. *Single Euro Cash Area*) – Enotno območje evro gotovine
SEPA (angl. *Single Euro Payments Area*) – Enotno območje plačil v evrih, ki uporabnikom plačilnih storitev ne glede na državo nalogodajalca in prejemnika v območju SEPA omogoča izvajanje plačil pod enakimi osnovnimi pogoji, pravicami in obveznostmi ter poslovnimi običaji
SEPA Direct Debit - direktna obremenitev SEPA je nalog za poravnavo, ki jo urejajo pravila sheme SEPA za direktne obremenitve za izvajanje plačil v evrih na območju SEPA. Pojem "SEPA Direct Debit" oz. "direktna obremenitev SEPA" ne vključuje R-sporočil po poravnavi
SEPA Core Direct Debit Scheme Rulebook - pravila Evropskega sveta za plačila (EPC) za izvajanje direktnih obremenitev v evrih v SEPA standardu in po osnovni shemi SEPA (Pravila delovanja osnovne sheme SEPA za direktne obremenitve)
SEPA EDD B2B (angl. *Business to Business Direct Debit Scheme-B2B*) – Shema SEPA B2B za eksterne direktne obremenitve
SEPA EDD CORE – plačilni sistem SEPA Eksterni Direct Debit po osnovni shemi SEPA
SEPA EKP – shema za procesiranje čezmejnih SEPA plačil
SEPA IDD B2B (angl. *Business to Business Direct Debit Scheme-B2B*) – Shema SEPA B2B za interne direktne obremenitve
SEPA IDD CORE – plačilni sistem SEPA Interni Direct Debit po osnovni shemi SEPA omogoča izvrševanje eksternih (čezmejnih) kreditnih plačil malih vrednosti med udeleženkami v standardih SEPA
SEPA kreditno plačilo - plačilo v evrih med strankami s transakcijskimi računi pri bankah na območju SEPA, pri čemer plačilo sproži plačnik, kot je opredeljeno v vsakokrat veljavnem dokumentu SEPA SCT Scheme Rulebook
SEPA SCT Scheme Rulebook – pravila Evropskega sveta za plačila (EPC – European Payments Council) za izvajanje kreditnih plačil v evrih v SEPA standardu (Pravila EPC za izvajanje SEPA kreditnih plačil)
SHA *(*angl. *Shared Cost Option*) – Opcija delitve stroškov – nalogodajalec in upravičenec nosita vsak stroške svoje banke
SIMP – Sepa Infrastruktura za Mala Plačila, SEPA skladna infrastruktura za procesiranje SEPA plačilnih instrumentov
SLA (angl. *Service Level Agreement*) – sporazum o ravni zagotavljanja storitev
STEP2 M-PEDD CORE – sistem za obdelavo SEPA direktnih obremenitev, ki ga upravlja družba EBA Clearing.
SPS (angl. *SEPA payment scheme*) – plačilne sheme SEPA
STP (angl. *Straight-through-processing*) – popolna avtomatizacija procesiranja plačil
SWIFT (angl. Society for Worldwide Interbank Financial Telecommunications) – globalni sistem za prenos finančnih podatkov
TARGET2 (angl. *Trans-European Automated Real-time Gross Settlement Express Transfer System*) – plačilni sistem, ki zagotavlja bruto poravnavo plačil v evrih v realnem

času s poravnavo v centralno-bančnem denarju. Sistem temelji na enotni tehnološki platformi, pravno pa je strukturiran kot množica plačilnih sistemov (komponent sistema TARGET2) centralnih bank držav članic Evropske unije, ki upravljajo lastno komponento sistema

TQM (angl. *Total Quality Management*) – pristop k prenovi poslovanja z nenehnim izboljševanjem kakovosti poslovanja

UNIFI (angl. *Universal Financial Industry message scheme*) – univerzalna shema finančne industrije za prenos sporočil, UNIFI (ISO 20022) XML standardi – obvezni SEPA standardi v odnosu banka–banka in priporočeni standardi v odnosu banka–komitent.

ZBS – Združenje bank Slovenije

XML (angl. *Extensible Markup Language*) – razširljiv označevalni jezik