Датум пријема рада: 09.06.2015.
Датум прихватања рада: 20.06.2015.
Прегледни рад
УДК: 336.717.13:339.727.22]:004
DOI: 10.7251/NOE1619089S

ИНФОРМАЦИОНО-ТЕХНОЛОШКИ АСПЕКТ УПРАВЉАЊА РИЗИЦИМА У ПЛАТНИМ СИСТЕМИМА

THE IT ASPECT OF THE PAYMENT SYSTEMS RISK MANAGEMENT

Проф. др Раде Станкић,
Економски факултет, Београд, Србија
rstankic@ekof.bg.ac.rs

Мр Марко Станкић,
Београд, Србија
stamarem@hotmail.com

Резиме: *Управљање платним системом подразумева управљање основним ризицима који карактеришу те системе, где је један од најважнијих – оперативни ризик. Управљање оперативним ризиком се у великом делу односи на управљање информационим системом платног система. Пораст ефикасности платног система нераскидиво је повезан са имплементацијом најсавременијих хардверско-софтверских решења, због чега управљање оперативним ризиком у савремним условима мора бити континуиран и динамичан процес. Информациона технологија има важну улогу и код управљања осталим ризицима који су иманентни платним системима. Референтне међународне институције дефинишу стандарде и препоруке на којима се базира рад савремених платних система, и тиме операторима система пружају основне смернице за менаџмент ризика у платном систему. Међутим, не постоје универзална правила примењива у свим случајевима, односно свака институција менаџмент ризика треба да прилагоди конкретном систему, околностима у оквиру којих функционише, ресурсима са којима се располаже и другим факторима..*

Кључне ријечи: *Информационе технологије; платни систем; оперативни ризик; управљање ризицима..*

Abstract: *Management of payment system implies and requires management of core risks immanent to those systems, operational risk being the most important. Managing the operational risk in payment system to the great extent means management of its information technology infrastructure. The increase in the payment system efficiency is essentially connected to implementation of state-of-art hardware and software solutions, at the same time requiring operational risk management to be a dynamic and continual process. Information technology has significant role in the management of all other risks immanent to payment systems, also. International institutions and organisations are creating standards and recommendations for modern payment systems, by which they provide systems' operators with core guidelines for payment system risk management. Still, there are no universal rules applicable in all cases, meaning every institution has to adjust its risk management to that particular system, environment that it is functioning in, resources that are available and other elements.*

Key Words: *Information Technologies; Operational Risk; Risk Management, Payment System .*

1. УВОД

Електронски платни системи функционишу у различитим облицима већ неколико деценија. Износи који се обрађују у електронским великопродајним системима (енгл. *Electronic Wholesale Payment Systems*) могу да буду огромни. На пример, амерички платни системи FEDWIRE (телекомуникациона мрежа којом управља *Систем федералних резерви*, за трансфере између финансијских институција које имају рачуне код банака федералних резерви.) и CHIPS (*Clearing House Interbank Payments System*) „обрну" износ еквивалентан друштвеном бруто производу САД за 2,5 дана.

Британски CHAPS (*Clearing House Automated Payments System*) дневно обави плаћања у износу од 90 милијарди фунти, што представља четвртину друштвеног бруто производа Велике Британије. Јапанском систему за међубанкарски трансфер средстава потребно је мање од три радна дана да постигне обрт који је једнак друштвеном бруто производу Јапана, док се овакав обрт у Немачкој постиже за четири дана. Вредности трансакција у платном систему *TARGET2*, Европске монетарне уније, приказане су у Табели 1.

ТАБЕЛА 1. ВРЕДНОСТИ ТРАНСАКЦИЈА У СИСТЕМУ *TARGET2* У МИЛИЈАРДАМА ЕВРА. [1]

Земља/год	2009	2010	2011	2012	2013	%
Немачка	171300	213841	210260	195561	151591	30,72%
Француска	93757	94072	102300	110252	87565	17,75%
Холандија	73476	77458	79204	105508	69341	14,05%
Шпанија	91063	88311	94391	88333	65095	13,19%
Италија	32241	33197	33052	32663	37465	7,59%
Белгија	27027	24591	27207	26635	21402	4,34%
Луксембург	10299	10258	14711	18015	17009	3,45%
Финска	7228	9061	12101	21872	9894	2,01%
ЕУ	11941	9503	9359	8893	8618	1,75%
Аустрија	7266	6988	6939	6486	7513	1,52%
Грчка	7464	7180	6000	5021	5308	1.08%
Ирска	7752	7642	5284	4398	3720	0,75%
Португалија	4251	5152	5670	3709	3461	0,70%
Данска	3742	3405	3332	2896	2736	0,55%
Словачка	880	682	707	840	627	0,13%
Словенија	586	582	594	714	608	0,12%
Кипар	390	455	429	701	337	0,07%
Естонија	87	84	304	320	323	0,07%
Бугарска	-	181	286	313	275	0,06%
Пољска	132	181	299	301	144	0,03%
Малта	0	77	109	261	132	0,03%
Летонија	194	200	228	186	105	0,02%
Литванија	96	97	123	137	99	0,02%
Руминија	-	-	50	115	75	0,02%
Укупно	551172	593194	612936	634132	493442	100,00%

Управљање ризиком у платним системима веома је важно из следећих разлога:

- Платни систем је централни део домаће и међународне финансијске инфраструктуре;
- Екстремно велике вредности плаћања увек су последица трговине на тржишту новца, тржишту хартија од вредности и међународне трговине;
- Платни системи су од критичног значаја за функционисање економије;
- Платни системи су примарни канал за трансмисију монетарне политике, али су исто тако и директан канал за трансмисију поремећаја и финансијских шокова;
- Инструмени и процедуре у платним системима су важни за поверење јавности у националну валуту.

Приступ код управљања савременим платним системима треба да се заснива на управљању ризицима који карактеришу те системе. Модели и методе које се примењују у појединачним случајевима могу се значајно разликовати. Међутим, уочава се тежња за њиховом униформношћу до мере до које то дозвољавају специфичности система и разлике друштвено-економског окружења у коме систем функционише. Платне системе карактеришу следећи ризици: ликвидносни ризик, кредитни ризик, оперативни ризик, правни ризик и системски ризик. [2]

2. ИНФОРМАЦИОНО-ТЕХНОЛОШКИ АСПЕКТ УПРАВЉАЊА РИЗИЦИМА У ПЛАТНИМ СИСТЕМИМА

Информационо - комуникациона инфраструктура, њено одржавање и сигурност, може имати пресудни значај за одржање конкурентске позиције, солвентности, рентабилности сваке финансијске институције, па и институције која је учесник или оператор неког платног система.

Глобализација финансијских услуга, заједно са убрзаним порастом значаја информационих технологија у финансијским системима, чине да активности финансијских институција и ниво и категорије ризика буду све сложенијег карактера. То има своју импликацију и на платне системе, а нарочито оне од системског значаја, међународног карактера или ако су пак релативно важан систем у некој глобално значајној економији света. У условима глобализације многе финансијске институције су, са својом организационом мрежом, глобално присутни "играчи" и због тога им је потребан сложенији систем управљања ризицима, прилагођен сваком од појединачних услова тржишта. Такође, финансијске институције веома често делове информационог система граде ослањајући се на *outsourcing*, чиме управљање оперативним ризиком постаје још сложеније, пре свега због тога што је систем везан не само за институцију у којој је оперативан, већ и за систем спољног провајдера сервиса.

Када је реч о финансијским ризицима, улога информационе технологије је велика, јер се неки од најважнијих механизама управљања овим ризицима базирају на информационо-технолошким решењима. То се пре свега односи на: резервације, лимите, редове за чекање итд. Међутим, оно што је кључно - ефикасно функционисање информационо-технолошког решења платног система омогућава правовремено испуњавање новчаних

обавеза и уједначене, равномерне токове ликвидности, пре свега између најважнијих финанасијских институција, а затим и привредних субјеката и становништва.

Референтне међународне институције дефинишу стандарде и препоруке на којима се базира рад савремених платних система, и тиме операторима система пружају основне смернице за менаџмент ризика у платном систему. То су превасходно стандарди које прокламује *Банка за међународна поравнања* (*Bank for International Settlement*), од којих су најважнији садржани у документу „*Основни принципи за системски важне платне системе*“ (*Core Principles for Sistemically Important Payment System-CPSIPS*). [3] Међутим, не постоје универзална правила примењива у свим случајевима, односно свака институција менаџмент ризика треба да прилагоди конкретном систему, околностима у оквиру којих функционише, ресурсима са којима се располаже и другим факторима.

Специфичност информационих система платних система у односу на друге информационе системе, огледа се, пре свега, у комплексности и важности улоге који они имају за функционисање новчаних токова. Из те специфичности произилази и комплексније управљање ризиком, које се директно рефлектује на сложеност дизајна тих система и његових процеса. То се, нарочито, огледа у императивном креирању редудантности компоненти и бекап решења, који ће обезбедити континуитет пословања у свим ситуацијама које одступају од редовног стања. Ефикасност и поузданост платног система је у директној зависности од информационо-технолошке основе система, као и архитектуре свих његових компоненти. Одржавање стабилног и ефикасног функционисања система је динамичан процес који имплицира адекватан менаџмент ризика у систему, како не би дошло до отказивања система или његовог дела, односно како би његови кључни ресурси били максимално расположиви корисницима.

Највећа корелација информационе технологије и платног система, ипак се јавља код оперативног ризика, где је управљање информационим системом саставни критични део овог процеса.

3. УПРАВЉАЊЕ ОПЕРАТИВНИМ РИЗИКОМ У ПЛАТНИМ СИСТЕМИМА

Платни систем је један од делова финансијског система чије је ефикасно функционисање у највећој мери зависно од начина примене информационо-комуникационе технологије. Њен значај се прожима кроз све кључне ризике иманентне платном систему, а најзначајнију улогу има код управљања оперативним ризиком, код кога се највећи део процеса управљања базира на адекватном управљању информационим системом платног система.

Базелски комитет дефинише оперативни ризик као ризик губитка који ће резултирати из интерног процеса који неадекватно или уопште не функционише, или губитка због људских грешака, грешака у систему или узрока везаних за екстерне догађаје.

Оперативни ризик можемо дефинисати као потенцијал да дође до пропуста у оперативном процесу који може резултирати губицима у пословању.

Оперативни ризик представља ризик да стабилност функционисања система буде угрожена оперативним факторима, као што је нефункционисање техничког дела процеса или услед оперативних грешака. Оперативни ризик се реализује у случајевима непоузданости информационог система, неадекватних мера контроле, грешака људског фактора и грешака код управљања системом. Превентивно деловање у правцу минимизирања овог ризика од посебног је значаја ако се има у виду његов карактер – а то је да релизовање оперативног ризика, у највећем броју случајева, представља директан импулс за иницирање реализације системског ризика, и то знатно брже и директније у поређењу са осталим ризицима.

Реализација оперативног ризика не значи само системски ризик за тај појединачни платни систем, већ и системски ризик за платне системе финансијских институција-учесница у систему, као и за њихове клијенте, правна и физичка лица, којима би било онемогућено да врше плаћања, односно да измирују своје обавезе. Сва плаћања која би била усмерена ка примаоцу чији се рачун води код друге институције, не би могла бити реализована. Не само да би финансијске институције за које се врши обрачун биле онемогућене да врше плаћања и измирују своје обавезе, већ би то био случај и са правним и физичким лицима чији се рачуни воде код тих институција.

Поред система међубанкарских плаћања и обрачуна по тим плаћањима, реализација оперативног ризика у одређеном систему представља системски ризик и за све друге системе који се поравнавају у оквиру тог система, односно када се оперативни ризик реализује у систему који представља тачку повезивања великог броја подсистема, он тада имплицира својеврсну мултипликацију

„домино ефекта“ системских ризика. У случају система као што је то, рецимо, *RTGS* (*Real Time Gross Settlement*) платни систем, то би практично значило блокаду целокупног финансијског система земље.

Веома важно је анализирати информационо-технолошку архитектуру појединих система и испитати њихове импликације на реализацију оперативног ризика. Посебну пажњу треба посветити *плану континуитета пословања* (енгл. *business continuity plan*), као једном од основних средстава у управљању оперативним ризиком.

Најважнији део ових планова превасходно чини: адекватан инфомационо-технолошки оквир система, односно његов дизајн, како се њиме управља, редовна тестирања делова и компоненти, адекватан ниво сервисирања система, располагање са добро обученим и компетентним људским ресурсима, највиши ниво физичког обезбеђења система, итд. Кључни део планова континуитета пословања је софтеверско-хардверски и комуникациони оквир система, подршка, одражавање, унапређивање и развој, како би се достигао жељени ниво квалитета сервиса.

Основни механизми за превазилажење оперативног ризика укључују:

- Примену безбедносних стандарда;
- Обезбеђивање бекап система;
- Интерне процедуре за одржавање континуитета пословања;
- Адекаватно обучено и специјализовано особље.

Захтеви за сигурност и поузданост платног система идентификују се кроз процес оцењивања ризика по сигурност тог система. Оцена самог ризика може бити квалитативна и квантитативна, у зависности од опортуности и примењивости одређеног решења.

Без обзира на методолошки приступ, један од основних принципа треба да буде то да трошкови контрола треба да су у равнотежи са штетом у пословању која би могла настати као резултат нарушене сигурности.

Процес процене ризика представља основу утврђивања активности и приоритета код управљања ризицима по сигурност информационог система и пословног процеса, као и за имплементацију контрола изабраних као заштита од тих идентификованих ризика. Процењивање ризика је потребно понављати периодично како би се обухватиле евентуалне измене које би могле утицати на резултате оцењивања ризика.

Када су захтеви за сигурност и ризици идентификовани, и када су донете одлуке о поступању са ризицима, треба одабрати и имплементирати одговарајуће контроле како би се ризици свели на прихватљив ниво. Контроле се могу одабрати на основу неког од постојећих стандарда или се могу применити нове контроле како би се задовољиле специфичне потребе платног система. Избор сигурносних контрола зависи од критеријума оператора система и мора бити заснован на оценама о прихватљивости ризика, анализи алтернатива поступања са ризиком, уважавајући, ако такав постоји, стандардни приступ управљања ризицима који се код тог типа система примењује, али узевши у обзир и специфичности датог система.

Свест о оперативном ризику значајно је порасла током последњих година, било да је реч о платном систему или о индивидуалном учеснику у таквим системима – појединачној финансијској институцији. Платни систем се састоји од мреже међуповезаних елемената: оператора, учесника и евентуално обрачунских агената. Оперативни проблем на било ком кључном елементу има потенцијал да угрози целокупни систем. Платни систем мора бити сигуран, поуздан, ефикасан и безбедан. Он мора функционисати поуздано и у критичним тренуцима, без дуготрајне нерасположивости сервиса, осим у случају најгорих могућих сценарија. Озбиљан ванредни догађај може спречити оператора система да функционише са примарног сајта, и у том случају грешке у плановима континуитета пословања могу спречити безбедан наставак пословања са резервног сајта.

Оно што је за одређене околности и време адекватно може се променити услед нових догађаја и развоја. Током последњих деценија велика пажња се посвећивала дизајну система у погледу контроле ликвидносног и кредитног ризика. Након дешавања 11. септембра 2001. године, оперативном ризику се посвећује вишеструко већа пажња него што је то било пре тога. Поменути догађаји су нагласили значај документованих, валидних и тестираних планова континуитета пословања помоћу којих се могу превазићи и најекстремнија дешавања.

Напредак у информационој технологији може да промени композицију оперативног ризика. Нове технологије се имплементирају не само због смањења ризика већ, на првом месту, због уштеда у трошковима. Софистицирана технологија обезбеђује брзо, сигурно и ефикасно процесирање операција платног система. Међутим, тако компликована

технологија повећава оперативни ризик везан за оштећење хардвера и софтвера и проблема мреже који могу резултирати у паду система. Оперативни ризик може индиректно покренути реализацију ликвидносног и кредитног ризика, који могу угрозити укупну стабилност финансијског система.

У већини случајева пад система резултира из оштећења хардвера, софтверских проблема, извора енергије, проблема са мрежом и људских грешака. Оперативни ризик природно расте са растом удаљености између оперативних сајтова. У складу са тим, локација операција је један од фактора од критичног значаја. Такође, комплексност сервиса повећава оперативни ризик. Један од фактора је и раст обима промета, што утиче не само на техничке перформансе система, већ и на могућност људских грешака због притиска под којим се запослени због тога налазе.

Финансијским институцијама је пре свега због одржавања сопственог угледа и интегритета у јавности, одувек било јако важно да, у мери у којој је то могуће, спрече преваре, проневере, да се смањи број грешака и сл. Због тога је одавно схваћена потреба дефинисања унутрашњих процеса и контрола. Касније су оне допуњене функцијом ревизије. Ипак, управљање оперативним ризиком на начин на који се данас третира, релативно је новијег датума, посебно у поређењу са другим ризицима везаним за пословање финансијских институција.

Неадекватно управљање оперативним ризиком узрокује отказивање стратешких параметара система, са директним индуковањем системског ризика.

ЗАКЉУЧАК

Може се закључити да су ризици у електронским платним системима неизбежни, а задатак финансијске институције се састоји у томе да са њима управља на што бољи начин. Да би се финансијске институције заштитиле од оперативног, правног и репутационог ризика, услуге електронског платног система морају да се пружају конзистентно и благовремено, у складу са високим очекивањима клијената у погледу сталне и брзе расположивости, али и у складу са потенцијално високом тражњом за трансакцијама.

Финансијске институције морају да буду способне да пружају услуге електронског платног система свим крајњим корисницима и да буду у стању да одрже такву расположивост у свим околностима. Ефективни механизми за реаговање на инциденте су такође од кључног значаја за умањење оперативног, правног и репутационог ризика који настају као последица неочекиваних догађаја, укључујући интерне и екстерне нападе, који могу да угрозе систем. Да би се одговорило очекивањима клијената, финансијске институције морају да имају ефективан капацитет, пословни континуитет и планове за сваку евентуалност.

Методолошки постаматрано пракса показује да се већина оператора платних система ослања на основне препоруке дефинисане у „*Основним принципима за системски важне платне системе*“, који су прерасли и у методолошку основу процене адекватности управљања ризицима у платном систему, коју примењују *Европска централна банка*, *Међународни монетарни фонд* и *Светска банка*, за потребе различитих програма и пројеката. Када је реч о учесницима, важан документ су препоруке Базелског комитетета за супервизију банака (*Basel Committee on Banking Supervision-BCBS)* [4], везане за оперативни ризик. Поред тога, од великог су значаја и индустријски стандарди, на првом месту универзално значајних организација као што је *ISO* и др.

Када је реч о квантификацији управљања ризиком, постоје бројни покушаји креирања општих методологија, међутим, ниједан се метод, за сада, не може сматрати шире прихваћеним, односно углавном се суочавају са бројним критикама. У том смислу, може се рећи да је за сада најадекватнији приступ „*моделирање сопствене методологије*“ у зависности од конкретног стања, сврхе, величине, релативног значаја у односу на друге системе и других карактеристика система.

ЛИТЕРАТУРА

[1] http://www.ecb.europa.eu/paym/t2/html/index.en.html

[2] “Банкарско пословање и платни промет”, Живковић А., Маринковић С., Станкић Р., Економски факултет, Београд, 2012.

[3] https://www.bis.org/cpmi/publ/d43.pdf

[4] “Principles for the Sound Management of Operational Risk“, Bank for International Settlement, Basel Committee on Banking Supervision (BCBS), 2011.