НАРОДНА БАНКА СРБИЈЕ

УПРАВА ЗА НАДЗОР НАД ФИНАНСИЈСКИМ ИНСТИТУЦИЈАМА
ЦЕНТАР ЗА СУПЕРВИЗИЈУ ИНФОРМАЦИОНИХ СИСТЕМА

АНАЛИЗА ОДГОВОРА ФИНАНСИЈСКИХ ИНСТИТУЦИЈА НА УПИТНИК О ИНФОРМАЦИОНОМ СИСТЕМУ

Упитник спроведен у октобру 2012.

Март 2013.

Садржај:

1. Увод

Упитник о информационом систему финансијске институције (у даљем тексту: Упитник) спроведен је у периоду од 2. до 22. октобра 2012. године и био је намењен свим финансијским институцијама које Народна банка Србије контролише, односно над којима врши надзор (банке, друштва за осигурање, даваоци финансијског лизинга и друштва за управљање добровољним пензијским фондовима). Упитником су покривена значајна подручја у вези са информационим системом, а добијени резултати допринели су бољем свеобухватном сагледавању и оцени постојећег стања и процеса управљања информационим системима у финансијским институцијама.

Упитник је обухватио 114 питања, груписаних у осам[1] области:

I. Оквир за управљање информационим системом
II. Управљање ризиком информационог система
III. Ревизија информационог система
IV. Безбедност информационог система
V. Континуитет пословања и опоравак активности у случају катастрофе
VI. Развој и одржавање информационог система
VII. Поверавање активности у вези са информационим системом трећим лицима
VIII. Електронско банкарство

Већина питања била је конципирана као „Да/Не“, уз мањи број отворених питања и могућност да се сваки одговор додатно појасни. Од финансијских институција захтевало се да одговоре на сва питања из Упитника и попуне приложену табелу о активностима у вези са информационим системом које су поверене трећим лицима, као и да доставе одговарајућу организациону шему и топологију рачунарске мреже. Свака институција била је дужна да одреди једног члана највишег руководства као лице одговорно за попуњавање Упитника које ће потврдити тачност и потпуност свих пружених информација.

* * *

Подаци приказани у овој анализи представљају само збирни преглед тренутног стања у време спровођења Упитника, по врстама финансијских институција, без улажења у резултате детаљније анализе и оцене сваке појединачне институције. Преглед који је овде дат сачињен је искључиво на основу одговора финансијских институција на питања из Упитника.

[1] Област VIII била је намењена само банкама.

2. Анализа постојећег стања по областима из Упитника

2.1. Оквир за управљање информационим системом

Ова област је обухватила питања на основу којих су добијене информације о основним поставкама процеса управљања информационим системом. Постављена су питања о постојању утврђених надлежности и одговорности у вези са управљањем информационим системом, одговарајућој организацији и успостављеним функцијама, постојању уређених линија извештавања највишег руководства о релевантним чињеницама у вези с функционалношћу и безбедношћу информационог система, стратегији развоја информационог система и др.

У погледу организације и броја запослених, може се констатовати да је у финансијским институцијама на пословима из области информационих система и технологија ангажовано 1.440 запослених, или 3,5% укупног броја.

Број запослених на пословима у вези са информационим системом у односу на укупан број запослених у финансијским институцијама

	Укупан број запослених	Број запослених у надлежним ОЈ	Учешће у укупном броју запослених
Банке	29.129	1.158	4,0%
Друштва за осигурање	11.388	264	2,3%
Даваоци финансијског лизинга	436	14	3,2%
Друштва за управљање ДПФ	159	4	2,5%
УКУПНО	41.112	1.440	3,5%

Извор: Народна банка Србије

Банке

Стратегију развоја информационог система има 30 банака, од којих је код њих 29 тај документ одобрило и усвојило највише руководство банке. Четири банке су навеле да надлежности и одговорности за успостављање, надзор и унапређење процеса управљања информационим системом нису дефинисане унутрашњим општим актом.

Осам банака (24%) навело је да нема усвојену и документовану методологију којом се дефинишу критеријуми, начини и поступци управљања пројектима у вези са информационим системом.

Друштва за осигурање

Од 21 друштва за осигурање, колико их је навело да има стратегију развоја информационог система, код 17 друштава ту стратегију је одобрило и усвојило највише руководство друштва. Слично стање је и у погледу надлежности и одговорности за успостављање, надзор и унапређење процеса управљања информационим системом, које је унутрашњим општим актом дефинисало 18 друштава.

На питање да ли постоји усвојена и документована методологија којом се дефинишу критеријуми, начини и поступци управљања пројектима у вези са информационим системом, 21 друштво (75%) дало је негативан одговор.

Даваоци финансијског лизинга

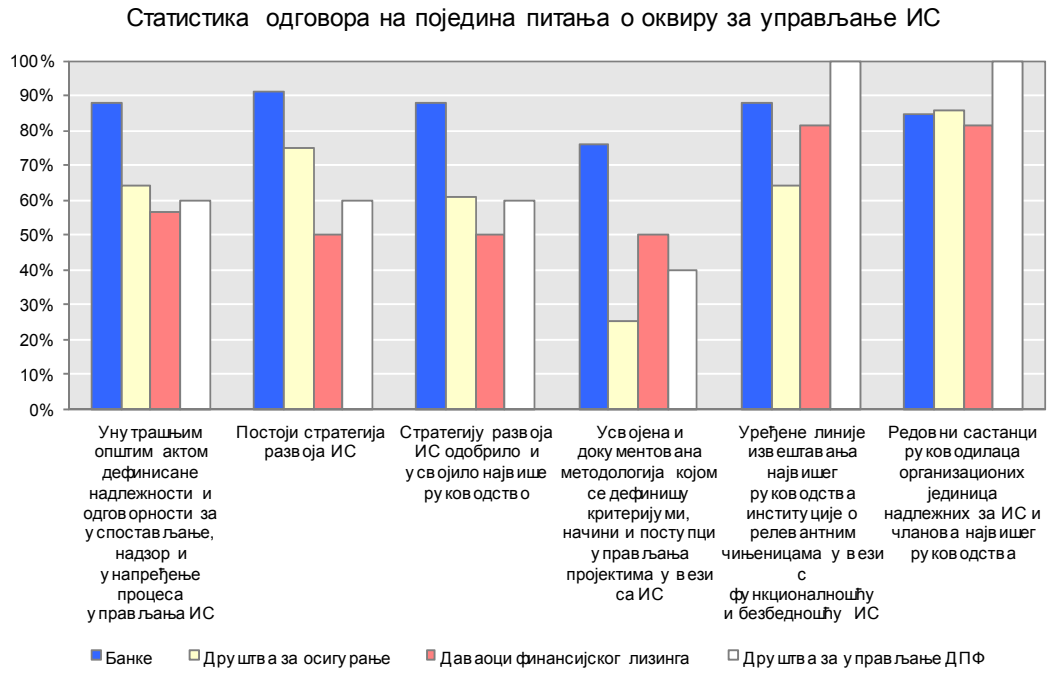
Девет давалаца финансијског лизинга је унутрашњим општим актом дефинисало надлежности и одговорности за успостављање, надзор и унапређење процеса управљања информационим системом, при чему је један број њих навео да су ове надлежности и одговорности пренете на оснивача. Стратегију развоја информационог система има осам давалаца финансијског лизинга и све је одобрило и усвојило највише руководство институције.

Такође, осам давалаца финансијског лизинга (50%) навело је да нема усвојену и документовану методологију којом се дефинишу критеријуми, начини и поступци управљања пројектима у вези са информационим системом.

Друштва за управљање добровољним пензијским фондовима

Три друштва за управљање добровољним пензијским фондом навела су да постоји стратегија развоја информационог система, као и да је ту стратегију одобрило и усвојило највише руководство друштва. Такође, три друштва су унутрашњим општим актом дефинисала надлежности и одговорности за успостављање, надзор и унапређење процеса управљања информационим системом.

Три друштва немају усвојену и документовану методологију којом се дефинишу критеријуми, начини и поступци управљања пројектима у вези са информационим системом.



2.2. Управљање ризиком информационог система

Одговори на питања постављена у овом делу Упитника пружили су основне информације о томе да ли су финансијске институције препознале ризик информационог система и у којој мери је тај ризик укључен у целокупан систем управљања ризицима.

Банке

На основу одговора банака, може се закључити да је већина њих (27) уочила значај ризика информационог система, укључивши га у свеобухватни систем управљања ризицима.

Истовремено, 12 банака (36%) изјавило је да постојећим стратегијама и политикама управљања ризицима није обухваћен тај ризик. Имајући у виду да је 28 банака навело да су одговарајуће контроле дефинисане ради ублажавања ризика информационог система, овакви одговори највероватније указују на то да та врста ризика није посебно дефинисана или да нема јасно утврђене методологије за његову процену и сл. Поред тога, девет банака (27%) навело је да у постојећи процес управљања ризицима и у систем интерног извештавања о ризицима нису укључене активности у вези са информационим системом које су поверене трећим лицима.

Друштва за осигурање

У 24 друштва за осигурање свеобухватни систем управљања ризицима укључује и управљање ризиком информационог система. Такође, 22 друштва су навела да постојеће стратегије и политике за управљање ризицима обухватају и ризик информационог система, док их је исти број навео да су, ради ублажавања тог ризика, дефинисане одговарајуће административне, техничке и физичке контроле.

Активности у вези са информационим системом које су поверене трећим лицима 12 друштава (43%) није укључило у постојећи процес управљања ризицима и у систем интерног извештавања о ризицима.

Даваоци финансијског лизинга

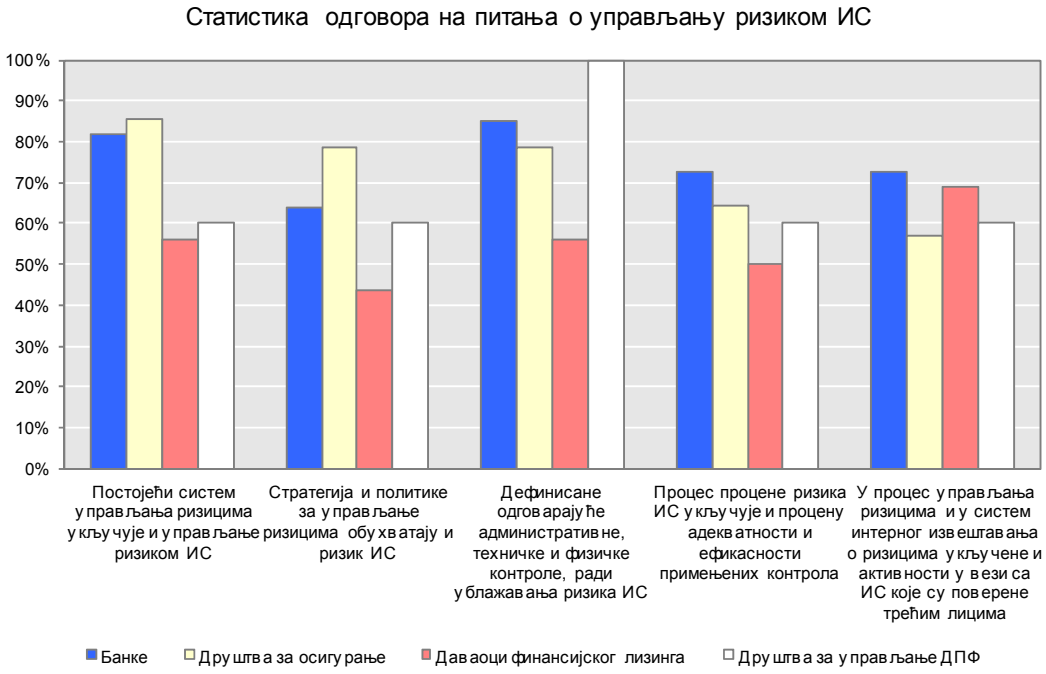
Половина свих давалаца финансијског лизинга навела је да је управљање ризицима уређено путем политике групација којима припадају. Девет давалаца финансијског лизинга је управљање ризиком информационог система укључило у постојећи систем управљања ризицима, а исти број њих је изјавио да су одговарајуће контроле дефинисане ради ублажавања тог ризика.

С друге стране, девет давалаца финансијског лизинга (56%) својим стратегијама и политикама управљања ризицима није обухватило ту врсту ризика, а њих пет (31%) навело је да у процес управљања ризицима, као и у систем интерног извештавања о ризицима, нису укључене активности у вези са информационим системом које су поверене трећим лицима.

Друштва за управљање добровољним пензијским фондовима

Два друштва за управљање добровољним пензијским фондом навела су да у постојећи систем управљања ризицима није укључено управљање ризиком информационог система, а исти број њих тај ризик није обухватио својим стратегијама и политикама управљања ризицима. Такође, активности у вези са информационим системом које су поверене трећим лицима два друштва нису укључила у процес управљања ризицима и у систем интерног извештавања о ризицима.

Међутим, сва друштва су изјавила да, ради ублажавања ризика информационог система, имају дефинисане одговарајуће административне, техничке и физичке контроле.



2.3. Ревизија информационог система

На основу одговора на питања из овог дела Упитника добијена су општа сазнања о томе у којој мери и на који начин се у финансијским институцијама врши унутрашња ревизија информационог система.

Банке

Већина банака, њих 28, обухватила је актуелним програмом унутрашње ревизије и ревизију информационог система, а 29 банака навело је да се критеријуми, начини и поступци ревизије информационог система заснивају на процени ризика. Поред тога, 18 банака је у току 2012. године, ради независне процене информационог система и процеса управљања тим системом, ангажовало треће лице (које истовремено није спољни ревизор банке).

С друге стране, 16 банака (48%) навело је да међу ангажованим унутрашњим ревизорима нема лица у чијем је опису посла тај сегмент ревизије.

Друштва за осигурање

Када су у питању друштва за осигурање, њих 17 је актуелним програмом унутрашње ревизије обухватило и ревизију информационог система. Таква

ревизија је у току 2012. године обављена у десет друштава, а најчешће навођени предмет ревизије били су безбедност и чување података. На процени ризика заснивају се критеријуми, начини и поступци ревизије информационог система 20 друштава. Седам друштава навело да је спроведена независна процена информационог система од стране трећег лица, које је у појединим случајевима спровео оснивач друштва.

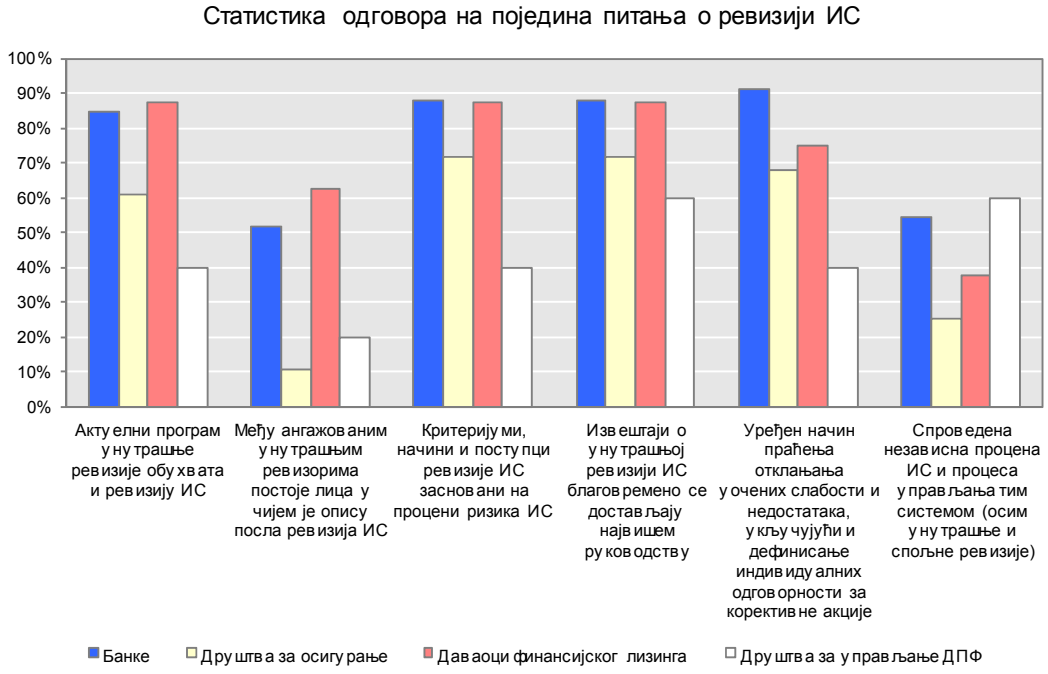
Само три друштва (11%) имају међу ангажованим унутрашњим ревизорима и лица у чијем је опису посла ревизија информационог система.

Даваоци финансијског лизинга

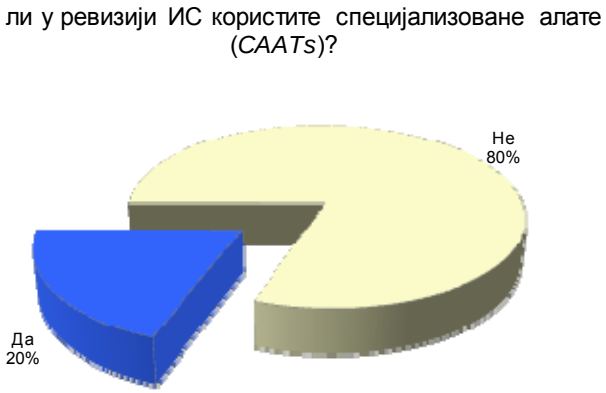
Код давалаца финансијског лизинга унутрашња ревизија, као и управљање ризицима, често је поверена матичној компанији, односно другој чланици групе друштава. Како је у великом броју случајева то банка која послује у Србији, праксе унутрашње ревизије информационих система давалаца финансијског лизинга сличне су као код банака. У 12 таквих институција је у периоду 2009–2012. обављена унутрашња ревизија, која је у неком сегменту обухватила и информациони систем. Шест давалаца финансијског лизинга навело да је спроведена и независна процена информационог система од стране трећег лица.

Друштва за управљање добровољним пензијским фондовима

Два друштва за управљање добровољним пензијским фондом су актуелним програмом унутрашње ревизије обухватила и ревизију информационог система, при чему су се изјаснила и да се та ревизија заснива на процени ризика.



Само мањи број финансијских институција (20) навео је да при обављању унутрашње ревизије информационих система користе специјализоване алате, односно софтвер за рачунарски потпомогнуту ревизију (*Computer Assisted Audit Tools – CAATs*).



2.4. Безбедност информационог система

Ова област је обухватила 25 питања која су омогућила да се добију информације од значаја за оцену постојећег стања у области информационе безбедности у финансијским институцијама.

Банке

Већина банака, тачније 31 банка, има политику безбедности информационог система, али четири од њих нису обезбедиле да сви корисници информационог система буду упознати са садржином ове политике – што чини 18%, рачунајући и банке које немају тај документ.

Такође, 31 банка има успостављен систем управљања корисничким правима приступа информационом систему, а њих 30 је уредило процес надзора и ревидирања тих права. Међутим, пет банака (15%) изјаснило се да не практикује вишефакторску аутентификацију корисника информационог система. Удаљени приступ информационом систему омогућен је у 27 банака, од којих њих 26 примењује додатне мере заштите приликом таквог приступа.

Све банке су навеле да примењују софтвер за заштиту информационог система од малициозног програмског кôда, као и контроле за физичку заштиту ресурса тог система, а њих 30 изјаснило се да поседује системе за спречавање, откривање и сигнализирање упада у информациони систем. Систем надгледања информационог система и генерисања логова не постоји у девет банака (27%).

Друштва за осигурање

Политику безбедности информационог система има 21 друштво за осигурање (75%), при чему је уједно обезбеђено да сви корисници информационог система буду упознати са садржином такве политике.

Сва друштва су успоставила систем управљања корисничким правима приступа информационом систему, с тим што у четири друштва (14%) не постоји процес надзора и ревидирања тих права. Вишефакторску аутентификацију корисника информационог система не практикује шест друштава (21%). Удаљени приступ информационом систему омогућила су 23 друштва и у ту сврху примењују додатне мере заштите.

Контроле за физичку заштиту ресурса информационог система примењује 27 друштава. Системе за спречавање, откривање и сигнализирање упада у информациони систем или других потенцијалних безбедносних инцидената нема 12 друштава (43%). Седам друштава (25%) изјаснило се да нема успостављен систем надгледања информационог система и генерисања логова.

Даваоци финансијског лизинга

С обзиром на то да је знатан број давалаца финансијског лизинга све активности у вези са информационим системом или највећи део њих, укључујући и чување и обраду података, поверио банци оснивачу, честа је пракса да се примењују и одговарајуће политике и стандарди оснивача. Девет таквих институција навело је да има политику безбедности информационог система, напомињући да је то политика оснивача/групе, док их седам (44%) нема такав акт.

Сви даваоци финансијског лизинга имају успостављен систем управљања корисничким правима приступа информационом систему. Њих 15 има уређен процес надзора и ревидирања тих права, а исто толико их је навело да, где постоји потреба, практикује вишефакторску аутентификацију корисника информационог система. Удаљени приступ том систему, уз примену додатних мера заштите у ту сврху, омогућило је 13 давалаца финансијског лизинга.

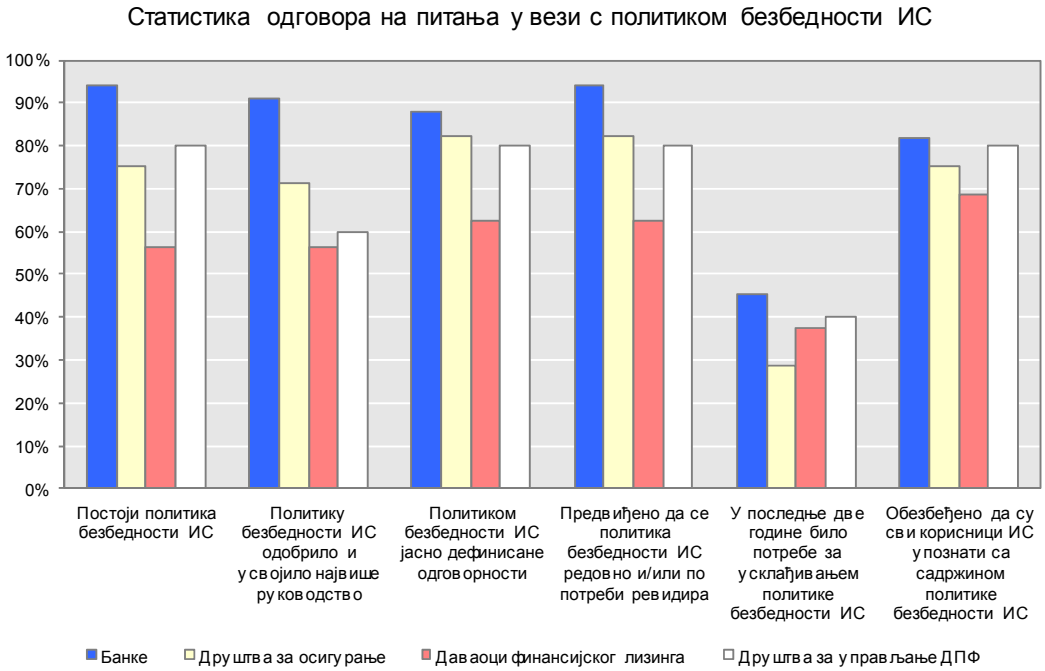
Сви даваоци финансијског лизинга имају софтвер за заштиту информационог система од малициозног програмског кôда, а њих 15 примењује контроле за физичку заштиту ресурса тог система. Систем надгледања информационог система и генерисања логова има 13 давалаца финансијског лизинга, а њих 12 је навело да поседује системе за спречавање, откривање и сигнализирање упада у информациони систем.

Друштва за управљање добровољним пензијским фондовима

Политику безбедности информационог система имају четири друштва за управљање добровољним пензијским фондом, с тим што је преостало друштво навело да примењује одговарајућу политику групе којој припада. Четири друштва су обезбедила да сви корисници информационог система буду упознати са садржином такве политике.

Сва друштва су навела да имају успостављен систем управљања корисничким правима приступа информационом систему, од којих у четири постоји процес надзора и ревидирања тих права. Четири друштва су навела да, где постоји потреба, практикују вишефакторску аутентификацију корисника информационог система, а исто толико их је омогућило удаљени приступ том систему, примењујући притом додатне мере заштите.

Сва друштва су навела да примењују софтвер за заштиту информационог система од малициозног програмског кôда, као и контроле за физичку заштиту ресурса тог система. Четири друштва имају успостављен систем надгледања информационог система и генерисања логова, а три су навела да имају системе за спречавање, откривање и сигнализирање упада у информациони систем.

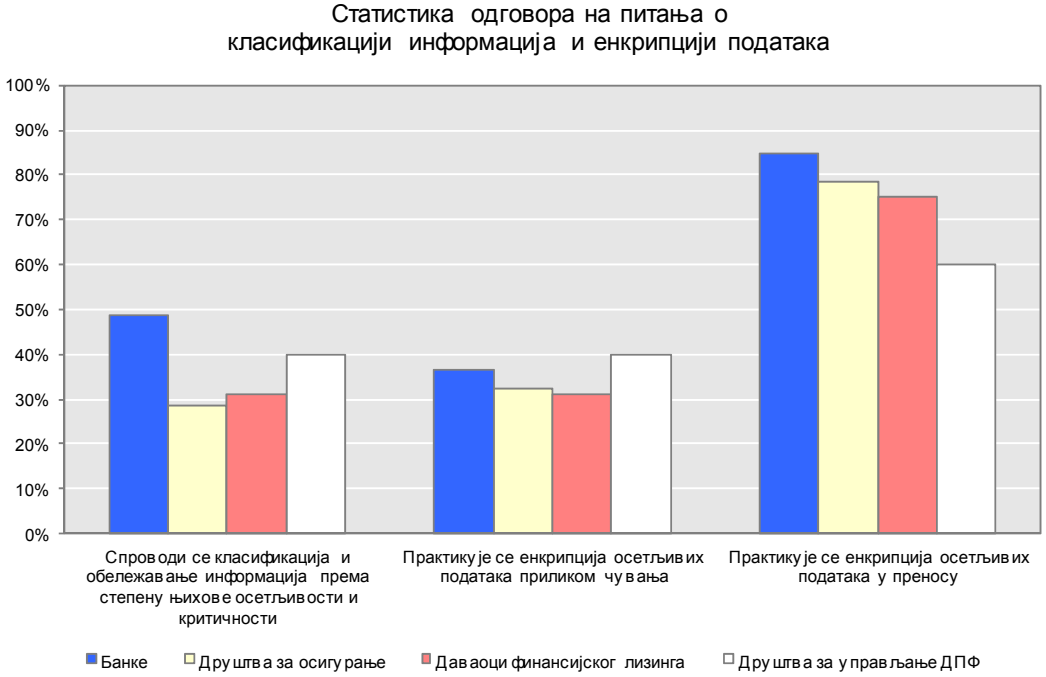


Добре праксе налажу да финансијске институције, кроз своје унутрашње акте (политику безбедности информационог система и њене пратеће, односно саставне документе), успоставе оквир за управљање безбедношћу информационог система, који треба да одражава основна начела те безбедности. Кроз те акте уређују се, између осталог, принципи, критеријуми, начини и

поступци за класификацију информација, управљање корисничким правима приступа, физичку заштиту ресурса информационог система, заштиту од малициозног програмског кôда и др.

Обезбеђивање адекватног нивоа заштите информација требало би да има полазиште у њиховој класификацији. То подразумева да се за све информације утврди степен осетљивости и критичности с обзиром на могуће последице њиховог евентуалног губитка, неовлашћеног откривања или измене и сл., како би се могао одредити потребан ниво заштите тих информација. С тим у вези, управо један од начина за унапређење нивоа заштите осетљивих информација јесте примена одговарајућих криптографских метода.

Резултати Упитника показују да тренутно мање од 40% свих финансијских институција спроводи класификацију информација (при чему је тај проценат највећи код банака – близу 50%), док између 30% и 40% њих практикује енкрипцију осетљивих података приликом чувања. Када је реч о енкрипцији података који се преносе кроз мрежу, статистика је знатно боља – близу 80% свих институција одговорило је потврдно, у чему опет предњаче банке са 85%.



2.5. Континуитет пословања и опоравак активности у случају катастрофа

Ради обезбеђивања несметаног и континуираног одвијања свих значајних пословних процеса и расположивости ресурса информационог система који су подршка тим процесима, као и ограничавања губитака у ванредним ситуацијама, добре праксе налажу да финансијске институције управљају континуитетом свог пословања. Тај процес, између осталог, укључује и усвајање, редовно усклађивање и тестирање одговарајућих планова и процедура за поступање у случају настанка таквих ситуација. Имајући у виду значај ове области, она је у Упитнику покривена са 21 питањем.

Банке

План континуитета пословања (*Business Continuity Plan – BCP*) имају све банке, а само код једне од њих, до достављања одговора на Упитник, тај план није усвојио управни одбор. План опоравка активности у случају катастрофа (*Disaster Recovery Plan – DRP*) усвојило је 30 банака, од којих је једна банка навела да нема детаљне процедуре за његово спровођење. Са својим улогама и одговорностима у случају настанка околности које би захтевале примену тих планова упознати су запослени у 32 банке. Тестирање *BCP* и *DRP* спроводи 29 банака, од којих њих 28 документује резултате тог тестирања и о тим резултатима извештава највише руководство. Међутим, само 23 банке (70%) изјавиле су да су у планирање и тестирање *BCP* и *DRP* укључене и активности поверене трећим лицима.

Већина банака, тачније 31, усвојило је процедуре и дефинисало одговорности у вези с креирањем резервних копија података, али њих седам, или укупно 27% свих банака, нема процедуре за тестирање тих копија, тј. успешности њихове рестаурације. Такође, на питање да ли је обезбеђено да је у сваком тренутку најмање једна ажурна и комплетна резервна копија података складиштена на примереној удаљености у односу на примарну локацију, четири банке (12%) одговориле су одрично. Расположивост резервног рачунарског центра обезбедило је 30 банака и све оне су навеле да се подаци између примарног и резервног центра синхронизују.

Друштва за осигурање

Девет друштава за осигурање (32%) има *BCP*, који је највише руководство одобрило и усвојило. С друге стране, 12 друштава (43%) навело је да има усвојен *DRP* и детаљне процедуре за његово спровођење. Сва друштва која имају усвојен *BCP* и/или *DRP* упознала су своје запослене с њиховим улогама и

одговорностима у случају настанка околности које би захтевале примену тих планова. Тестирање тих планова спроводи десет друштава, али само њих шест документује резултате тих тестова.

Када је реч о резервним копијама података, 23 друштва (82%) усвојила су процедуре и дефинисала одговорности у вези с креирањем тих копија, од чега је њих 20, тј. 71% укупног броја, навело да има и процедуре за њихово тестирање. Осам друштава (29%) изјаснило се да није обезбеђено да је у сваком тренутку најмање једна ажурна и комплетна резервна копија података складиштена на примереној удаљености у односу на примарну локацију. Резервни рачунарски центар на располагању има 11 друштава, од којих се код њих девет подаци синхронизују с примарним центром.

Даваоци финансијског лизинга

Од давалаца финансијског лизинга, њих десет (62%) навело је да има *BCP*, који је у осам случајева највише руководство одобрило и усвојило. Такође, осам ових институција (50%) усвојило је *DRP*, као и детаљне процедуре за његово спровођење. Сви даваоци финансијског лизинга који имају *BCP* и/или *DRP* упознали су своје запослене с њиховим улогама и одговорностима у случају настанка околности које би захтевале примену тих планова, али је само њих пет (31%) навело да су у планирање и тестирање *BCP* и *DRP* укључене и активности поверене трећим лицима. Осам давалаца финансијског лизинга навело је да спроводи тестирање ових планова, као и да се резултати тих тестова документују и достављају највишем руководству.

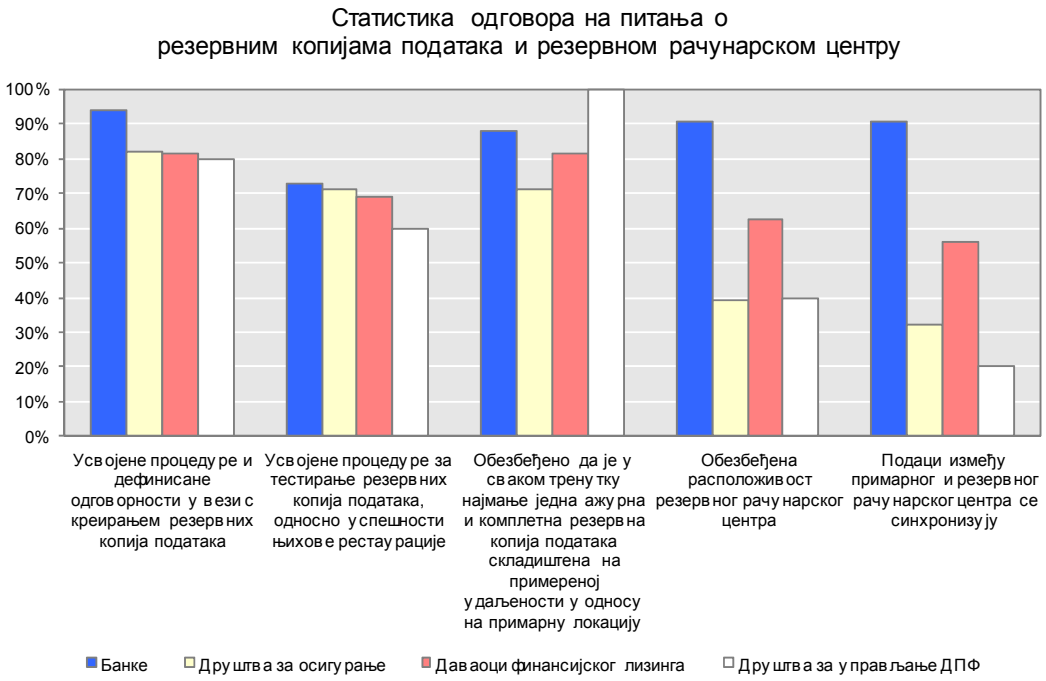
Усвојене процедуре и дефинисане одговорности у вези с креирањем резервних копија података има 13 давалаца финансијског лизинга (81%), колико их је и обезбедило да је у сваком тренутку најмање једна ажурна и комплетна копија складиштена на примереној удаљености у односу на примарну локацију. Процедуре за тестирање тих копија усвојило је њих 11, или 69% укупног броја давалаца финансијског лизинга. Резервни рачунарски центар на располагању има десет ових институција, од којих се код њих девет подаци синхронизују с примарним центром.

Друштва за управљање добровољним пензијским фондовима

Два друштва за управљање добровољним пензијским фондом имају *BCP*, који је највише руководство одобрило и усвојило, док су три друштва навела да имају усвојен *DRP* и детаљне процедуре за његово спровођење. Сва друштва која имају усвојен *BCP* и/или *DRP* упознала су своје запослене с њиховим улогама и одговорностима у случају настанка околности које би захтевале примену тих планова. Три друштва су навела да се ти планови тестирају, као и да су спровела

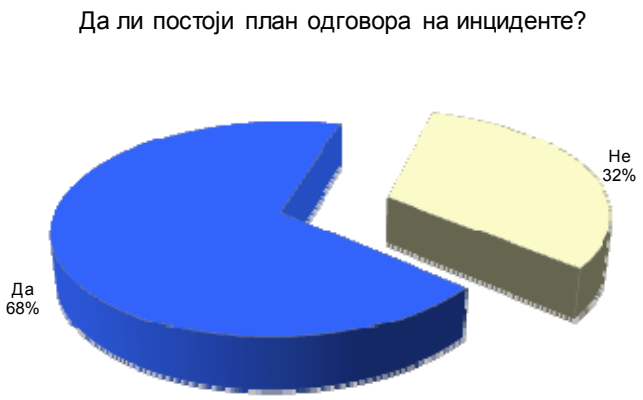
тестове у току 2012. године, али само два друштва документују резултате тих тестова.

Четири друштва су усвојила процедуре и дефинисала одговорности у вези с креирањем резервних копија података, док су три друштва навела да имају усвојене и процедуре за тестирање тих копија. Два друштва имају на располагању резервни рачунарски центар, од којих се код једног подаци синхронизују с примарним центром.



Саставни део управљања континуитетом пословања јесте и управљање инцидентима[2]. Мање од 5% финансијских институција изјаснило се да је у последње две године било већих инцидената, а њих 68% навело је да има план одговора на инциденте.

[2] Под инцидентом се подразумева непланирани и нежељени догађај који може нарушити безбедност или функционалност информационог система.



2.6. Развој и одржавање информационог система

Овај део Упитника састојао се од 25 питања, на основу којих су добијене основне информације о апликативним софтверским решењима која се развијају интерно и процесу тог развоја, затим о управљању хардверским и софтверским компонентама, управљању променама на информационом систему, планираним значајним променама у наредном периоду и др.

Општа констатација је да 90% финансијских институција развој и одржавање одређених апликативних софтверских решења[3] поверава спољним добављачима – специјализованим софтверским кућама или својим матичним компанијама, док само мањи број њих има искључиво интерни развој. Најчешћа је ситуација да се та два приступа комбинују, тако што се развој и одржавање главне пословне апликације поверава трећем лицу, док се интерно, у већини случајева, развијају „споредне“ апликације или одређени модули главне пословне апликације.

Банке

Интерни развој одређених софтверских компонената има 29 банака, од којих су две навеле да немају документован комплетан процес тог развоја. Скоро све банке воде детаљну и ажурну евиденцију софтверских и хардверских компонената информационог система, али њих пет (15%) није именовало лица одговорна за управљање и заштиту тих компонената, исто колико их није дефинисало правила њиховог прихватљивог коришћења.

[3] Не мисли се на куповину лиценци за софтвер који је комерцијално доступан на тржишту као готово решење, без прилагођавања.

Што се тиче управљања променама на информационом систему, 30 банака има дефинисан поступак иницирања, анализе и одобравања захтева за промену, а 32 банке су навеле да су све промене хардверских и софтверских компонената, укључујући и нове компоненте и системе, тестиране и одобрене пре пуштања у продукцијски рад. С друге стране, десет банака (30%) нема дефинисан посебан поступак за управљање хитним променама. У претходној години дана 22 банке су имале знатнијих промена на свом информационом систему, док је 21 банка навела да такве промене планира у наредној години дана. Између осталог, пет банака планира миграцију података на нови систем, шест њих планира увођење нових функционалности, а две у плану имају обнављање опреме.

Седам банака сматра да постоје пословни процеси који су од значаја за њихово пословање а који нису апликативно покривени, где наводе формирање базе оперативних ризика, праћење захтева за измену апликативног софтвера, обраду специфичних кредита и др. Поред тога, 14 банака је навело да се у функционисању појединих пословних процеса, као што је обрада кредитног рејтинга клијента, процена појединих врста ризика и сл., користе кориснички управљане апликације[4].

Друштва за осигурање

Одређена апликативна софтверска решења интерно развија 13 друштава за осигурање (46%) при чему као примере наводе главне пословне апликације, веб--апликације и апликације за пословно извештавање. Од тих друштава која имају интерни развој софтвера, четири је навело да нема документован комплетан процес тог развоја. Скоро сва друштва воде детаљну и ажурну евиденцију софтверских и хардверских компонената информационог система и именовала су лица одговорна за управљање и заштиту тих компонената, док седам друштава (25%) није дефинисало правила њиховог прихватљивог коришћења.

Скоро сва друштва, њих 26, навела су да су све промене хардверских и софтверских компонената, укључујући и нове компоненте и системе, тестиране и одобрене пре пуштања у продукцијски рад, док су поступак иницирања, анализе и одобравање захтева за промену на информационом систему дефинисала 22 друштва. Само 14 друштава (50%) има дефинисан посебан поступак за управљање хитним променама, а њих десет (36%) навело је да нема хронолошки документоване све промене софтверских компонената и архитектуре база података. У претходној години дана 16 друштава је имало знатнијих промена на свом информационом систему, а њих 18 изјаснило се да у наредној години дана планира такве промене, као нпр. миграцију података на нови систем главних пословних апликација или прелазак на нови оперативни систем.

[4] Нпр. употреба специјално креираних *Excel* докумената и сл.

Значајне пословне процесе који нису апликативно покривени навело је да има 12 друштава, наводећи притом књиге штета, провизије заступника, актуарске извештаје и др. Њих 20 изјаснило се да постоје значајни пословни процеси који се ослањају на кориснички управљане апликације, као што су актуарски прорачуни, преноси премија, извештавање Народне банке Србије и др.

Даваоци финансијског лизинга

Ниједан давалац финансијског лизинга не користи интерно развијен софтвер. Скоро сви имају детаљну и ажурну евиденцију хардверских и софтверских компонената информационог система, док их је четири (25%) навело да није именовало лица одговорна за управљање и заштиту тих компонената. Исто толико давалаца финансијског лизинга није дефинисало правила њиховог прихватљивог коришћења.

Управљање променама на информационом систему, према одговорима на питања из Упитника, уређено је код већине давалаца финансијског лизинга, с тим што се њих седам (44%) изјаснило да нема дефинисан посебан поступак за управљање хитним променама. Осам давалаца финансијског лизинга навело је да је у претходној години дана имало знатнијих промена на свом информационом систему, а два да такве промене имају у плану у наредној години дана.

Само један давалац финансијског лизинга сматра да има значајне пословне процесе који нису апликативно покривени, али се њих девет изјаснило да се неки од таквих процеса ослањају на кориснички управљане апликације.

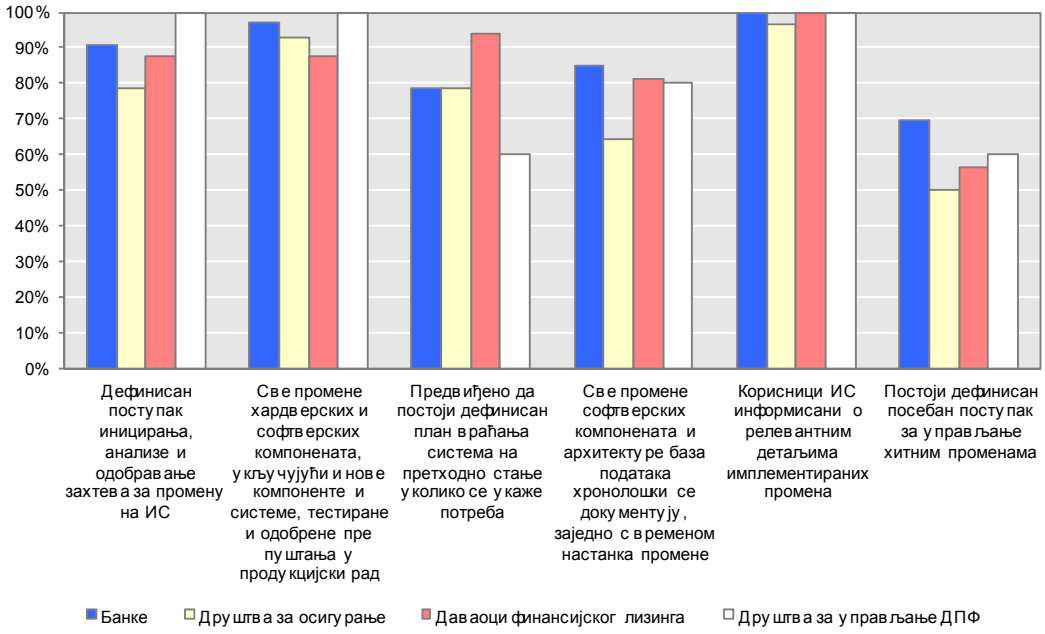
Друштва за управљање добровољним пензијским фондовима

Три друштва за управљање добровољним пензијским фондом нека од апликативних софтверских решења развијају интерно, при чему једно од тих друштава нема документован комплетан процес тог развоја. У погледу управљања хардверским и софтверским компонентама информационог система, сва или скоро сва друштва потврдно су одговорила на постављена питања.

Такође, у делу управљања променама на информационом систему одговори су већином потврдни, с тим што треба напоменути да и код ових институција, две институције (40%) немају дефинисан посебан поступак за управљање хитним променама. Два друштва су навела да су у претходној години дана имала знатнијих промена на информационом систему, и то замену рачунарске опреме, а три друштва да веће промене планирају у наредној години дана, не наводећи о каквим променама је реч.

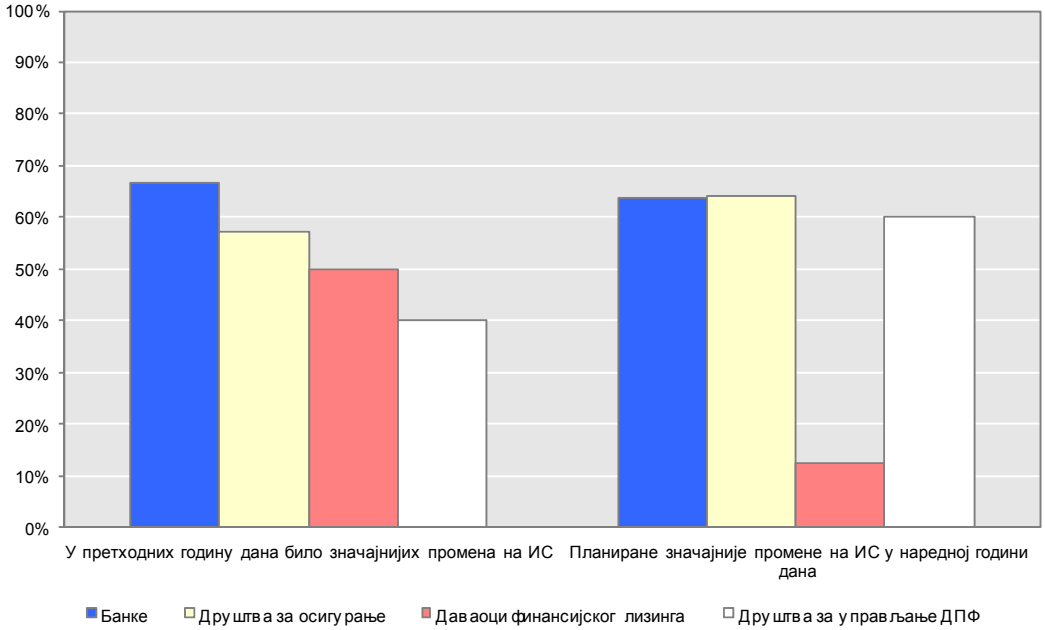
Сва друштва сматрају да су им сви значајни пословни процеси апликативно покривени, али је њих четири навело да неки од тих процеса зависе од кориснички управљаних апликација.

Статистика одговора на питања о управљању променама на ИС

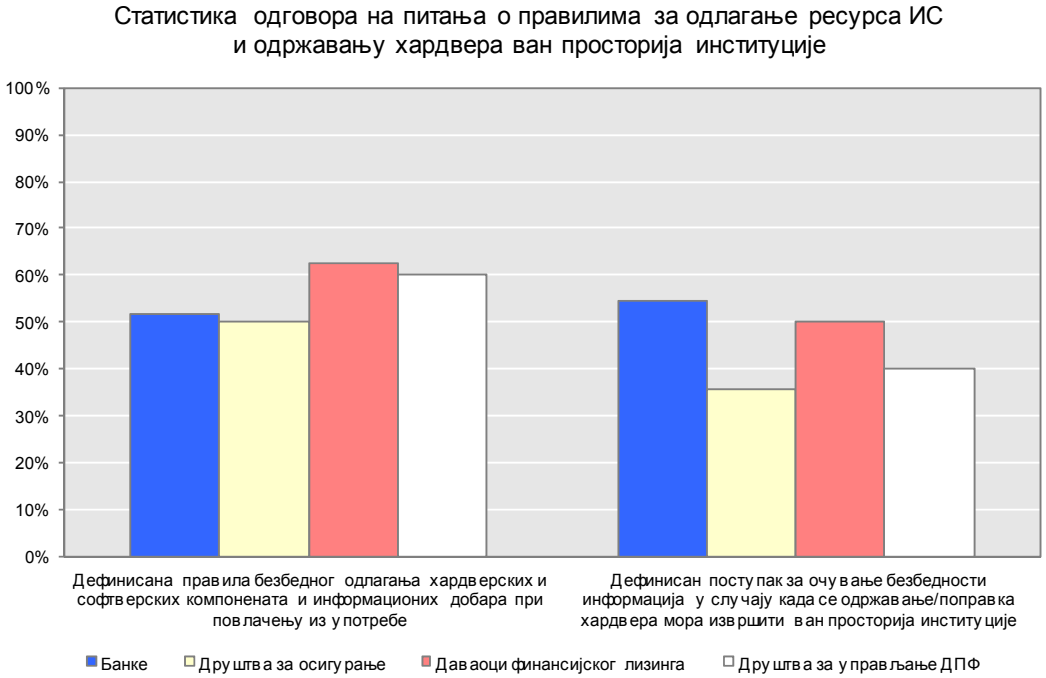


Адекватно управљање променама веома је важно за очување безбедности и функционалности информационог система. Имајући у виду обим тих промена, важна је констатација да је већина финансијских институција уредила тај процес.

Статистика одговора на питања о значајним променама на ИС



Додатну пажњу потребно је посветити заштити података забележених на хардверским компонентама приликом одржавања ван просторија институције, као и при повлачењу ресурса информационог система из употребе.



2.7. Поверавање активности у вези са информационим системом трећим лицима

За потребе Упитника, поверавање активности у вези са информационим системом трећем лицу обухватило је шири спектар активности него што је то дефинисано новом регулативом[5], а што је омогућило да се стекне боља слика о постојећој пракси и начину на који су финансијске институције уредиле ове процесе. У Упитнику је једино назначено да се под поверавањем активности у вези са информационим системом не сматра коришћење стандардизованих сервиса (*SWIFT*, *Bloomberg*, *Reuters* и др.), телекомуникационих услуга и сл.

Банке

Пружаоцу услуга који је оснивач банке, чланица исте групе или сл. активности је поверило 16 банака, а њих 29 поверило је активности пружаоцу услуга који није лице повезано с банком имовинским и управљачким односима. Притом, 18 банака је навело да се неке од поверених активности обављају изван

[5] Тачка 40. Одлуке о минималним стандардима управљања информационим системом финансијске институције („Службени гласник РС“, бр. 23/2013).

граница Републике Србије. Најчешће се поверавају активности развоја и одржавања главне банкарске апликације, процесирање трансакција платним картицама, електронско банкарство и процена ризика.

Већина банака дефинисала је поступак и критеријуме за доношење одлуке о поверавању активности (29 банака) и уредила начин вршења надзора над обављањем поверених активности (30 банака). Међутим, девет банака (27%) навело је да нема уређен начин на који се обезбеђује континуитет обављања активности у случају раскида уговорног односа с пружаоцима услуга или прекида пружања тих услуга. Такође, 17 банака (52%) навело је да уговорима о поверавању није обезбеђено преузимање података у стандардном формату након престанка ангажовања пружалаца услуга, док се њих 16 (48%) изјаснило да уговори не обезбеђују могућност неометаног вршења спољне ревизије и супервизије од стране Народне банке Србије над обављањем поверених активности. Осам банака (24%) не практикује да се у уговору с пружаоцем услуга јасно дефинише да подаци остају у власништву банке.

Друштва за осигурање

У 18 друштава за осигурање постоје активности које су поверене пружаоцу услуга који је оснивач друштва, чланица исте групе или сл., а њих 23 је одређене активности поверило пружаоцу услуга који није лице повезано с друштвом имовинским и управљачким односима. Од свих друштава која су поверила активности, њих 20 је навело да се неке од тих активности обављају изван граница Републике Србије. Активности које се најчешће поверавају су развој и одржавање главне пословне апликације и услуге чувања и обраде података (*data center*), као и апликације за кадровску евиденцију и управљање документима.

Већина друштава, њих 24, уредила је начин вршења надзора над обављањем поверених активности. Такође, 24 друштва практикују да се у уговору с пружаоцем услуга јасно дефинише да подаци остају у власништву (поседу) друштва, али, истовремено, само њих 18 је уговорило да подаци буду преузети у стандардном формату након престанка ангажовања пружалаца услуга. Могућност неометаног вршења спољне ревизије и супервизије од стране Народне банке Србије над обављањем поверених активности, уговорима с пружаоцима услуга обезбедила су 22 друштва. С друге стране, десет друштава (36%) није уредило начин на који се обезбеђује континуитет обављања активности у случају раскида уговорног односа с пружаоцима услуга или прекида пружања тих услуга, а поступак и критеријуме за доношење одлуке о поверавању активности није дефинисало њих 11 (39%).

Даваоци финансијског лизинга

Од давалаца финансијског лизинга, њих 12 изјаснило се да је одређене активности поверило пружаоцима услуга који су лица с њима повезана имовинским и управљачким односима (оснивачи, чланице групе или сл.), а њих 15 да је активности поверило пружаоцима услуга који не спадају у напред наведену групу. Да се неке од поверених активности обављају изван граница Републике Србије, одговорило је 12 давалаца финансијског лизинга. Као што је већ речено, у доста случајева ове институције свом оснивачу, који је најчешће банка, поверавају активности чувања и обраде података, администрирања и сл.

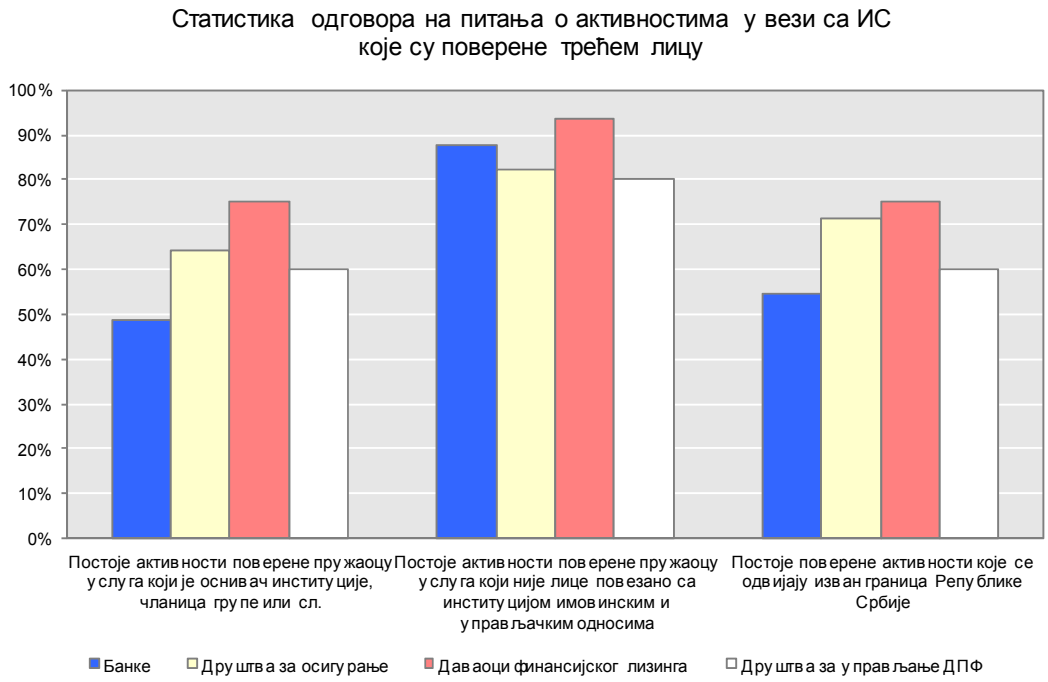
Према одговорима на питања из Упитника, ова област је код давалаца финансијског лизинга прилично уређена. Њих 13 има дефинисан поступак и критеријуме за доношење одлуке о поверавању активности, исто колико их је уредило начин вршења надзора над обављањем тих активности. Уређен начин на који се обезбеђује континуитет обављања активности у случају раскида уговорног односа с пружаоцима услуга или прекида пружања тих услуга има 12 давалаца финансијског лизинга, а исти број њих је навео да је уговорена могућност неометаног вршења спољне ревизије и супервизије од стране Народне банке Србије над обављањем поверених активности. Такође, 13 давалаца финансијског лизинга у уговорима с пружаоцима услуга јасно дефинишу да подаци остају у њиховом власништву, тј. поседу, али истовремено само њих осам је тим уговорима обезбедило да подаци буду преузети у стандардном формату након престанка ангажовања пружаоца услуга.

Друштва за управљање добровољним пензијским фондовима

Три друштва за управљање добровољним пензијским фондом поверила су активности пружаоцу услуга који је оснивач друштва, чланица исте групе или сл., а четири пружаоцу услуга који није лице повезано с друштвом имовинским и управљачким односима. Три друштва су навела да се неке од поверених активности обављају изван граница Републике Србије. Најчешће је поверен развој и одржавање главне пословне апликације, а наводи се и књиговодствени софтвер.

Три друштва су дефинисала поступак и критеријуме за доношење одлуке о поверавању активности, исто колико их је уредило начин вршења надзора над обављањем тих активности. Такође, три друштва имају уређен начин на који се обезбеђује континуитет обављања активности у случају раскида уговорног односа с пружаоцима услуга или прекида пружања тих услуга, а исти број њих је навео да уговори обезбеђују могућност неометаног вршења спољне ревизије и супервизије од стране Народне банке Србије над обављањем поверених активности. Четири друштва практикују да се у уговору с пружаоцем услуга јасно дефинише да подаци остају у власништву (поседу) друштва, али само два

друштва су уговорила преузимање тих података у стандардном формату након престанка ангажовања пружаоца услуга.

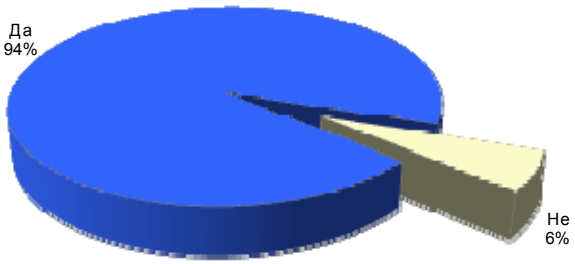


2.8. Електронско банкарство

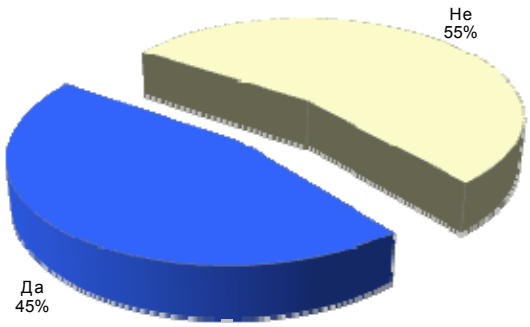
Због своје специфичности, овај део Упитника био је намењен само банкама, а обухватио је нека основна питања која се односе на послове интернет банкарства и мобилног банкарства.

Услуге интернет банкарства својим клијентима пружа 31 банка, а њих 15 је навело да пружа и услуге мобилног банкарства. Неколико банака је навело да планира да услугу мобилног банкарства уведе током 2013. године. За потврду идентитета корисника електронског банкарства банке користе различите методе аутентификације, односно комбинације тих метода (лозинка, ЛИБ, једнократна лозинка, токен, смарт картица, мини ЦД, дигитални сертификат и др.). Све банке које пружају ове услуге навеле су да поседују дигитални сертификат за потврду сопственог идентитета на дистрибутивном каналу електронског банкарства, да је обезбеђена обавезна употреба сигурносних протокола приликом извршавања трансакција, као и да се генеришу и чувају записи (логови) који могу да у одговарајућој мери осигурају непорецивост и доказивост активности у електронском банкарству.

Да ли банка пружа услуге интернет банкарства?



Да ли банка пружа услуге мобилног банкарства?



3. Закључак

Резултати до којих се дошло на основу анализе одговора из Упитника пружили су значајне информације за сагледавање и оцену постојећег стања информационих система у финансијским институцијама, као и пракси у управљању тим системима, и то за сваку појединачну институцију и за групу финансијских институција у целини. Поред тога, анализа је омогућила да се процени утицај који ће примена Одлуке о минималним стандардима управљања информационим системом финансијске институције[6] (у даљем тексту: Одлука) имати на пословање ових институција.

Управљање ризиком информационог система није адекватно уређено у свим финансијским институцијама. Неке институције су укључиле овај ризик у своје стандарде и политике управљања ризицима, друге га виде у оквиру оперативног ризика и ипак на неки начин управљају њиме, док га остале уопште нису препознале. Одлуком се прописује обавеза финансијских институција да свеобухватним системом управљања ризицима обухвате и ризик информационог система. У области које је потребно додатно унапредити, а које се, такође, уређују Одлуком, спадају и корпоративно управљање информационим системом и унутрашња ревизија информационог система.

У делу који се тиче безбедности информационог система, одговори на постављена питања показали су, између осталог, да класификација информација у већем броју финансијских институција није уређена. Одлуком се први пут финансијским институцијама прописује обавеза да спроводе класификацију информација у свом информационом систему. Такође, и обавеза управљања континуитетом пословања се за неке врсте институција први пут прописује Одлуком, па отуда потиче тренутна неуједначеност у пракси.

На основу одговора на питања о развоју и одржавању информационог система, може се закључити да је ова област у већини финансијских институција солидно уређена, имајући у виду да се и она Одлуком први пут уређује. Потребно је додатно унапредити област поверавања активности у вези са информационим системом трећем лицу, како би се испунили сви услови прописани Одлуком.

У одговорима финансијских институција на питања из Упитника може се уочити доста неуједначен ниво у погледу управљања информационим системом, што је последица и тога да је ова област важећим прописима била различито и само делимично уређена. Очекује се да ће се применом новог, јединственог регулаторног оквира за све финансијске институције тај ниво знатно унапредити и у што већој мери уједначити – водећи, наравно, рачуна о природи, обиму и сложености пословања сваке институције.

[6] „Службени гласник РС“, бр. 23/2013.