На основу члана 15. став 1. и члана 63. став 2. Закона о Народној банци Србије („Службени гласник РС“, бр. 72/2003, 55/2004, 85/2005 – др. закон, 44/2010, 76/2012 и 106/2012), Извршни одбор Народне банке Србије доноси

О Д Л У К У
О МИНИМАЛНИМ СТАНДАРДИМА УПРАВЉАЊА ИНФОРМАЦИОНИМ СИСТЕМОМ ФИНАНСИЈСКЕ ИНСТИТУЦИЈЕ

I. УВОДНЕ ОДРЕДБЕ

1. Овом одлуком утврђују се минимални стандарди и услови стабилног и сигурног пословања који се односе на управљање информационим системима у банкама, друштвима за осигурање, даваоцима финансијског лизинга, друштвима за управљање добровољним пензијским фондовима, као и платним институцијама, институцијама електронског новца и јавном поштанском оператору у делу њиховог пословања који се односи на пружање платних услуга и/или издавање електронског новца (у даљем тексту: финансијска институција).

Овом одлуком уређују се и минимални стандарди за управљање континуитетом пословања и опоравак активности у случају катастрофа у финансијској институцији.

Ова одлука примењује се на све финансијске институције, осим ако појединим њеним одредбама није друкчије утврђено.

2. Поједини појмови, у смислу ове одлуке, имају следеће значење:

1) *информациони систем* је свеобухватни скуп технолошке инфраструктуре (хардверске и софтверске компоненте), организације, људи и поступака за прикупљање, смештање, обраду, чување, пренос, приказивање и коришћење података и информација;

2) *ресурси информационог система* обухватају софтверске компоненте, хардверске компоненте и информациона добра;

3) *софтверске компоненте* обухватају све типове системског и апликативног софтвера, софтверске развојне алате, као и остали софтвер;

4) *хардверске компоненте* обухватају рачунарску опрему, комуникациону опрему, медије за чување података, као и осталу

техничку опрему која служи као подршка функционисању информационог система;

5) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и сл.;

6) *корисници информационог система* су сва лица која су овлашћена да користе информациони систем (запослени у финансијској институцији, запослени у другим лицима који приступају информационом систему финансијске институције, клијенти финансијске институције који информационом систему финансијске институције приступају преко електронских интерактивних комуникационих канала и др.);

7) *ризик информационог система* је могућност настанка негативних ефеката на финансијски резултат и капитал, остваривање пословних циљева, пословање у складу с прописима и репутацију финансијске институције услед неадекватног управљања информационим системом или друге слабости у том систему која негативно утиче на његову функционалност или безбедност, односно угрожава континуитет пословања финансијске институције;

8) *контроле* су политике, процедуре, праксе, технологије и организационе структуре које се односе на информациони систем, утврђене да би се обезбедило разумно уверење да ће пословни циљеви финансијске институције бити остварени и да ће нежељени догађаји бити спречени или откривени, а могу се разликовати према начину примене (управљачке, техничке и физичке) и намени (превентивне, детективне и корективне);

9) *управљачке контроле* обухватају доношење и примену политика, стандарда, планова, процедура и других унутрашњих аката, као и успостављање одговарајуће организационе структуре, а ради постизања и одржавања адекватног нивоа функционалности и безбедности информационог система;

10) *техничке контроле* су контроле примењене у хардверским и софтверским компонентама информационог система;

11) *физичке контроле* су контроле којима се ресурси информационог система штите од неовлашћеног физичког приступа, крађе, физичког оштећења или уништења;

12) *превентивне контроле* су контроле намењене спречавању настанка проблема и инцидената;

13) *детективне контроле* су контроле намењене откривању и препознавању проблема и инцидената и указивању на настале проблеме и инциденте;

14) *корективне контроле* су контроле намењене ограничавању и отклањању проблема и последица инцидената;

15) *инцидент* је сваки непланирани и нежељени догађај који може нарушити безбедност или функционалност информационог система;

16) *безбедност информационог система* подразумева очување поверљивости, интегритета, расположивости, аутентичности, доказивости, непорецивости и поузданости у информационом систему;

17) *поверљивост* означава да подаци и информације нису откривени или доступни неовлашћеним лицима;

18) *интегритет* означава да су подаци, информације и процеси заштићени од неовлашћеног или непредвиђеног мењања, односно да евентуалне такве промене не остају неопажене;

19) *расположивост* означава да су подаци, информације и процеси доступни и употребљиви на захтев овлашћеног лица;

20) *аутентичност* означава да је идентитет лица заиста онај за који се тврди да јесте;

21) *доказивост* означава да свака активност у информационом систему може бити једнозначно праћена до њеног извора;

22) *непорецивост* означава немогућност порицања активности извршене у информационом систему или пријема информације;

23) *поузданост* означава да информациони систем доследно и очекивано врши предвиђене функције и пружа тачне информације;

24) *ауторизација* је процес доделе права приступа корисницима информационог система;

25) *идентификација* је процес представљања корисника информационог система приликом пријаве и у току извођења активности у том систему;

26) *аутентификација* је процес провере и потврде корисничког идентитета коришћењем једног од следећих елемената или њихове комбинације:

– нешто што само корисник зна (нпр. лозинка, лични идентификациони број и сл.),

– нешто што само корисник поседује (нпр. магнетна картица, чип картица, токен, криптографски кључ и сл.),

– нешто што само корисник јесте (биометријске карактеристике као што су отисак прста, очна дужица, глас, рукопис и сл.);

27) *повлашћени приступ информационом систему* је приступ ресурсима информационог система који овлашћеним корисницима (администратори системског софтвера, администратори мреже, администратори база података и сл.) омогућава заобилажење техничких контрола;

28) *удаљени приступ информационом систему* је приступ ресурсима информационог система са удаљене локације посредством телекомуникационе инфраструктуре над којом финансијска институција нема потпуну контролу;

29) *оперативни и системски записи* означавају хронолошке записе о догађајима и активностима на ресурсима информационог

система (записи оперативних система, апликативног софтвера, база података, мрежних уређаја и сл.);

30) *малициозни програмски кôд* је било који облик програмског кôда створен с намером да се неовлашћено оствари приступ ресурсима информационог система, прикупе информације, изазове неочекивано понашање или прекид у функционисању овог система, односно да се на други начин потенцијално наруши поверљивост, интегритет или расположивост тих ресурса (нпр. рачунарски вируси, црви, тројански коњи и др.);

31) *критични/кључни пословни процеси* су пословни процеси или функције чије неадекватно функционисање може значајније угрозити пословање финансијске институције;

32) *најдужи прихватљив прекид* (*MAO – Maximum Acceptable Outage*) означава најдужи прихватљив период нерасположивости пословног процеса, односно критично време за опоравак тог процеса;

33) *циљни ниво активности* (*SDO – Service Delivery Objective*) означава одговарајући ниво опоравка пословног процеса који треба да буде постигнут током циљног времена опоравка;

34) *циљно време опоравка* (*RTO – Recovery Time Objective*) означава период, односно фазе у том периоду током којих треба да буде постигнут одговарајући ниво опоравка пословног процеса;

35) *циљна тачка опоравка* (*RPO – Recovery Point Objective*) означава најдужи прихватљив период од последње резервне копије података до наступања нерасположивости пословног процеса, односно најдужи прихватљив период за који подаци могу бити изгубљени;

36) *резервна копија података* представља копију најмање оних изворних података (софтверске компоненте и информациона добра) који су потребни за опоравак, односно за поновно успостављање пословних процеса;

37) *електронске услуге* су услуге које клијенти банке, платне институције, институције електронског новца и јавног поштанског оператора користе са удаљене локације преко интернета, а које обухватају приступање платном и другом рачуну, иницирање платне трансакције и друге активности којима се приступа подацима у вези са услугама ових финансијских институција који би могли бити предмет преварних радњи или других злоупотреба.

II. ОКВИР ЗА УПРАВЉАЊЕ ИНФОРМАЦИОНИМ СИСТЕМОМ

3. Финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, успостави адекватан информациони систем, који испуњава најмање следеће услове:

1) поседује функционалности, капацитете и перформансе који омогућавају пружање одговарајуће подршке пословним процесима;

2) обезбеђује благовремене, тачне и потпуне информације значајне за доношење пословних одлука, ефикасно обављање пословних активности и управљање ризицима, односно за сигурно и стабилно пословање финансијске институције;

3) пројектован је са одговарајућим контролама за валидацију података на улазу, у току процеса обраде, као и на излазу из тог система, ради спречавања нетачности и неконзистентности у подацима и информацијама.

Финансијска институција је дужна да обезбеди да сви пословно значајни системи за обраду података, као и систем извештавања, буду интегрални део информационог система.

4. Финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационог система, успостави, надзире, редовно ревидира и унапређује процес управљања овим системом ради смањења изложености ризицима и очувања безбедности и функционалности тог система, као и да унутрашњим општим актом, у складу са законом, утврди овлашћења и одговорности својих органа управљања и надзора који се односе на ове послове.

5. Финансијска институција је дужна да, у складу са стратегијом пословања, као и с природом, обимом и сложеношћу пословања, донесе стратегију развоја информационог система.

У складу са стратегијом развоја информационог система, финансијска институција дужна је да донесе одговарајуће стратегијске и оперативне планове.

Финансијска институција је дужна да, по потреби, мења стратегију развоја информационог система, и то нарочито ако то захтевају одговарајуће измене и/или допуне стратегије пословања.

Финансијска институција је дужна да о свакој измени и/или допуни стратегије развоја информационог система обавести Народну банку Србије у року од 15 дана од дана њеног усвајања.

6. Финансијска институција је дужна да, ради адекватног управљања информационим системом, обезбеди одговарајућу организациону структуру, с јасно утврђеном поделом послова и дужности запослених, односно са утврђеним унутрашњим контролама којима се спречава сукоб интереса.

Финансијска институција је у оквиру поделе послова и дужности из става 1. ове тачке нарочито дужна да јасно утврди послове и дужности запослених који су у непосредној вези са ефикасним и одговарајућим управљањем безбедношћу информационог система.

7. Финансијска институција је дужна да обезбеди примену свих унутрашњих општих аката и процедура у вези са информационим системом, као и да обезбеди да сви корисници овог система буду упознати са садржајем тих аката и процедура, у складу с њиховим овлашћењима, одговорностима и потребама.

8. Финансијска институција је дужна да усвоји и документује одговарајућу методологију којом ће се утврдити критеријуми, начин и поступци управљања пројектима у вези са информационим системом.

9. Финансијска институција је дужна да утврди критеријуме, начин и поступке извештавања свог надлежног органа о релевантним чињеницама у вези с функционалношћу и безбедношћу информационог система.

III. УПРАВЉАЊЕ РИЗИКОМ ИНФОРМАЦИОНОГ СИСТЕМА

10. Одредбе прописа којима се уређују општи услови и начин управљања ризицима у пословању финансијских институција примењују се и на управљање ризиком информационог система, осим ако овом одлуком није друкчије уређено.

11. Финансијска институција је дужна да, у оквиру свеобухватног система управљања ризицима, успостави процес управљања ризиком информационог система који обухвата идентификовање и мерење, односно процену тог ризика, као и његово ублажавање, праћење и контролу.

12. Финансијска институција је дужна да ризиком информационог система управља тако да омогући несметано управљање безбедношћу овог система и управљање континуитетом пословања финансијске институције.

Управљање ризиком информационог система мора да обухвати целокупан информациони систем финансијске институције и да буде интегрисано у све фазе развоја тог система.

13. Финансијска институција је дужна да адекватно управља ризицима који произлазе из уговорних односа с правним и физичким лицима чије се активности односе на њен информациони систем.

Финансијска институција је дужна да континуирано надзире начин и квалитет уговорених активности из става 1. ове тачке.

IV. УНУТРАШЊА РЕВИЗИЈА ИНФОРМАЦИОНОГ СИСТЕМА

14. Финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационог система, методологијом рада унутрашње ревизије обухвати критеријуме, начин и поступке унутрашње ревизије тог система засноване на резултатима процене ризика.

15. Унутрашња ревизија информационог система финансијске институције обавља се у складу с прописима којима се уређује пословање финансијских институција.

V. БЕЗБЕДНОСТ ИНФОРМАЦИОНОГ СИСТЕМА

16. Финансијска институција је дужна да, у складу са сложеношћу информационог система, донесе унутрашњи општи акт којим ће се успоставити оквир за управљање безбедношћу тог система (у даљем тексту: политика безбедности информационог система).

Политиком безбедности информационог система нарочито се уређују принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности овог система, као и овлашћења и одговорности у вези са овом безбедношћу и ресурсима тог система.

Финансијска институција је дужна да политику безбедности информационог система усклађује с променама у окружењу и у самом информационом систему.

17. Финансијска институција је дужна да процес управљања безбедношћу информационог система успостави као континуирани процес идентификовања потреба за овом безбедношћу и постизања и одржавања адекватног нивоа те безбедности.

Финансијска институција је дужна да, у складу с природом, обимом и сложеношћу пословања, као и сложеношћу информационог система:

1) поделу послова у вези са безбедношћу тог система изврши тако да се у унутрашњим актима којима се уређује организација њеног пословања јасно могу утврдити послови и дужности запослених у вези с том безбедношћу;

2) одреди кључне запослене задужене за безбедност информационог система водећи рачуна о томе да њихова позиција има значајан утицај на активности и доношење одлука у вези с том безбедношћу;

3) у управљање безбедношћу информационог система укључи довољан број запослених који имају одговарајућу стручност и професионално искуство.

Финансијска институција је дужна да идентификује и прати потребе за безбедношћу информационог система, и то најмање на основу резултата процене ризика тог система и обавеза које произлазе из прописа, унутрашњих општих аката, уговорних односа и сл.

18. Финансијска институција је дужна да, ради постизања и одржавања адекватног нивоа безбедности информационог система, успостави одговарајуће контроле.

19. Финансијска институција је дужна да унутрашњим актима утврди ближе критеријуме, начин и поступке за класификацију информационих добара према степену осетљивости и критичности – с обзиром на могуће последице нарушавања њихове поверљивости, интегритета и расположивости, да доследно примењује ту класификацију, као и да у складу с тим обезбеди адекватан ниво заштите ових добара.

Финансијска институција је дужна да именује лице, односно лица запослена у тој институцији која ће бити одговорна за управљање информационим добрима, те за класификацију и заштиту ових добара.

20. Финансијска институција је дужна да спроводи одговарајућу контролу приступа ресурсима информационог система, као и да с тим у вези успостави адекватан систем управљања корисничким правима приступа.

Системом управљања корисничким правима приступа нарочито се обухватају процеси евидентирања корисника информационог система, ауторизације, идентификације и аутентификације, као и надзор над корисничким правима приступа.

Финансијска институција је дужна да обезбеди да се ауторизација корисника информационог система заснива на принципу доделе најмањих могућих права приступа ресурсима тог система која омогућују ефикасно обављање послова.

Финансијска институција је дужна да периодично и по потреби, а најмање једном годишње, ревидира корисничка права приступа.

При управљању корисничким правима приступа, финансијска институција је дужна да посебно уреди повлашћени и удаљени приступ информационом систему.

21. Финансијска институција је дужна да, на основу резултата процене ризика информационог система, успостави адекватан систем надгледања тог система и генерисања оперативних и системских записа.

Финансијска институција је дужна да обезбеди одговарајућу заштиту записа из става 1. ове тачке, као и да утврди време чувања, те учесталост, опсег и начин праћења тих записа.

Записи из става 1. ове тачке морају садржати довољну количину информација ради идентификовања проблема, реконструисања догађаја и откривања неовлашћених приступа и активности на ресурсима информационог система, као и ради утврђивања одговорности с тим у вези.

22. Финансијска институција је дужна да, применом одговарајућих контрола, ресурсе информационог система и друге системе који су подршка функционисању информационог система заштити од неовлашћеног физичког приступа, од крађе, као и од физичког оштећења или уништења изазваног људским или природним фактором.

Финансијска институција је нарочито дужна да обезбеди интегритет података о платним трансакцијама при њиховој обради, чувању и предузимању свих других радњи у вези с тим подацима.

23. Финансијска институција је дужна да, применом одговарајућих контрола, ресурсе информационог система заштити од малициозног програмског кôда.

VI. УПРАВЉАЊЕ КОНТИНУИТЕТОМ ПОСЛОВАЊА И ОПОРАВАК АКТИВНОСТИ У СЛУЧАЈУ КАТАСТРОФА

24. Финансијска институција је дужна да, ради обезбеђивања несметаног и континуираног функционисања свих својих значајних система и процеса, као и ограничавања губитака у ванредним ситуацијама, успостави процес управљања континуитетом пословања.

25. Финансијска институција је дужна да обезбеди да управљање континуитетом пословања буде засновано на анализи утицаја на пословање и на процени ризика, које нарочито обухватају:

1) утврђивање ресурса и система потребних за одвијање појединачних пословних процеса, као и њихове међузависности и повезаности;
2) процену ризика у вези с појединачним пословним процесима, укључујући и вероватноћу настанка нежељених догађаја и њихов потенцијални утицај на континуитет пословања, финансијско стање и репутацију финансијске институције;
3) утврђивање прихватљивих нивоа ризика и техника за ублажавање идентификованих ризика;
4) утврђивање најдужег прихватљивог прекида (*MAO*) појединачних пословних процеса;
5) утврђивање критичних/кључних пословних процеса и активности.

Финансијска институција је дужна да, у складу са спроведеним активностима из става 1. ове тачке, усвоји стратегију опоравка коју ће применити у случају прекида пословања, а која нарочито садржи:

1) приоритете опоравка пословних процеса, као и ресурса и система потребних за њихово одвијање;
2) циљне нивое активности (*SDO*);
3) циљна времена опоравка (*RTO*);
4) циљне тачке опоравка (*RPO*).

26. Управни одбор банке и даваоца финансијског лизинга, односно надлежни орган друштва за осигурање, друштва за управљање добровољним пензијским фондом, платне институције, институције електронског новца и јавног поштанског оператора дужан је да, на основу активности спроведених у складу с тачком 25. ове одлуке, донесе план континуитета пословања (*Business Continuity Plan*), као и план опоравка активности у случају катастрофа (*Disaster Recovery Plan*) којим се превасходно уређује стварање услова за опоравак и расположивост ресурса информационог система потребних за одвијање критичних/кључних пословних процеса.

План континуитета пословања нарочито садржи:

1) опис процедура у случају прекида пословања;
2) ажуран списак свих ресурса неопходних за поновно успостављање континуитета пословања;

3) податке о тимовима који ће бити одговорни за поновно успостављање пословања у случају настанка непредвиђених догађаја и о именованим члановима тих тимова, укључујући и њихове јасно утврђене дужности и одговорности, као и план унутрашњих и спољних линија комуникације;

4) резервну локацију – у случају прекида пословања и немогућности поновног успостављања пословних процеса на примарној локацији.

План опоравка активности у случају катастрофа нарочито садржи:

1) процедуре за опоравак информационог система кад наступе катастрофални догађаји;

2) приоритете опоравка ресурса информационог система;

3) податке о тимовима који ће бити одговорни за опоравак информационог система и о именованим члановима тих тимова, укључујући и њихове јасно утврђене дужности и одговорности;

4) резервну локацију за опоравак информационог система, односно локацију резервног рачунарског центра.

Финансијска институција је дужна да, ради ефикасног спровођења планова из става 1. ове тачке, обезбеди да сви запослени буду упознати са својим улогама и одговорностима у случају наступања ванредних ситуација.

Финансијска институција је дужна да предузима све неопходне активности ради усклађивања планова из става 1. ове тачке с пословним променама, укључујући и промене у производима, активностима, процесима и системима, с променама у окружењу, као и с пословном политиком и стратегијом пословања.

Финансијска институција је дужна да, периодично и после настанка значајних промена, а најмање једном годишње, тестира планове из става 1. ове тачке, као и да документује резултате тих тестирања и обезбеди њихово укључивање у извештавање надлежног органа финансијске институције.

За спровођење планова из става 1. ове тачке, као и одредаба ст. од 4. до 6. те тачке, одговоран је извршни одбор банке и даваоца финансијског лизинга, односно надлежни орган друштва за осигурање, друштва за управљање добровољним пензијским фондом, платне институције, институције електронског новца и јавног поштанског оператора који, у складу са законом, води послове друштва.

27. Финансијска институција је дужна да, при управљању континуитетом пословања, узме у обзир и активности поверене трећим лицима и зависност од услуга тих лица.

28. Финансијска институција је дужна да, у случају настанка околности које захтевају примену плана континуитета пословања и плана опоравка активности у случају катастрофа, обавести о томе Народну банку Србије, и то најкасније наредног дана од дана настанка тих околности. Народна банка Србије може захтевати додатну документацију у вези с релевантним чињеницама о овим околностима и одредити рок за достављање те документације.

29. Финансијска институција је дужна да успостави процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности ресурса информационог система.

Финансијска институција је дужна да Народну банку Србије обавести у случају инцидента који је озбиљно угрозио или нарушио њено пословање, односно који би могао озбиљно угрозити или нарушити њено пословање, и то:

1) ако је настао услед нарушавања функционалности ресурса информационог система – одмах по утврђивању околности о настанку тог инцидента;
2) ако је настао као последица нарушавања безбедности информационог система – одмах по сазнању о том инциденту;
3) ако је настао код пружаоца услуге, а имао је или је могао имати значајан утицај на информациони систем финансијске институције – одмах по утврђивању околности о настанку тог инцидента, односно сазнању о том инциденту.“.

Након обавештења из става 2. ове тачке, ако је инцидент и даље у току, финансијска институција је дужна да Народну банку Србије континуирано обавештава о битним догађајима и другим релевантним информацијама у вези са инцидентом (статус инцидента), као и о активностима предузетим ради ублажавања инцидента и његовим последицама. Ово обавештење садржи и детаљан опис инцидента, информације о процени броја корисника на које је инцидент утицао, оквирно време потребно да се инцидент реши, потенцијални утицај на друге финансијске институције, као и битне догађаје и друге релевантне информације од настанка инцидента (нпр. информације о томе да ли је инцидент ескалирао, да ли су откривени нови узроци и о ефикасности примењених активности).

Финансијска институција је дужна да Народној банци Србије достави завршни извештај о насталом инциденту у року од 15 дана од дана престанка инцидента, односно од дана када процени да су успостављени редовно пословање финансијске институције и стабилан рад информационог система. Овај извештај садржи коначне информације о инциденту – датум почетка и датум окончања инцидента, дужина трајања инцидента, врста инцидента (недоступност хардверских компоненти, проблеми у раду софтверских компоненти или безбедносни инцидент), опис инцидента, узроци настанка и последице инцидента, активности које је финансијска институција спроводила током инцидента, план активности којима ће превентивно деловати и спречити поновне појаве истог инцидента, број корисника на које је инцидент утицао, настали финансијски трошкови повезани са инцидентом, утицај на друге финансијске институције и, по потреби, друге релевантне информације.

29а. Финансијска институција је дужна да тромесечно извештава Народну банку Србије о инцидентима који су повезани са злоупотребом осетљивих података корисника финансијских услуга, неодобреним платним трансакцијама, злоупотребом, крађом или губитком платних инструмената, укључујући коришћење техничких манипулација на банкоматима (АТМ), преварним радњама и злоупотребама корисника финансијских услуга, злоупотребама фактора аутентификације и система за аутентификацију и сл. а који нису имали директан утицај на њен информациони систем.

Извештај из става 1. ове тачке доставља се најкасније 10. у првом месецу тромесечја, а Народна банка Србије може ближе уредити начин достављања овог извештаја.

30. Финансијска институција је дужна да успостави процес управљања резервним копијама података, те да у ту сврху утврди детаљне процедуре и одговорности.

Управљање резервним копијама података мора да обухвати поступке израде, чувања и тестирања ових копија, као и опоравка података и софтверских компонената, како би се омогућило поновно успостављање пословних процеса у оквиру циљног времена опоравка.

Финансијска институција је дужна да обезбеди да су резервне копије података ажурне и адекватно заштићене, а поступци опоравка тестирани и успешни.

Најмање једна ажурна и комплетна резервна копија података мора бити адекватно ускладиштена на одговарајућој удаљености од примарне локације – на основу резултата процене ризика

информационог система и уз узимање у обзир потребе за избегавањем утицаја истих ризика на обе локације.

31. Финансијска институција је дужна да, на основу активности спроведених у складу с тачком 25. ове одлуке, обезбеди расположивост резервног рачунарског центра и његову адекватну опремљеност, функционалност и ниво безбедности, као и његову одговарајућу удаљеност од примарног рачунарског центра, уз узимање у обзир потребе за избегавањем утицаја истих ризика на обе локације.

VII. РАЗВОЈ И ОДРЖАВАЊЕ ИНФОРМАЦИОНОГ СИСТЕМА

32. Финансијска институција је дужна да успостави процес развоја информационог система у складу с релевантним променама унутар финансијске институције и у окружењу, како би се обезбедила континуирана адекватност тог система.

33. Финансијска институција процес развоја информационог система спроводи у складу са усвојеном стратегијом развоја информационог система и методологијом управљања пројектима, уз узимање у обзир функционалних захтева и потреба за безбедношћу.

Финансијска институција је дужна да, током развоја информационог система унутар финансијске институције, успостави и документује процес тог развоја, који обухвата анализу и пројектовање, програмирање, тестирање и увођење у продукцију.

Финансијска институција је дужна да на одговарајући начин раздвоји развојно, тестно и продукционо окружење.

34. Финансијска институција је дужна да успостави процес управљања хардверским и софтверским компонентама у свим фазама њиховог животног циклуса – од набавке или развоја до повлачења из употребе.

Финансијска институција је дужна да обезбеди да управљање хардверским и софтверским компонентама обухвати, између осталог, одржавање детаљне и ажурне евиденције ових компонената, именовање лица запосленог, односно запослених у финансијској институцији одговорних за управљање и заштиту тих компонената, као и утврђивање правила њиховог прихватљивог коришћења и безбедног одлагања при повлачењу из употребе.

35. Финансијска институција је дужна да обезбеди адекватно одржавање хардверских и софтверских компонената информационог

система према препорукама произвођача и да чува записе о том одржавању, као и да се стара о томе да се притом не угрози безбедност или функционалност овог система.

36. Финансијска институција је дужна да успостави процес управљања променама хардверских и софтверских компонената информационог система како би се избегло да оне доведу до неочекиваног и нежељеног понашања овог система, односно наруше његову безбедност или функционалност.

Управљање променама софтверских компонената информационог система обухвата нарочито следеће поступке:

1) утврђивање почетних верзија ових компонената;
2) иницирање, анализу и одобравање захтева за променом;
3) хронолошко документовање свих промена ових компонената и архитектуре база података, заједно с временом настанка промене;
4) информисање корисника информационог система о детаљима извршених промена.

Финансијска институција је дужна да обезбеди да све промене хардверских и софтверских компонената, укључујући и нове компоненте и системе, буду тестиране и одобрене пре пуштања у продукцијски рад, као и да утврди план враћања на претходно стање.

Финансијска институција је дужна да унутрашњим општим актом уреди процес управљања хитним променама хардверских и софтверских компонената информационог система.

37. Финансијска институција која планира миграцију података на нови систем главних пословних апликација (*core business application*) или у други рачунарски центар, односно која врши промену локације рачунарског центра, дужна је да о томе обавести Народну банку Србије најкасније 30 дана пре почетка тестирања планираног у вези с том миграцијом.

Обавештење из става 1. ове тачке нарочито садржи:

1) детаљне описе система између којих се подаци преносе;
2) план, динамику и опис активности у вези с миграцијом података, укључујући и методологију тестирања;
3) резултате процене ризика и опис контрола које ће се применити током миграције података с циљем очувања поверљивости, интегритета и расположивости података;

4) план враћања на стање пре миграције података, који укључује динамику тог враћања и опис активности, као и критеријуме за доношење одлуке за примену овог плана.

Изузетно од става 1. ове тачке, финансијска институција која планира миграцију података због статусне промене за коју је дужна да прибави претходну сагласност, односно дозволу Народне банке Србије дужна је да, истовремено са захтевом за давање ове сагласности, односно дозволе, Народној банци Србије достави и обавештење с подацима из става 2. те тачке, а банка је дужна да достави и захтев за омогућавање функционисања привременог рачуна правног следбеника (у даљем тексту: захтев за привремени рачун) који мора потписати законски заступник правног следбеника – ради поступања Народне банке Србије по том захтеву у случајевима утврђеним овом тачком.

Привремени рачун правног следбеника представља рачун банке која престаје да постоји због статусне промене који је отворен у Народној банци Србије у складу с прописима, односно правилима рада платног система у којем та банка учествује а који због статусне промене преузима правни следбеник, ради његовог привременог функционисања у року утврђеном овом одлуком.

Финансијска институција која донесе одлуку о примени плана враћања на стање пре миграције података дужна је да о томе без одлагања обавести Народну банку Србије.

Ако донесе одлуку о примени плана враћања на стање пре миграције података због статусне промене, банка је дужна да о томе обавести Народну банку Србије најкасније наредног радног дана од дана када је започела миграцију података, и то најкасније један сат пре почетка периода утврђеног Дневним терминским планом рада RTGS платног система Народне банке Србије (у даљем тексту: RTGS НБС систем) за извршавање налога за пренос у том систему.

Народна банка Србије омогућава функционисање привременог рачуна из става 4. ове тачке у случају да банка донесе одлуку о примени плана враћања на стање пре миграције података.

Изузетно од става 7. ове тачке, ако постоје објективне околности услед којих могу бити угрожени интереси клијената банке која спроводи поступак миграције података због статусне промене, Народна банка Србије може, на образложени захтев који банка доставља уз документацију из става 3. ове тачке, посебно утврдити рок спровођења поступка миграције података и омогућити функционисање привременог рачуна у том року.

Финансијска институција је дужна да поступак миграције података због статусне промене спроведе најкасније у року од десет радних дана од дана почетка примене плана из става 5. ове тачке, односно у року који утврди Народна банка Србије у складу са ставом 8. ове тачке.

Привремени рачун правног следбеника из ове тачке, као и поступање Народне банке Србије у складу са захтевом за привремени рачун ближе се уређују правилима рада RTGS НБС система.

38. Финансијска институција је дужна да обезбеди израду, чување и редовно одржавање документације која се односи на информациони систем, како би та документација у сваком тренутку била тачна, потпуна и ажурна.

Финансијска институција је дужна да свим корисницима информационог система обезбеди приступ одговарајућим документима у складу с потребама посла.

39. Финансијска институција је дужна да обезбеди адекватно, континуирано стручно оспособљавање и обучавање запослених за коришћење информационог система и очување његове безбедности и функционалности.

VIII. ПОВЕРАВАЊЕ АКТИВНОСТИ У ВЕЗИ СА ИНФОРМАЦИОНИМ СИСТЕМОМ ТРЕЋИМ ЛИЦИМА

40. Поверавање активности у вези са информационим системом финансијске институције трећим лицима (у даљем тексту: поверавање активности) обавља се у складу с прописима којима се уређује пословање финансијских институција, осим ако овом одлуком није друкчије прописано.

Активностима из става 1. ове тачке сматрају се све активности које обухватају обраду, чување и/или приступ подацима којима располаже финансијска институција а односе се на њено пословање, као и активности развоја и/или одржавања главних пословних апликација.

Поверавање активности укључује и поверавање активности лицима повезаним с финансијском институцијом имовинским и управљачким односима (лица са учешћем, чланице групе друштава којој та институција припада и др.) која послују у Републици Србији или у иностранству.

Поверавањем активности не сматра се коришћење стандардизованих сервиса (*SWIFT*, *Bloomberg*, *Reuters* и др.) или телекомуникационих услуга, као ни набавка софтвера који је као готово решење комерцијално доступан на тржишту (*off-the-shelf*) и сл.

Поверавање активности врши се на основу уговора закљученог између финансијске институције и лица коме се те активности поверавају (у даљем тексту: пружалац услуга).

41. Финансијска институција која одређене активности намерава да повери дужна је да уреди:

1) процес одлучивања о поверавању активности и критеријуме за доношење те одлуке;
2) начин укључивања тих активности у процес управљања ризицима и у систем интерног извештавања о ризицима;
3) начин на који обезбеђује континуитет обављања активности које је поверила и мере које предузима у случају раскида уговорног односа с пружаоцима услуга, као и у случају привременог застоја или престанка пружања тих услуга;
4) начин вршења надзора над обављањем активности које је поверила, укључујући и надзор над усклађеношћу тих активности с прописима, добрим пословним обичајима и општеприхваћеним стандардима из одговарајуће области.

Банка која намерава да трећем лицу повери активности чије је извршење значајно за обезбеђивање континуитета њених критичних функција, дужна је да обезбеди континуитет тих функција за случај примене инструмената и/или мера реструктурирања, на један од следећих начина:

1) обавезивањем тог лица да обавља поверене активности у свим ситуацијама у којима је потребно обезбедити континуитет критичних функција банке у реструктурирању, односно банке за посебне намене;
2) уговором са алтернативним добављачем који би могао да обезбеди континуитет обављања критичних функција банке у реструктурирању, односно банке за посебне намене;
3) детаљним планом обезбеђивања континуитета обављања критичних функција употребом интерно расположивих ресурса банке у реструктурирању, односно банке за посебне намене.

42. Пре доношења одлуке о сваком појединачном поверавању активности, односно о промени пружаоца услуга – финансијска институција је дужна да:

1) изврши детаљну анализу потенцијалног пружаоца услуга која се односи на његову способност пружања услуга, финансијско стање и пословну репутацију;

2) утврди да ли прописи државе или држава у којима потенцијални пружалац услуга послује омогућују Народној банци Србије несметано вршење непосредне контроле тог пословања у делу који се односи на обављање поверених активности или је у вези с тим активностима;

3) процени могуће потешкоће и време потребно за избор другог пружаоца услуга, или могућност наставка обављања тих активности унутар финансијске институције у случају престанка пружања уговорених услуга, као и да с тим у вези донесе одговарајућу излазну стратегију, која мора да садржи списак мера и активности које је потребно предузети, као и динамику њиховог спровођења од тренутка престанка пружања уговорених услуга до избора другог пружаоца услуга или потпуног успостављања процеса обављања тих активности унутар финансијске институције.

При доношењу одлуке из става 1. ове тачке, финансијска институција нарочито процењује утицај поверавања активности на:

1) континуитет пословања и репутацију финансијске институције;

2) трошкове, финансијски резултат, ликвидност и солвентност финансијске институције;

3) ризични профил финансијске институције;

4) квалитет услуга које финансијска институција пружа клијентима.

43. Финансијска институција је дужна да обезбеди да пружалац услуга њој, спољном ревизору и Народној банци Србије омогући благовремен и неограничен приступ документацији и подацима у вези с повереним активностима.

Финансијска институција је дужна да обезбеди да сваки уговор закључен с пружаоцем услуга садржи одредбу којом се пружалац услуга обавезује да испуни обавезу из става 1. ове тачке, као и одредбу која финансијској институцији омогућава да једнострано раскине овај уговор ако то наложи Народна банка Србије и у складу с тим налогом.

Финансијска институција је дужна да Народној банци Србије омогући и несметано вршење непосредне контроле обављања поверених активности у просторијама пружаоца услуга, односно на локацији на којој се поверене активности обављају.

44. Финансијска институција је дужна да обезбеди да се поверавањем активности не угрози безбедност или функционалност информационог система, као и да подаци финансијске институције остану у њеном поседу.

Финансијска институција је дужна да обезбеди да пружалац услуга поверене активности обавља у складу са политиком безбедности информационог система и другим актима финансијске институције којима се уређује безбедност њеног информационог система.

Финансијска институција и пружалац услуга дужни су да при поверавању активности, односно обављању поверених активности поступају у складу са законом којим се уређује заштита података о личности, као и другим прописима којима се уређује чување тајне настале у пословању финансијских институција.

45. Финансијска институција може одређене активности да повери, односно пружаоца услуга да промени само ако о томе обавести Народну банку Србије најкасније 30 дана пре закључења уговора о поверавању активности.

Ако се мења уговор из става 1. ове тачке а да се при томе не мења поверена активност, односно пружалац услуга или се не утиче на резултате анализе из тачке 42. став 1. одредба под 1) ове одлуке, односно на резултате процене из тачке 42. став 2. те одлуке – финансијска институција је дужна да најкасније 15 дана пре закључења анекса тог уговора о томе обавести Народну банку Србије и достави јој нацрт тог анекса.

Обавештење из става 1. ове тачке нарочито садржи:

1) одлуку надлежног органа управљања финансијском институцијом о поверавању активности, односно о промени пружаоца услуга;
2) опис активности које финансијска институција намерава да повери, обавезе и услове које је пружалац услуга дужан да испуни, као и рок на који ће активности бити поверене;
3) основне податке о пружаоцу услуга (пословно име, седиште, матични број и ПИБ, односно други одговарајући подаци за страног пружаоца услуга);
4) резултате анализе из тачке 42. став 1. одредба под 1) ове одлуке;
5) излазну стратегију из тачке 42. став 1. одредба под 3) ове одлуке;
6) резултате процене из тачке 42. став 2. ове одлуке;

7) нацрт уговора о поверавању активности;

8) доказ о томе да прописи државе, односно држава у којима пружалац услуга послује омогућавају Народној банци Србије да несметано врши непосредну контролу пословања у делу који се односи на обављање поверених активности или је у вези с њима – ако пружалац услуга има седиште изван Републике Србије или је уговорено да поверене активности обавља изван Републике Србије.

Рок из става 1. ове тачке рачуна се од дана достављања уредне документације из те тачке.

46. *Брисана је.*

47. Пружалац услуга може другом лицу поверити активности које је финансијска институција њему поверила или друге послове који су у вези с тим активностима само уз претходну сагласност финансијске институције, коју она даје у сваком појединачном случају, уз сходну примену одредаба тач. од 41. до 44. ове одлуке.

Финансијска институција може сагласност из става 1. ове тачке дати само ако је најкасније 30 дана пре тога обавестила Народну банку Србије о намераваном поверавању активности или послова из тог става.

Обавештење из става 2. ове тачке нарочито садржи:

1) нацрт одлуке надлежног органа управљања финансијском институцијом о давању сагласности из става 1. ове тачке;

2) опис активности које пружалац услуга намерава да повери, као и обавеза и услова које је друго лице из става 1. ове тачке дужно да испуни;

3) основне податке о другом лицу из става 1. ове тачке (пословно име, седиште, матични број и ПИБ, односно други одговарајући подаци за страно лице);

4) резултате анализе из тачке 42. став 1. одредба под 1) ове одлуке;

5) ревидирану излазну стратегију из тачке 42. став 1. одредба под 3) ове одлуке;

6) резултате процене из тачке 42. став 2. ове одлуке;

7) нацрт уговора између пружаоца услуга и другог лица из става 1. ове тачке о поверавању активности из тог става;

8) доказ о томе да прописи државе, односно држава у којима друго лице из става 1. ове тачке послује омогућавају Народној банци Србије несметано вршење непосредне контроле пословања у делу који се односи на обављање поверених активности или је у вези с њима – ако то лице има седиште изван Републике Србије или је уговорено да поверене активности обавља изван Републике Србије.

Рок из става 2. ове тачке рачуна се од дана достављања уредне документације из те тачке.

48. Финансијска институција одговара у целини за активности које је поверила пружаоцима услуга.

Финансијска институција је дужна да континуирано врши надзор над пруженим услугама, као и проверу квалитета пружених услуга у вези с повереним активностима.

Ако у поступку контроле, односно надзора утврди да финансијска институција, због пропуста у раду пружаоца услуга или другог лица из тачке 47. ове одлуке, не поступа у складу са овом одлуком и другим прописима – Народна банка Србије може финансијској институцији наложити да раскине уговор о поверавању активности закључен с пружаоцем услуга.

48а. Финансијска институција је дужна да Народној банци Србије достави уговор из тачке 40. став 5. ове одлуке, укључујући и анексе тог уговора – у року од 15 дана од дана закључења тог уговора, односно анекса.

У случају раскида уговора из става 1. ове тачке, финансијска институција о томе без одлагања обавештава Народну банку Србије.

IX. ЕЛЕКТРОНСКЕ УСЛУГЕ

49. Банка, платна институција, институција електронског новца и јавни поштански оператор који пружају електронске услуге (у даљем тексту: пружалац електронских услуга) дужни су да, као саставни део управљања ризиком информационог система, успоставе процес управљања ризицима који произлазе из пружања електронских услуга.

50. Пружалац електронских услуга дужан је да при пружању електронских услуга примени безбедне и ефикасне методе за проверу и потврду идентитета и овлашћења лица, процеса и система.

Пружалац електронских услуга дужан је да корисницима при коришћењу ових услуга обезбеди аутентификацију која укључује комбинацију најмање два међусобно независна елемента за потврђивање корисничког идентитета.

Изузетно од става 2. ове тачке, пружалац електронских услуга може применити аутентификацију корисника која се врши коришћењем једног елемента за потврђивање корисничког идентитета, у случају:

1) плаћања мале новчане вредности, у складу са оквирним уговором о платним услугама, под условом да се ризицима који се односе на укупан износ ових плаћања управља на одговарајући начин (нпр. утврђивање максималног износа ових трансакција у одређеном периоду након којих ће се спровести аутентификација у складу са ставом 2. ове тачке или предузети додатне мере заштите),

2) плаћања према примаоцима плаћања која је платилац унапред одредио (нпр. утврђивање тзв. беле листе примаоца плаћања),

3) пренос новчаних средстава између два платна рачуна истог корисника код истог пружаоца електронских услуга,

4) пренос електронског новца који се обавља у оквиру истог пружаоца електронских услуга, који је заснован на анализи ризика ових платних трансакција,

5) других трансакција и услуга које су на основу анализе ризика процењене као нискоризичне.

Пружалац електронских услуга може да примени аутентификацију корисника из става 3. ове тачке само ако је најмање 30 дана пре дана почетка пружања услуге о томе обавестио Народну банку Србије и уз то обавештење доставио свеобухватну и детаљну анализу ризика и начина управљања ризицима који произлазе из пружања услуга на начин утврђен у одредбама 1) до 5) тог става и другу одговарајућу документацију која се односи на ову анализу.

Анализа из става 4. ове тачке обухвата посебно и анализе из става 3. одредбе под 4) и 5) ове тачке, ако пружалац електронских услуга намерава да примени аутентификацију корисника коришћењем једног елемента за потврђивање корисничког идентитета у случајевима из тих одредаба.

Рок из става 4. ове тачке рачуна се од дана достављања уредне документације из тог става.

51. Пружалац електронских услуга дужан је да усвоји и примени правила којима се на одговарајући начин, у складу с тржишном праксом и проценом ризика, ограничава број покушаја пријаве на систем за пружање електронских услуга, односно покушаја аутентификације, да одреди најдуже време без активности корисника након пријаве на тај систем, као и да утврди рокове важења параметара аутентификације.

При коришћењу једнократних лозинки ради аутентификације (нпр. *One Time Password – OTP*), пружалац електронских услуга дужан је да обезбеди да временско важење те лозинке буде ограничено на период који је потребан за обављање аутентификације.

Пружалац електронских услуга дужан је да утврди највећи могући број неуспешних покушаја пријаве на систем за пружање електронских услуга након којих ће тај систем бити трајно или привремено блокиран, као и да успостави процедуре за безбедно поновно активирање овог система.

Пружалац електронских услуга дужан је да утврди најдуже могуће време без активности корисника на систему за пружање електронских услуга по пријављивању у тај систем, након којег долази до аутоматског одјављивања корисника из овог система (тзв. завршетак сесије).

Пружалац електронских услуга дужан је да обезбеди одговарајућу потврду свог идентитета на дистрибутивном каналу за пружање електронских услуга како би корисници могли да провере пружаоца електронске услуге.

Пружалац електронских услуга је дужан да обезбеди постојање оперативних и системских записа како би се у одговарајућој мери обезбедила непорецивост и доказивост радњи у вези са пружањем електронских услуга.

X. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

52. Друштво за осигурање, давалац финансијског лизинга и друштво за управљање добровољним пензијским фондом који до 30. јуна 2014. године повере трећем лицу одређене активности из тачке 40. ове одлуке, дужни су да, најкасније 31. јула 2014. године, о томе обавесте Народну банку Србије.

Уз обавештење из става 1. ове тачке, друштво за осигурање, давалац финансијског лизинга и друштво за управљање добровољним пензијским фондом дужни су да Народној банци Србије доставе документацију и податке утврђене у тачки 45. став 2. ове одлуке.

Банка која до 31. децембра 2013. године повери трећем лицу одређене активности из тачке 40. ове одлуке дужна је да Народној банци Србије, најкасније 31. јануара 2014. године, достави излазну стратегију из тачке 42. став 1. одредба под 3) те одлуке.

Ако треће лице из става 3. ове тачке има седиште изван Републике Србије или је уговорено да поверене активности обавља изван Републике Србије – банка је дужна да Народној банци Србије, уз излазну стратегију из става 3. ове тачке, достави и доказ из тачке 45. став 2. одредба под 8) ове одлуке.

53. Тач. 17. и 18. и тач. од 68. до 72. Одлуке о управљању ризицима банке („Службени гласник РС“, бр. 45/2011, 94/2011, 119/2012 и 123/2012) престају да важе 1. јануара 2014. године.

Тач. 6. и 8. Одлуке о минималним условима организационе и техничке оспособљености друштва за управљање добровољним пензијским фондом („Службени гласник РС“, бр. 23/2006) престају да важе 1. јула 2014. године.

54. Ова одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику РС“ и примењиваће се од 1. јануара 2014. године на банке, а од 1. јула 2014. године на друштва за осигурање, даваоце финансијског лизинга и друштва за управљање добровољним пензијским фондовима.

ИО НБС бр. 7
12. марта 2013. године
Б е о г р а д

Председавајућа
Извршног одбора Народне банке Србије
Г у в е р н е р
Народне банке Србије

др Јоргованка Табаковић, с.р.