НАРОДНА БАНКА НА РЕПУБЛИКА МАКЕДОНИЈА

Врз основа на член 47 став 1 точка 6 од Законот за Народната банка на Република Македонија („Службен весник на Република Македонија" бр. 158/10, 123/12, 43/14, 153/15, 6/16) и член 68 став 1 точка 6 од Законот за банките („Службен весник на Република Македонија" бр. 67/07, 90/09, 67/10, 26/13, 15/15, 153/15 и 190/16), а во врска со член 48 став 1 точка 6 од Законот за Народната банка на Република Македонија, Советот на Народната банка на Република Македонија донесе

О Д Л У К А
за Методологијата за сигурност на информативниот систем на банката („Службен весник на Република Македонија" бр. 78/18)

I. ОПШТИ ОДРЕДБИ

1. Со оваа одлука се пропишува Методологијата за сигурноста на информативниот систем на банката којашто се состои од правила за воспоставување процес за управување со сигурноста на информативниот систем, планирање, развој и спроведување на стратегијата за управување со информативната технологија, за обезбедување непрекинатост во работењето, како и сигурносни правила во однос на системите за современи канали и друштвата за услуги на банката за информативниот систем.

2. Под сигурност на информативниот систем на банката, според оваа одлука, се подразбира исполнување на следниве принципи:

- **Доверливост**: информативниот систем е достапен само за корисниците кои имаат овластен пристап до него;
- **Интегритет**: заштита на точноста и комплетноста на информативниот систем;
- **Расположливост**: непречен пристап до информативниот систем за овластените корисници.

II. ДЕФИНИЦИИ

3. Одделни изрази употребени во оваа одлука го имаат следново значење:

3.1. „Ризик од несоодветност на информативните системи" е ризикот од загуба за банката поради губење, неовластено користење или нерасположливост на информациите, информативните средства и/или услугите што ги нуди банката.

3.2. Под „информативни средства" се подразбираат информациите без оглед на кој медиум се сместени заедно со софтверските и хардверските компоненти преку кои се остварува пристап до нив, нивна обработка, пренос и чување.

3.3. Под „административни сигурносни контроли" се подразбираат политиките, правилата, упатствата и процедурите донесени од страна на органите на банката преку кои се воспоставува процесот за управување со сигурноста на информативниот систем.

3.4. Под „технички сигурносни контроли" се подразбира употребата на сигурносни мерки коишто се вградени во компјутерската опрема, системскиот софтвер, комуникациската опрема и апликативните програмски решенија.

3.5. Под „физички сигурносни контроли" се подразбира преземањето соодветни мерки за ограничување и контрола на физичкиот пристап до информативните средства, за да се заштити банката од шпионажа, саботажа, пожар, поплава, вандализам, природна катастрофа и од друг вид на оштетување или уништување на целиот или на делови од информативниот систем.

3.6. Под „сигурност во дигиталниот простор" (англ. Cybersecurity) се дефинира способноста на банката да обезбеди заштита на информативните средства и телекомуникациските мрежи од напади коишто може да предизвикаат прекин, оневозможување, уништување или нивно злонамерно преземање со кое би се нарушила сигурноста на информативниот систем.

3.7. Под „ниво на подготвеност од нападите од дигиталниот простор" се подразбираат воспоставените практики, процеси и однесувања во банката коишто одговараат на соодветното ниво на инхерентен ризик за да ја поткрепат или да ја зголемат спремноста и отпорноста од нападите од дигиталниот простор.

3.8. Под „отпорност од напади од дигиталниот простор" се подразбира можноста на банката да ги предвиди, подготви и да се одбрани од нападите во дигиталниот простор и брзо да воспостави оперативност на нарушените деловни процеси.

3.9. „Тежок прекин на деловните процеси" претставува состојба во која банката не е способна да ги исполни преземените деловни обврски поради причини коишто не може да ги контролира, или во случаи кога банката е физички или телекомуникациски оштетена, односно не се достапни информациите и информативните системи на кои се одвиваат критичните операции на банката.

3.10. Под „целно време за обнова (англ. RTO – Recovery Time Objective)" се подразбира временски период во чии рамки е неопходно да се воспостават деловните процеси со соодветна технолошка поддршка, при појава на тежок прекин на деловните процеси.

3.11. Под „целна точка за обнова (англ. RPO – Recovery Point Objective)" се подразбира последната временска точка од која податоците може да бидат обновени и да се продолжи со деловниот процес при појава на тежок прекин на деловните процеси.

3.12. Под „системи на современи канали" се подразбираат системи преку кои се нудат банкарски услуги и производи преку интерактивни електронски комуникациски канали поврзани на јавни телекомуникациски мрежи, како што се далечински пристап до финансиски информации, информации за производи и услуги и извршување платежни трансакции.

3.13. „Платежна трансакција" претставува уплата, исплата или пренос на средства, коишто се иницирани од страна на плаќач или примач, независно од обврската помеѓу плаќачот и примачот.

3.14. „Платежна трансакција преку средства за далечинска комуникација" претставува платежна трансакција којашто е иницирана по пат на интернет или уред што може да се користи за далечинска комуникација.

3.15. Под „анализа на ризик на трансакција" се подразбира оценка на ризикот кон одредена трансакција којашто ги зема предвид следниве критериуми: карактеристиките на плаќање на клиентот и неговото поведение, вредноста на трансакцијата, видот на плаќањето и банкарскиот производ и профилот на примачот на плаќањето.

3.16. Под „персонализирани средства за сигурност" се подразбираат средства коишто се персонализираат од страна на банката за потребите на автентикација на корисникот при користење на системите за современи канали.

3.17. Под „значаен инцидент поврзан со сигурноста на плаќањето" се подразбира инцидент којшто има или може да има значителен одраз врз сигурноста и непрекинатоста во работењето на платниот систем на банката или на доверливоста на извршените плаќања и состојби на сметки. Проценката на материјалноста на инцидентот треба да ги земе предвид бројот на потенцијално погодени клиенти, износот и влијанието кон другите платежни системи и целокупната инфраструктура.

3.18. „Автентикација на корисник" претставува постапка којашто ѝ овозможува на банката да го потврди идентитетот на корисникот на современите канали, вклучувајќи ја и употребата на неговите персонализирани средства за сигурност.

3.19. „Следењето на платежните трансакции" се дефинира како системи и механизми за следење на трансакциите, нивна контрола и проценка од ризикот од измама и обезбедување доказ за трансфер на одредени

информации или дека трансакциите се извршени од авторизиран и овластен корисник.

3.20. „Чувствителни податоци за плаќањата" се податоците, вклучително и персонализираните средства за сигурност, коишто може да се употребат за да се изврши измама.

3.21. Под друштво за услуги на банката за информативниот систем се подразбира:

- друштво за помошни банкарски услуги чија основна дејност е управување и водење систем за обработка на податоци и коешто врз основа на писмен договор, обработува и чува податоци за банката при извршувањето на банкарските и финансиските активности; и/или
- надворешно лице, кое врз основа на писмен договор обработува и чува податоци за банката при извршувањето на банкарските и финансиските активности.

III. ПРОЦЕС ЗА УПРАВУВАЊЕ СО СИГУРНОСТА НА ИНФОРМАТИВНИОТ СИСТЕМ

4. Заради постигнување и постојано одржување на сигурноста на информативниот систем, Банката е должна да воспостави процес за управување со сигурноста на информативниот систем што опфаќа:
- Оценка на ризикот што во себе вклучува оценка на ризикот за информативната сигурност и оценка на ризикот од нападите од дигиталниот простор;
- Спроведување сигурносни контроли;
- Тестирање на сигурноста и тестирање на отпорноста на системите од напади од дигиталниот простор;
- Следење и надградба и
- Поделба на надлежностите на органите на банката од аспект на управувањето со сигурноста на информативниот систем.

5. Процесот за управување со сигурноста на информативниот систем од точка 4 од оваа одлука е дефиниран во Политиката за сигурност на информативниот систем на банката и треба да им одговара на природата, обемот и сложеноста на финансиските активности коишто ги врши и ризиците на коишто е изложена.

Оценка на ризикот за информативната сигурност и оценка на ризикот од нападите од дигиталниот простор

6. Оценката на ризикот за информативната сигурност треба да опфати:
- идентификација на средствата на информативниот систем на банката;
- класификација на средствата на информативниот систем на банката, односно доделување вредност на средствата според нивната значајност;
- анализа на веројатноста за појавата на закани и слабости на информативниот системот, земајќи ги предвид настанатите штетни настани и процесот на постојана анализа и следење на нови слабости во информативниот систем,

особено земајќи ги предвид резултатите од извршените тестирања од точките 9 и 10 од оваа одлука;
- доделување приоритет на ризиците во зависност од големината на потенцијалната загубата што може да ја предизвикаат за банката.

За извршената оценка на ризикот за информативниот систем банката е должна, најмалку еднаш годишно, да изработи сумарен извештај во кој ризиците ќе се категоризирани според табелата дадена во анексот 1 на оваа одлука.

7. Банката е должна да воспостави редовен процес на оценка на ризикот од нападите од дигиталниот простор и да утврди стратегија за обезбедување на нивото на подготвеност. Овој процес треба да ги содржи најмалку следниве елементи:
- фактори коишто придонесуваат кон зголемено ниво на ризик од заканите од дигиталниот простор;
- утврдување на нивото на подготвеност од нападите од дигиталниот простор и усогласување со ризикот од заканите од дигиталниот простор;
- предлагање корективни активности коишто се потребни за подобрување на нивото на подготвеност;
- воспоставување процес на размена на информации за навремено спречување на нападите од дигиталниот простор со други надворешни институции.

Оценката на ризиците од нападите од дигиталниот простор треба да се направи при појава на нови закани, при измени во деловниот модел на банката со воведување нови банкарски производи и услуги, значајни измени во организациската структура и ширење на други пазари и користење други надворешни лица и добавувачи.

Спроведување на сигурносните контроли

8. Банката е должна да ја донесе Политиката за сигурност на информативниот систем од точка 5 од оваа одлука којашто треба да ги содржи најмалку следниве елементи и сигурносни контроли:
- класификација на информациите и информативните средства според значајност;
- заштита на личните податоци, во согласност со важечките прописи во Република Македонија;
- методологија за спроведување на оценката на ризиците поврзани со сигурноста на информативниот систем во која се дефинирани нивоата на прифатливост на ризиците и методологија за оценка на ризиците од дигиталниот простор и утврдување на нивото на подготвеност од нападите од дигиталниот простор;
- начин на обезбедување сигурност во дигиталниот простор и план за отпорност од напади од дигиталниот простор;
- примена на стратегија на банката за управување со идентификуваните ризици и нивото на подготвеност од нападите од дигиталниот простор, преку воспоставување акциски план и буџет за обезбедување на сигурноста на информативниот систем;
- годишен план за обука за лицата со посебни права и одговорности, вработените и клиентите на банката, за правилно користење на услугите

коишто се достапни преку информативниот систем на банката и информирање за новите закани и измами коишто доаѓаат од дигиталниот простор;
- управување со различни нивоа на сигурносни инциденти и воспоставување соодветен механизам за нивното идентификување, пријавување и ефикасно отстранување на заканите за сигурноста на информативниот систем преку преземање соодветни активности;
- дефинирање на улогата на организациската единица за информациска технологија во банката, којашто е должна да поседува соодветен кадровски капацитет и интерни процедури за работа, во согласност со усвоените акти од областа на сигурноста на информативниот систем;
- дефинирање соодветна ревизорска трага за критичните делови од информативниот систем на повеќе нивоа, како што се оперативен систем, бази на податоци, телекомуникациска опрема, со цел да се потврди идентитетот и редоследот на активностите коишто се извршувале на информативниот систем;
- дефинирање на начинот на управување со сигурносните надградби, надградбите на нови верзии, промените во параметрите и кодовите на апликациите, подготовката и ставањето на апликациите во употреба;
- дефинирање на начинот на воспоставување план за непрекинатост во работењето на банката и соодветна заштита на податоците;
- начин на воспоставување антивирусна заштита, заштита од штетни програми и заштита на интегритетот на податоците;
- дефинирање на начинот на телекомуникациско поврзување и обезбедување заштита на податоците коишто се пренесуваат;
- дефинирање сигурносни зони во банката преку што ќе се ограничи физичкиот пристап до информациите и информативните средства на банката;
- дефинирање на начинот на воспоставување дополнителни безбедносни механизми, како што се противпожарна заштита, заштита од поплава, следење, сензори и аларми;
- дефинирање на улогата на внатрешната и надворешната ревизија во обезбедувањето на сигурноста на информативниот систем и
- дефинирање на дозволените исклучоци од Политиката, постапката за нивно одобрување и дефинирање прифатливо ниво на ризик од несоодветност на информативните системи.

За ефикасна примена на политиката од оваа точка, банката е должна да воспостави соодветни интерни акти.

Политиката треба да содржи опис на административните, техничките и физичките сигурносни контроли и начинот на нивната примена во банката.

Тестирање на сигурноста и тестирање на отпорноста на системите од напади од дигиталниот простор

9. Банката е должна да воспостави процес на професионално, независно и објективно тестирање на ефикасноста и на соодветноста на спроведените сигурносни контроли содржани во политиката за сигурност на информативниот систем.

10. Банката е должна најмалку еднаш на две години да спроведе професионално и независно тестирање на отпорноста на своите системи од напади од дигиталниот простор според реални сценарија и соодветни информации за да се потврди ефикасноста на спроведените контроли и соодветноста на нивото на подготвеност од нападите од дигиталниот простор.

Обемот, фреквенцијата и предметот на тестирање на отпорноста на системите треба да бидат определени во зависност од нивото на ризик од заканите од дигиталниот простор.

Следење и надградба

11. Банката е должна да воспостави процес преку кој постојано ќе ги прибира и ќе врши анализа на информациите за настанатите загуби како последица на сигурносни инциденти при работењето. Банката е должна да воспостави процес преку кој постојано ќе ги прибира и ќе врши анализа на информациите поврзани со нови слабости и закани за сигурноста на информативниот систем и ќе преземе активности за нивно надминување.

Поделба на надлежностите на органите на банката од аспект на управувањето со сигурноста на информативниот систем

12. Банката е должна да воспостави соодветна организациска поставеност за управување со сигурноста на информативниот систем, што подразбира јасно дефинирани надлежности и одговорности на органите на банката во процесот за управување со сигурноста на информативниот систем.

Надзорниот одбор е одговорен за усвојување на политиката за сигурност на информативниот систем и годишно следење на нејзиното спроведување.

Одборот за управување со ризиците е одговорен за воспоставување политика за сигурност на информативниот систем, следење на нејзината примена, анализирање на извештаите за изложеноста на ризик од несоодветност на информативниот систем и предлага стратегии, мерки и инструменти за заштита од ризиците.

Управниот одбор изготвува политика за сигурност на информативниот систем и е одговорен за управувањето и следењето на ризикот од несоодветност на информативниот систем на кои е изложена банката во работењето.

13. Заради управување со сигурноста на информативниот систем, Банката треба да именува лице одговорно за сигурноста на информативниот систем, кое ќе ги координира политиката за сигурност на информативниот систем и процесите поврзани со различните технолошки платформи и работни задачи.

Лицето од став 1 на оваа точка е должно да биде независно од лицата кои работат во организациските делови на банката што преземаат ризици поврзани со сигурноста на информативниот систем.

Лицето одговорното за сигурноста на информативниот систем, најмалку двапати годишно, го известува Надзорниот одбор за работите поврзани со сигурноста на информативниот систем.

14. Известувањето од точка 13 став 3 од оваа одлука треба да ги содржи најмалку следниве елементи:

- податоци за идентификуваните ризици и нивната контрола;
- регистрирани случаи на исклучоци од Политиката за сигурност на информативниот систем согласно со точка 8 став 1 алинеја 17 од оваа одлука, со посочување на ризиците;
- информации за договорите со друштвата за услуги на банката за информативниот систем;
- резултати од извршените тестирања на сигурноста на информативниот систем, сигурносни инциденти и соодветни реакции од страна на органите на банката и
- идентификувани потреби за промените во политиката за сигурност на информативниот систем на банката, од аспект на нејзиното унапредување.

IV. ПЛАНИРАЊЕ, РАЗВОЈ И СПРОВЕДУВАЊЕ НА СТРАТЕГИЈАТА ЗА УПРАВУВАЊЕ СО ИНФОРМАТИВНАТА ТЕХНОЛОГИЈА

15. Банката е должна да воспостави рамка за планирање и развој на соодветна стратегија за управување со информативната технологија (во понатамошниот текст: ИТ-стратегија), којашто им одговара на природата, обемот и сложеноста на нејзините ИТ-активности.

16. Банката е должна да донесе, да ја документира и да ја поддржи ИТ-стратегијата преку развој на оперативни планови за спроведување реални цели, преку соодветно планирање на ресурсите и финансиите во соодветни временски периоди.

Стратегијата за ИТ треба да биде усогласена со деловната политика на банката. Таа треба повремено да се ажурира, а посебно при промена на деловниот модел, за да се обезбеди усогласеност на ИТ со оперативните планови и активности.

17. Банката е должна да воведе контролна рамка соодветна на големината, природата на измените, материјалното значење во деловниот модел и обемот на ИТ-активностите за да овозможи ефикасно спроведување на ИТ-стратегијата, преку воспоставување соодветна проектна организација, следење на буџетот и редовно известување.

18. Банката е должна да дефинира улоги и одговорности на органите на банката и соодветните тела за спроведување на ИТ-стратегијата коишто имаат соодветно искуство во организација и надзор на значајни и сложени технолошки промени.

19. Банката е должна да ги идентификува и да ги оцени ризиците поврзани со успешно спроведување на ИТ-стратегијата, како и да преземе мерки за нивно намалување.

V. ОБЕЗБЕДУВАЊЕ НЕПРЕКИНАТОСТ ВО РАБОТЕЊЕТО

20. Банката е должна да развива и да спроведува сопствен план за непрекинатост во работењето, којшто ќе се темели врз повеќе сценарија и којшто ќе овозможи оперативност и минимизирање на загубите во случај на тежок прекин на деловните процеси.

21. Планот од точка 20 на оваа одлука треба да овозможи идентификација на критичните операции на банката, вклучувајќи ги и оние коишто зависат од друштва за помошни банкарски услуги или од трети лица. За тие процеси банката треба:

- да определи методологија за оценка на штетите и да дефинира коефициенти на максимално дозволено време на нефункционирање на критичните деловни линии и да дефинира одделни вредности за целно време за обнова и целна точка за обнова (англ. RTO, RPO);
- да ги идентификува алтернативните механизми за непрекинатост во деловните процеси во случај на прекин на примарните механизми;
- да ја идентификува можноста за заштита и обнова на податоците коишто се потребни за продолжување на деловниот процес на оддалечена локација;
- да ја определи резервната локација на која ќе бидат заштитени податоците, која треба да биде на соодветна географска оддалеченост од примарната локација, за да се минимизира ризикот двете локации да бидат истовремено недостапни;
- да ги земе предвид можните решенија за надминување на ризиците поврзани со непрекинатоста и расположливоста на ИТ-системите и сервисите коишто произлегуваат од напади од дигиталниот простор и да подготви соодветен план за отпорност од напади од дигиталниот простор (т.н. cyber resilience plan);
- да ги земе предвид физичките мерки за заштита на критичната инфраструктура на Банката на примарната и на резервната локација и да обезбеди соодветни услови за нивно непречено и сигурно функционирање;
- да ги земе предвид улогите и одговорностите на лицата кои се одговорни за ИТ-инфраструктурата во услови на користење услуги од надворешни лица, преку соодветни планови и активности за обезбедување непрекинатост и отпорност во работењето.

За ефикасна примена на планот од точка 20 од оваа одлука, банката е должна да воспостави процедури преку кои соодветно ќе се применат елементите дефинирани во став 1 од оваа точка.

Банката е должна да обезбеди соодветен капацитет и расположливост на ИТ-системите на резервната локација, согласно со коефициентите од став 1 алинеја 1 од оваа точка, за да може вработените кои се предвидени со плановите непречено да работат со овие системи во кризни услови.

22. Банката е должна најмалку еднаш годишно да врши тестирање на непрекинатоста во работењето преку развој на комплексни сценарија и опфаќање поголем број на системи и учесници во тестирањето.

Во сценаријата треба да бидат опфатени тестирања на најмалку следниве системи: главната банкарска апликација, комуникацијата со платните системи во земјата и странство (НБРМ, КИБС, СВИФТ).

За резултатите од извршеното тестирање да се достави сумарен извештај до Народната банка.

23. Во зависност од големината, природата и обемот на финансиски активности на Банката, гувернерот на Народната банка може да определи вредности за целно време за обнова и целна точка за обнова на деловните процеси коишто се дефинирани во точка 21 став 1 на оваа одлука.

VI. СИСТЕМИ НА СОВРЕМЕНИ КАНАЛИ

24. Покрај критериумите наведени во точка 2 од оваа одлука, за системите на современи канали коишто вклучуваат далечински пристап до банката со можност за извршување платежни трансакции преку средства за далечинска комуникација, сигурноста на информативниот систем треба да обезбеди автентикација на корисникот и следење на платежните трансакции.

Автентикација на корисникот

25. Автентикација на корисникот може да се врши преку три елементи: знаење (нешто што само корисникот го знае), владение (нешто што само корисникот го поседува) и/или својственост (нешто што корисникот е). Овие елементи се спроведени со користење на следниве методи:

- знаење: преку слог на знаци што му е познат единствено на корисникот, како што е лозинка, шифра, пин;
- владение: преку уред што единствено корисникот го поседува, како што е мобилен телефон, електронска картичка, клуч (токен), дигитален сертификат, код за еднократна употреба и/или
- својственост: преку некоја од единствените лични биометриски физички карактеристики на корисникот, како што се отпечаток од прст, ирис, препознавање говор или лице, геометрија на дланка.

Елементите од став 1 на оваа точка треба да бидат меѓусебно независни во смисла на пробивањето на тајноста на еден од методите не смее да доведе до загрозување на останатите.

Барем еден од елементите за знаење и владение не смее повторно да се употребува или да се репродуцира, ниту, пак, да може скришно да се украде преку интернет.

26. Во системите за современи канали, банката треба да примени сигурни и ефикасни методи за автентикација на корисниците и нивните овластувања.

27. За системите за современи канали коишто се достапни далечински преку интернет, банката е должна да обезбеди валидна потврда на својот идентитет преку преносниот канал, за да можат корисниците да го потврдат идентитетот на системот на банката.

28. Банката треба да обезбеди сигурен начин за пријава на клиентите, почетно ставање на располагање на алатките за автентикација на корисниците и интегритетот на софтверот којшто ќе се користи за плаќање.

29. Сите податоци коишто се употребуваат за идентификација и автентичност на корисниците и нивните овластувања на системите за современи канали треба соодветно да се заштитат од кражба, неовластен пристап или нивна неовластена измена.

30. Во системите за современи канали коишто вклучуваат: извршување далечински платежни трансакции, податоци за банкарски картички, измени во личните податоци и контактни информации за клиент, измени во овластените листи на примачи на плаќање (т.н. бели листи), Банката треба да примени засилена проверка на автентикација на корисникот којашто се врши преку комбинација од најмалку два од дефинираните елементи во точка 25 на оваа одлука.

По исклучок од став 1 на оваа точка, засилената проверка на автентикација на корисниците при извршувањето на далечинските платежните трансакции преку системите за современи канали може да не се врши во следниве случаи:

- интерни трансфери помеѓу две сметки на ист клиент;
- интерни трансфери во Банката, оправдани со ниска оценка од извршената анализа на ризик на трансакцијата и
- поединечни платежни трансакции со мала вредност, оправдани со ниска оценка од извршената анализа на ризик на трансакција.

Следење на платежните трансакции

31. Во современите канали треба се спроведат механизми за следење на активностите на клиентот и примените платежни трансакции коишто се наменети за спречување, откривање и дополнителна проверка на потенцијална измама. Овие механизми треба да бидат активирани пред секое прифаќање и одобрување на плаќањата.

Механизмите од став 1 на оваа точка треба да се засноваат најмалку на следниве параметри/правила и/или показатели:

- воведени т.н. црни листи во кои се регистрирани злоупотребени податоци за клиенти и украдени картички, црни листи на ИБАН броеви, податоци за фалсификувани документи на клиенти;
- невообичаено поведение на клиент или идентификувана промена во пристапот до современите канали (пример: измена во вообичаените интернет-адреси на пристап на клиентот или неговата брза промена на географска локација во

текот на една или повеќе сесии, т.н. невозможно патување, проверка на интегритетот на уредот од кој се вршат плаќањата, атипични плаќања на корисникот кон одредени категории трговци, невообичаени податоци за трансакциите).

32. Банката треба да има вградено системи коишто имаат можност да препознаат присуство на злонамерен софтвер во далечински воспоставениот канал (сесија) и познати сценарија за измама. Обемот, сложеноста и приспособливоста на овие системи треба да биде во зависност од утврдената оценка на ризикот.

33. Постапката за контрола и проценка на измами поврзани со високоризичните платежни трансакции треба да се спроведе во соодветно пропишан временски интервал, за да не се одложи неоправдано извршувањето на плаќањата преку современите канали.

34. Доколку банката одлучи согласно со својата анализа и проценка да изврши дополнителна проверка на платежната трансакцијата којашто е оценета како потенцијална измама, таа треба да трае согласно со соодветно пропишан временски интервал, или сè додека не се исполнат критериумите од точка 24 на оваа одлука.

35. Во системите за современи канали банката треба да вгради соодветни ревизорски траги со кои ќе се обезбеди утврдување на редоследот на извршените активности на корисниците во системот.

36. Банките треба да им помогнат и да ги советуваат корисниците за соодветна употреба на современите канали и соодветните новини, како и за сигурно спроведување на плаќањата.

Банките треба да ги информираат корисниците најмалку за следниве постапки:

- заштита на своите лозинки, мобилни уреди, сигурносни клучеви (токени) и уреди со кои се обезбедува потврда на автентичноста на извршените трансакции преку современите канали;
- соодветно и сигурно користење на личните уреди на корисникот како што се персонален компјутер, мобилен телефон и ажурирање на сигурносните компоненти кај корисникот како што се: антивирус, огнен ѕид, сигурносни надградби и сл.;
- употреба на легитимната интернет-адреса на банката преку која се врши плаќање преку современите канали и преземање на софтверското решение коешто се користи при плаќање;
- начин на прием на приговори на корисници, обезбедување корисничка поддршка, пријава или сомневање за сомнителни и/или изменети трансакции, сомнителна работа на софтверското решение, аномалии во текот на користење на услугите на современите канали и/или можни обиди за социјален инженеринг на страната кај корисникот;
- повратно информирање на банката кон корисникот во случај на потенцијални измами и/или да го предупреди корисникот за потенцијални напади или претстојни закани во системот за современи канали;

Доколку комуникацијата со корисниците се одвива по електронски пат треба да се обезбеди начин преку кој корисникот може да ја потврди автентичноста на примените пораки.

37. Банката треба да одреди и да воспостави лимити за плаќањата коишто корисниците ги вршат преку современите канали и да им овозможи на своите корисници натамошно ограничување во рамките на претходно зададените лимити. Лимитите за плаќања може да важат за сите плаќања извршени преку современите канали или, пак, на одделни начини за далечинска комуникација и/или банкарски производи и услуги.

Банката најмалку треба да ги воспостави следниве лимити:
- максимален износ на секое плаќање преку современите канали и
- вкупен износ на плаќања во тек на одреден временски интервал (ден, месец).

Банката треба да ги информира своите корисници за воспоставените лимити од став 1 на оваа точка.

38. Електронските извештаи коишто се разменуваат со корисниците треба да бидат достапни во сигурна околина. Доколку банките ги информираат периодично клиентите преку праќање редовни електронски извештаи или вонредно, по иницирани или извршени платежни трансакции преку дополнителен канал за комуникација, чувствителните податоци за плаќањата не би требало да бидат вклучени или ако се вклучени, тие треба да бидат прикриени.

VII. ДРУШТВО ЗА УСЛУГИ НА БАНКАТА ЗА ИНФОРМАТИВНИОТ СИСТЕМ

39. Друштвото за услуги на банката за информативниот систем задолжително треба да поседува сертификат согласно со меѓународниот стандард ИСО/ИЕЦ 20000.

40. Банка којашто има намера да склучи договор со друштво за услуги на банката за информативниот систем треба да ги исполнува најмалку следниве критериуми:

40.1. Да поседува заштитена копија на податоците од базите на податоци за работењето во последните три години. Заштитената копија треба физички да се чува на локациите наведени во потточка 40.2. и потточка 40.3. од оваа точка. Банката треба да врши ажурирање на заштитената копија на податоците во согласност со Политиката од точка 8 од оваа Одлука, а најмалку еднаш на секои 24 часа;

40.2. Да поседува најмалку еден функционален информативен систем лоциран на територијата на Република Македонија којшто ќе ги има најмалку следниве потсистеми:
- работа со население и правни лица,
- сметководство,
- платен промет во земјата и странство, и
- останати потсистеми за операциите коишто согласно со точка 21 од оваа одлука се оценети како критични за непрекинатоста во работењето;

40.3. Да поседува и дополнителен автономен информативен систем лоциран во Република Македонија, доколку друштвото од став 1 од оваа точка е лоцирано во

странство. Дополнителниот автономен информативен систем треба да биде на адекватна оддалеченост од системот наведен во потточка 40.2. од овој став. Овој дополнителен информативен систем треба да поседува соодветни потсистеми преку кои ќе може да се изготват ажурни извештаи за потребите на органите на банката, за известувања на Народната банка, како и за други органи или институции согласно со прописите во Република Македонија.

Во случаите кога банката има намера да користи друштво за услуги на банката за информативниот систем за процесирање на платежни трансакции засновани на платежни картички критериумите од оваа точка не се применуваат.

41. Пред да се изврши избор на друштвото за услуги на банката за информативниот систем, банката треба да ги преземе следниве активности:

- да изврши длабинска анализа на работењето на друштвото од правен, финансиски аспект и
- да изврши анализа на ризиците врз работењето на банката што можат да произлезат од користењето на услугите, при извршувањето на банкарските и финансиските активности во делот на информативниот систем.

Под избор на друштвото за услуги на банката за информативниот систем се подразбира склучување нов договор или продолжување на веќе постоечки договор за помошни услуги на банката.

42. Банката не смее да склучи договор со друштвото за услуги на банката за информативниот систем доколку на каков било начин се оневозможува, се ограничува или се отежнува пристапот на Народната банка при спроведувањето на супервизијата и надзорот, во согласност со Законот за банките.

43. Друштвото за услуги на банката за информативниот систем не смее да користи услуги на други помошни друштва, односно подизведувачи, за извршување на оние услуги за кои е склучен договорот, доколку тоа експлицитно не е наведено во него.

44. Работењето на друштвото за услуги на банката за информативниот систем треба да биде усогласено со Политиката на банката од точка 8 на оваа одлука.

45. Банката што донесла одлука да користи услуги од друштвото за услуги на банката за информативен систем, покрај елементите на политиката дефинирани во точка 8 став 1 од оваа одлука, треба да ги предвиди во политиката и следниве елементи:

- да го дефинира начинот на утврдување на единствените принципи и правила за избор на друштвото;
- да ги дефинира заштитните механизми што треба да бидат содржани во договорите со друштвото, како што се клаузулата за неоткривање на информациите, клаузулата за нивото на квалитет на услугите, клаузулата за координирано управување со сигурносните инциденти, клаузулата за спроведување независна ревизија и сл.;
- да утврди правила коишто треба да ги исполнува друштвото, а коишто ќе бидат усогласени со планот за непрекинатост во работењето на банката и плановите за отпорност од нападите од дигиталниот простор;

- да го дефинира начинот на следење на квалитетот на услугите и работата на друштвото, неговата финансиска состојба и неговиот профил на ризик, преку периодично тестирање на неговата усогласеност со политиката за сигурност на информативниот систем на банката и нивото на подготвеност од нападите од дигиталниот простор.

46. Доколку банката користи друштво за услуги на банката за информативниот систем за обезбедување сервис на СВИФТ (англ. SWIFT) при извршувањето на активностите од платниот промет во странство е должна:

- да го уреди функционирањето на сервисот на СВИФТ согласно со точките 41, 42, 44 и 45 од оваа одлука;
- да поседува сет на стандардизирани софтверски алатки за соодветно управување со размената на пораките;
- да назначи најмалку две лица во постојан работен однос во улога на лица одговорни за управување со сигурноста на инфраструктурата на СВИФТ (англ. SWIFTNet Security Officers). Овие лица треба да имаат непречен директен и индиректен пристап до сервисите за управување со инфраструктурата на СВИФТ за сертификати (англ. SWIFTNet PKI);
- доколку има потреба, банката може да назначи едно дополнително лице за управување со сигурноста на инфраструктурата на СВИФТ, коешто не мора да биде во постојан работен однос. Во ваквиот случај, активностите на лицата за управување со сигурноста на инфраструктурата на СВИФТ треба да се воспостават на принцип на двојна потврда на нивните активности;
- да не ги воспостави функциите за управување со инфраструктурата за сертификати врз принципот на заеднички систем на управување со сертификатите (англ. shared security officers), доколку на тој начин се нарушува непречениот пристап на лицата од став 1, алинеја 3 од оваа точка.

VIII. ИЗВЕСТУВАЊА

47. Банката е должна да ја извести Народната банка во случаите кога ќе идентификува дека се случило највисоко ниво на сигурносен инцидент во информативниот систем и значаен инцидент поврзан со сигурноста на плаќањето, согласно со дефинираните нивоа на сигурносни инциденти од точка 8 став 1 алинеја 7 од оваа одлука.

Банката е должна да го достави известувањето од став 1 на оваа точка до Народната банка, во рок што не е подолг од три дена од денот кога е утврдено дека настанал сигурносниот инцидент.

48. Банката е должна да го достави сумарниот извештај за идентификуваните ризици за информативниот систем, од точка 6 став 2 од оваа одлука, најдоцна до крајот на тековната година.

49. Банката е должна да ја извести Народната банка за промените во клучните делови на процесот на управување со сигурноста на информативниот систем, а посебно при промени на елементите од политиката дефинирани во точка 8 став 1 од оваа одлука.

IX. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

50. Оваа одлука стапува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Македонија", а ќе се применува од 1 јануари 2019 година.

Банката е должна да се усогласи со точка 31 и точка 32 од оваа одлука заклучно со 1 јануари 2020 година.

51. Со отпочнувањето со примена на оваа одлука, престанува да важи Одлуката за сигурноста на информативниот систем на банката („Службен весник на Република Македонија" бр. 31/2008, 78/08, 31/09 и 74/12).

О бр. 02-15/VIII-1/2018
26 април 2018 година
Скопје

Гувернер
и претседавач
на Советот на Народната банка
на Република Македонија
Димитар Богов

КАТЕГОРИЈА НА ИТ-РИЗИК	ДЕФИНИЦИЈА
I. Ризик за непрекинатоста и расположливоста на ИТ-системите	Ризик од настани којшто неповолно може да се одрази врз работата и расположливоста на ИТ-системите и податоците, вклучувајќи ја и неспособноста за навремено воспоставување на услугите на институцијата поради неисправности во хардверските и софтверските компоненти на ИТ-системите, слабости во управувањето на ИТ-системите или останати настани.
II. Ризик за сигурноста на ИТ	Ризик којшто произлегува од неовластен пристап до ИТ-системите и податоците од внатре во Банката и надвор од неа (пр. напади од дигиталниот простор).
III. Ризик од промените во ИТ	Ризик којшто произлегува од неспособноста на Банката да управува навремено и контролирано со промените во ИТ-системите, особено кога станува збор за големи и сложени промени во програмите.
IV. Ризик за интегритетот на ИТ-податоците	Ризик дека податоците коишто се чуваат и се обработуваат на ИТ-системите се непотполни, неточни или неконзистентни во различни ИТ-системи, на пример поради слаби или непостоечки контроли во текот на животниот циклус на податоците (дизајнирање на архитектурата на податоци, изработка на моделот на податоци и/или речникот на податоци, проверка на внесот на податоци, контрола врз издвојувањето на податоците, преносот и обработка, вклучително и излезните податоци), со што се нарушува способноста на Банката исправно и навремено да дава услуги и да обезбедува информации поврзани со управувањето (ризиците) со Банката.
V. Ризици поврзани со користење на друштвата за помошни услуги за ИТ	Ризик којшто настанува поради ангажирање на Друштвото или дел од групација да води ИТ-систем во кој се чуваат банкарски податоци и извршуваат банкарски и финансиски активности, при што таквиот начин на работа негативно влијае врз работата на Банката и начинот на нејзино управување со ризиците.

Анекс 1 – Категоризација на ИТ-ризици (препораки за унификација на категориите на ИТ-ризик во ЕУ[1])

Во дефинициите на сите категории за ИТ-ризик се опфатени и примери за ИТ-ризици со нивен опис коишто се наведени во следнава табела во прилог на овој анекс 1.

Прилог: Категории на ИТ-ризици и одреден број на ИТ-ризици коишто имаат сериозен потенцијал и може да предизвикаат оперативни прекини со материјална и финансиска штета и/или да ја нарушат репутацијата на Банката

Категории на ИТ-ризик	**ИТ-ризик (не е сеопфатна листата[2])**	**Опис на ризикот**	**Примери**
Ризик за непрекинатоста и расположливоста на ИТ-системите	*Несоодветно управување со капацитетот*	Недостатокот на доволно ресурси (хардверски, софтверски, вработени, надворешни друштва) може да доведе до неможност да се постигнат деловните барања, да настанаат прекини во функционирањето на системите, влошување на квалитетот на сервис и/или појава на оперативни грешки.	• Недоволниот капацитет на телекомуникациски линии може да доведе до недостапност на мрежата (интернет) за сервиси како што е електронското банкарство. • Недоволниот број на човечки ресурси (вработени или по договор со добавувачи) може да предизвика прекини во системот или оперативни грешки.
	Неисправност на ИТ-системите	Губење на расположливоста поради хардверски неправилности	• Неисправност при снимањето на меморија (диск, дисковен простор), сервери или друга ИТ-опрема поради проблеми поврзани со недостаток на одржувањето на опремата.

[1] Guidelines on ICT Risk Assessment under the SREP (European Banking Authority - EBA/GL/2017/05)

[2] Наведените ИТ-ризици најмногу влијаат врз категоријата на ИТ-ризик каде што се наведени, недвојбено дека тие може да влијаат и врз друга категорија на ИТ-ризик.

		Губење на расположливоста поради софтверски неправилности или грешки	• Бескраен циклус во апликација оневозможува извршување на трансакцијата • Прекини предизвикани од користење застарена опрема коишто не одговараат на моменталните барања во поглед на расположливоста и отпорноста и/или коишто веќе немаат поддршка од производителот
	Несоодветно планирање на непрекинатоста во работење и обнова од катастрофа	Неисправност во планираните ИТ-ресурси предвидени за непрекинатост и обнова од катастрофа (резервен компјутерски центар) во случај на негово активирање при настанат инцидент.	• Разлики во конфигурациските поставки на примарниот и резервниот компјутерски систем може да доведат до неможност на резервниот компјутерски центар да го овозможи планираниот квалитет на сервис.
	Напади од дигиталниот простор коишто имаат за цел да ги прекинат или да ги срушат системите	Напади од различни мотиви (активизам, уцени) коишто предизвикуваат оптоварување на системите и мрежите и на тој начин авторизираните корисници не може да пристапат до системите за современи канали.	• Дистрибуирани напади од типот на „откажување сервиси/услуги (DDoS)" во посредство на голем број ИТ-системи коишто се контролирани од страна на хакери коишто праќаат голем број легитимни барања преку интернет до сервисите на современите канали.
Ризик за сигурноста на ИТ	*Напади преку дигиталниот простор и/или внатрешни напади со користење ИТ-средства*	Напади извршени преку интернет или од внатрешни мрежи (пр. измама, шпионажа, саботажа и сл.) со помош на различни техники (социјален инженеринг, обиди за неовластен пристап преку користење слабости во ИТ-системите, употреба на злонамерни програми)	Различни типови напади: • APT (Advanced Persistent Threat – напредни постојани закани) за преземање на контролата на интерните системи или кражба на информации (кражба на идентитет, информации за кредитни картички и сл.)

		чијашто цел е да ја преземат контролата врз ИТ-системите.	• Злонамерен софтвер (англ. ransomware) којшто ги шифрира податоците за да се плати откуп • Инфекција на внатрешни ИТ-системи со т.н. „тројански коњ" апликација за прикриено следење и извршување на нивните активности • Искористување на слабостите на ИТ-системите или на веб-апликациите (вметнување SQL injection код) за добивање пристап до внатрешните ИТ-системи.
		Извршување измамнички платежни трансакции од страна на хакери преку разбивање или заобиколување на воспоставените сигурносни контроли на системите за современи канали и/или интерниот платен систем преку искористување на слабостите во контролниот систем.	• Напади на сервисите на современи канали за да се извршат неавторизирани трансакции • Креирање и испраќање измамнички платежни трансакции преку интерниот платен систем во Банката (неавторизирани СВИФТ пораки, инструкции примени преку електронска пошта)
		Извршување измамнички трансакции во делот на хартии од вредност од страна на хакери преку разбивање или заобиколување на воспоставените сигурносни контроли во делот на современите канали преку кои клиентот има пристап и до можноста за купување/продавање хартии од вредност.	• Напади при кои напаѓачите стекнуваат пристап до сметките на клиентите на електронско банкарство при што целно купуваат одредени хартии од вредност и со тоа влијаат врз пазарната цена на хартијата од вредност за да остварат материјална добивка (англ. pump and dump).
		Напади на комуникациски поврзувања и разговори од секаков тип или ИТ-системи за да се добијат информации и/или за да се извршува измама	• Прислушкување/пресретнување на незаштитен пренос на податоци за потврда на идентитет на корисник во форма на чист текст

	Несоодветна внатрешна сигурност на ИТ-системите	Стекнување неавторизиран пристап до критични ИТ-системи во рамките на институцијата за различни цели (пр. измама, извршување недозволени тргувања, кражба на податоци, активизам/саботажа) на различни начини (пр. злоупотреба/ескалација на привилегии, кражба на идентитет, социјален инженеринг, искористување на слабостите во системите, употреба на злонамерни програми)	• Инсталирање програма/уред за регистрирање притисоци на копчињата на тастатурата (англ. key loggers) за да се украде кориснички профил заради стекнување со неавторизирани доверливи податоци и/или извршување измама • Пробивање/погаѓање слаби лозинки за стекнување со неавторизиран пристап или добивање зголемени привилегии на пристап. • Администратор на системот употребува оперативен систем или алатки за манипулација со базите на податоци за да изврши измама.
		Неовластено манипулирање со ИТ поради несоодветни практики и постапки за управување со пристапот до ИТ-системите	• Неуспешното деактивирање/бришење на непотребни профили на пр. на вработени кои ги промениле/напуштиле своите работни места, вклучително и надворешни соработници на кои веќе не им е потребен пристап може да доведе до неавторизиран пристап до ИТ-системите • Одобрување прекумерен пристап и овластувања со кои може да се добие неовластен пристап и/или прикривање на недозволените активности

		Закани за сигурноста поради недостаток на обука на вработените, при што вработените не ги разбираат или ги занемаруваат сигурносните политики и процедури и постапките во ИТ или не се придржуваат до нив.	• Вработените му помагаат на напаѓачот во извршувањето на нападот (несвесно преку социјален инженеринг) • Лоши практики поврзани со корисничките профили: делење на лозинките, употреба на лесни лозинки, употреба на една лозинка за пристап до поголем број сервиси и сл. • Снимање нешифрирани доверливи податоци на преносливи компјутери и надворешни меморији (коишто може да се изгубат или украдат)
		Неавторизирано снимање и пренос на доверлива информација надвор од институцијата	• Лица кои крадат и намерно издаваат и изнесуваат доверлива информација на неавторизирани лица/јавноста
	Несоодветна физичка сигурност на ИТ-системите	Злоупотреба или кражба на ИТ-средства преку физички пристап, причинувајќи штета, загуба на имот и податоци или се овозможени други закани	• Физичка провала во зграда/канцеларија и/или компјутерски центар поради кражба на ИТ-опрема (компјутер, лаптоп, дисковен простор) и/или копирање податоци преку физички пристап до ИТ-системите.
		Намерно или случајно физичко оштетување на ИТ-средства предизвикано од тероризам, незгоди или случајни/погрешни постапки на вработените во институцијата и/или на трети лица (добавувачи, друштва за одржување/ поправка и сл.).	• Физички тероризам (терористички бомби) или саботажа на ИТ-системите • Уништување на ИТ-системите предизвикано од пожар, течење вода или други фактори
		Недоволна физичка заштита против природни непогоди кои резултираат во делумно и/или комплетно уништување на ИТ-системи/компјутерски центри.	• Земјотреси, екстремни температури, бури, снежни бури, поплави, пожар, грмотевици.

Ризик од промените во ИТ	*Недоволна контрола над промените во областа на ИТ-системите и нивниот развој*	Инциденти предизвикани од неоткриени грешки или слабости предизвикани од направени измени (пр. Непредвидени ефекти на измената или измени кои лошо се управувани пред се поради недостаток на тестирање или лоши практики во управувањето со промени) во програми, ИТ-системи и податоци.	• Пуштање во продукција на недоволно тестиран софтвер или конфигурациски измени со неочекувани, неповолни ефекти врз податоците (нивно оштетување или бришење) и/или работа на ИТ-системот (влошување на перформансите или нивно стопирање) • Неконтролирани промени на ИТ-системите или на податоците во продукциска околина • Пуштање во продукција недоволно сигурни ИТ-системи и интернет-апликации со што на хакерите им се овозможува да ги нападнат овие системи и/или да навлезат во внатрешните ИТ-системи • Неконтролирани промени во изворниот код на интерно развиени програми • Недоволно тестирање поради недостаток на соодветни услови за соодветна тестна околина.
	Несоодветна ИТ архитектура	Слабо управување со ИТ-архитектурата во проектирањето, спроведување и одржување на ИТ-системите (пр. софтвер, хардвер, податоци) може да доведе со текот на времето до скапи, сложени и комплексни промени коишто не ги исполнуваат во целост деловните потреби, ниту, пак, ги исполнуваат реалните барања за управување со ризикот.	• Несоодветно управување со промените од областа на ИТ-системите, софтверот и/или податоци во подолг временски период може да води кон сложени, хетерогени и тешки за управување ИТ-системи и архитектури коишто може да предизвикаат штети кон бизнисот и начинот на кој се управува со ризиците (пр. недостаток на флексибилност и агилност, инциденти и неисправности во поглед на ИТ, високи оперативни трошоци, намалена сигурност и отпорност на ИТ, намален квалитет на податоците и можноста за известување)

			• Прекумерното приспособување и проширување на деловните програмски пакети со помош на интерно развиени програми предизвикува неможност за пуштање идни верзии и надградби на деловните програми и ја изложува институцијата на ризик дека добавувачите нема да бидат во можност да ги поддржуваат.
	Несоодветно управување со животниот циклус и управување со надградбите	Неодржувањето соодветна евиденција на ИТ-инвентар во комбинација со добрите практики за управување со нивниот животен циклус и надградбите води кон недоволно надградени и застарени ИТ-системи коишто нема да може да ги поддржат деловните потреби и потребите за управување со ризиците.	• Ненадградени (некоригирани) и застарени ИТ-системи коишто може да откажат или да предизвикаат неповолни дејства кон деловните процеси или управувањето со ризиците (недостаток на флексибилност и агилност, прекини во ИТ, ослабена сигурност и отпорност на ИТ-системите).
Ризик за интегритетот на ИТ-податоците	*Лошо функционирање на обработката или употребата на ИТ-податоците*	Поради грешките и неисправностите во системите, комуникациите и/или апликациите и поради погрешно воспоставен процес на ЕТЛ (ETL – Extract, Transform, Load) во системот за чување на податоци, може да доведе до оштетување или нивно губење.	• Грешка во ИТ-системот при групни (вечерни) обработки, што предизвикува погрешни состојби на сметките на клиентите • Погрешно извршени SQL команди • Губење податоци поради грешки во копирањето на податоците (или репликацијата на податоците)
	Лошо дизајнирани механизми за контрола и проверка на податоците во ИТ-системите	Грешки поврзани со недостаток или неефикасен автоматизиран пренос на податоци и контролни механизми за прием (пр. при користење надворешни податоци), трансфер на податоци, обработка и контрола на резултатите во ИТ-системите (пр. механизми за контрола на точноста на	• Недоволно или неправилно форматирање на влезните податоци во апликациите и корисничките интерфејси • Недостаток на контроли за усогласување на излезните податоци

		влезните податоци, усогласување на податоците и пресметките)	• Недостаток на контроли во процесот на издвојување на податоците (преку SQL команди) што води кон погрешни податоци • Употреба на неисправни надворешни податоци за обработка
	Слабо контролирани измени на податоците во продукцискатa околина	Грешки во податоците настанати поради недостаток на контрола на точноста и оправданост на манипулацијата со податоците коишто се вршат во продукцискиот систем	• Развојните програмери или администратори на бази на податоци имаат директен пристап до податоците во продукциските ИТ-системи и вршат измени без контрола, како на пример при настанување на инцидент во ИТ-системот.
	Лошо проектирани и/или управувани архитектура на податоци, проток на податоци, модел на податоци и речници на податоци	Лошото управување со архитектурата на податоците, моделот на податоци, протокот на податоци и речникот на податоци може да доведе до различни верзии на едни исти податоци во ИТ-системите, коишто не се конзистентни поради различно применетите модели на податоци или дефиниција на податоци и/или поради разлики во постапката на нивно креирање и измена.	• Постоење на различни бази на податоци за клиентите за одделни производи или деловни единици со различни дефиниции и полиња за внес на податоци, што, пак, на ниво на целата институција предизвикува неусогласеност на податоците коишто тешко може да се споредуваат и/или да се интегрираат
Ризици поврзани со користење на друштва услуги на банката за ИТ	*Несоодветна зависност од сервиси дадени од трето лице /дел од групација*	Недостапност на клучни ИТ-сервиси, телекомуникациски сервиси и други помошни услуги од друштва за помошни услуги за ИТ. Загуба или оштетување на критични/чувствителни податоци доверени кон друштвото за помошни услуги	• Недостапност на клучни сервиси како резултат на неисправности во ИТ-системите или апликациите кај Друштвото • Прекини во телекомуникациските линии • Прекини во напојувањето со електрична енергија

	Несоодветно управување со друштвото за услуги на банка за ИТ	Значително паѓање на квалитетот на сервис или негов прекин поради несоодветната спремност и несоодветност на воспоставените контролни процеси врз Друштвото. Неефикасното управување со активностите кај Друштвото може да предизвика кон недостаток на соодветни вештини и способности за целосно идентификување, оценување, намалување и следење на ИТ-ризиците и може да предизвика ограничувања во оперативните активности.	• Лоши процедури за управување со инциденти, договорни механизми за контрола и гаранции вградени во Договорот со Друштвото со кои се зголемува зависноста во поглед на надворешните лица и на клучниот кадар • Несоодветните контроли на промените поврзани со ИТ-околината кај Друштвото може да предизвикаат значително нарушување на квалитетот на сервисите или нивен прекин.
	Несоодветна сигурност кај друштвата/ добавувачите/ делот од групацијата	Хакирање на системите на друштвата (или на трети страни) со директно загрозување на услугите коишто се пренесени во Друштвото или интегритетот на критични/доверливи податоци коишто се чуваат во Друштвото. Вработени во Друштвото може да стекнат неовластен пристап до критични/чувствителни податоци коишто се чуваат во Друштвото.	• Криминалци кои ги хакираат системите на Друштвото заради пристап до ИТ-системите на Банката за пристап до критични и чувствителни податоци коишто се чуваат во Друштвото или за нивно уништување. • Вработени во Друштвото кои имаат злонамерна цел да ги украдат и да ги продадат чувствителните податоци на Банката.