Народна Банка на Република Македонија

Супервизорски циркулар 9

СИГУРНОСТ НА ИНФОРМАТИВНИОТ СИСТЕМ НА БАНКИТЕ

Дирекција за супервизија

Супервизорски циркулар 9

1	**Дефиниција на сигурноста на информативниот систем**
2	Процес на информативна сигурност
3	Место и улога на УО, РО и ревизијата
4	Одговорен за сигурноста на информативниот систем
5	План за континуитет во работењето
6	Управување со обезбедувачите на ИТ сервиси
7	Утврдување на динамика на имплементација

Дефиниција на сигурноста на информативниот систем

- Целта за воспоставување на стандардите за сигурност на информативниот систем е да се обезбеди **непрекинатост на деловните процеси** и **минимизирање на евентуалната штета** која би ја претрпила банката со активна и превентивна имплементација на контроли со кои што ќе се намалат ризичните ефекти кои можат да бидат предизвикани **со појава на сигурносни инциденти**.

- **Доверливост** - информацијата им е достапна само на оние коишто имаат овластен пристап до неа.

- **Интегритет** - заштита на точноста и комплетноста и веродостојноста на информацијата и на процесите на нејзина обработка.

- **Расположивост** - овластените корисници имаат пристап до информацијата и до другите придружни средства потребни за нејзина презентација, кога за тоа има деловна потреба.

Доколку еден од овие принципи е неисполнет или е сериозно нарушен се смета информативниот систем на банката дека е НЕСИГУРЕН.

Супервизорски циркулар 9

1	Дефиниција на сигурноста на информативниот систем
2	**Процес на информативна сигурност**
3	Место и улога на УО, РО и ревизијата
4	Одговорен за сигурноста на информативниот систем
5	План за континуитет во работењето
6	Управување со обезбедувачите на ИТ сервиси
7	Утврдување на динамика на имплементација

Процес на информативна сигурност

Процесот треба да се состои од:

- **Проценка на ризикот** - Банката е должна да изгради континуиран процес на идентификација на слабостите и заканите кон своите информативни системи. Процесот треба да ја идентификува можноста и фреквенцијата на појавување на заканите за да се утврди евентуалната штета која би настанала доколку истите се случат;
- **Политика за сигурност на информативните системи** - Банката е должна да донесе политика за сигурност на информативниот систем која ќе претставува СТРАТЕГИЈА (план) на менаџментот за управување со идентификуваните ризици (од претходниот чекор) за сигурноста на информативниот систем на банката;
- **Имплементација на сигурносни контроли** - Банката е должна да воспостави административни, физички и технички контроли со кои ќе се изврши заштита на сигурноста на информациите и системите на повеќе нивоа;
- **Тестирање на сигурноста** - Банката е должна да воспостави процес на професионално, независно и објективно тестирање на ефикасноста и адекватноста на имплементираните контроли содржани во политиката за информативна сигурност.
- **Набљудување и надградба** - Банката е должна да воспостави процес на континуирано прибирање и анализа на информации од аспект на новите закани и слабости, актуелни напади кон банката или кон другите финансиски институции комбинирани со ефикасноста на постојните сигурносни контроли. Набљудувањето и надградбата Ќе го направат процесот на информативна сигурност континуиран.

Проценка на ризикот

Банката мора да одржува континуиран процес на проценка на ризиците кон информативната технологија, кој ги подразбира следните чекори:

- **Идентификација на средствата** на информативниот систем на банката (видови информации и типови системи за пренос на информациите);
- **Класификација на средствата** на информативниот систем на банката (доделување на вредност на средствата);
- **Анализа на веројатноста** на појава на заканите и слабостите на системот и кои се можните последици по информативниот систем на банката;
- **Доделување приоритет** во зависност од големината на ризикот.

Идентификација на средствата на информативниот систем

Идентификацијата на средствата кои се дел од информативниот систем на банката опфаќа анализа на широк спектар информации кои се важни за функционирањето на банката. Секое средство кое е дел од информативниот систем на банката во овој ѓекор треба да биде јасно идентификувано, а неговата припадност дефинирана.

Како примери на средства на информативниот систем на банката:

- **Електронска документација** – системска документација, упатства за користење, оперативни процедури, планови, тренинзи;
- **Пишана документација** – договори, упатства, пишани кредитни досиеја, документи кои содржат важни и доверливи податоци за банката;
- **Софтверски средства** – апликации, системски програми, развојни алатки;
- **Физички средства** – компјутери и комуникациска опрема, магнетни медиуми (касети и дискови), друга техничка опрема (агрегати), мебел;
- **Сервиси** – компјутерски и телекомуникациски сервиси што ги користи банката, вклучувајќи и електрична енергија и телекомуникациски поврзувања;

Идентификација на средствата на информативниот систем
Хардверска информативна книга

Пример за корисни информации кои може да се складираат во **хардверската информативна книга**:

- **за сервери**
  - производител и модел
  - капацитет на процесорот во милиони инструкции во секунда (МИПС)
  - главна меморија (RAM)
  - меморија (ХДД, ленти, силоси на ленти, ...)
  - мрежна поврзаност
  - функција
  - локација
- **за персонални компјутери (десктоп)**
  - производител и модел
  - кој го има (поседува) и со која цел
  - мрежна поврзаност
  - поврзување со надворешни мрежи (модем или безжична картичка)
  - локација
- **за мрежни уреди**
  - производител и модел
  - тип
  - ИП адреса

Идентификација на средствата на информативниот систем
Софтверска информативна книга

Пример за корисни информации кои може да се складираат во **софтверската информативна книга**:

- име на апликацијата (пр. Главна книга, население,...)
- производител или набавувач
- сериски број
- верзија на апликацијата (Version Level)
- верзија на надоградбата (Patch Level)
- Број на инсталирани копии
- Број на поседувани лиценци
- Тип на лиценца

Идентификација на средствата на информативниот систем
Мрежна информативна книга

Мрежна информативна книга:

- идентификување на сите внатрешни и надворешни поврзувања (вклушувајќи го интернет, модеми, безжично поврзување,...)
- да го опише начинот и типот на поврзување (ДСЛ, АДСЛ, dialup, wireless)
- да ни го прикаже капацитетот на врската помеѓу поврзувањата (bandwith)
- идентификување на енкриптираните канали или на друг начин канали за сигурна комуникација
- да ни го прикаже типот и капацитетот на мрежните поврзувачи (switch, router, hub)
- да ни ги прикаже главните компоненти за сигурност на информативните системи (firewall, IDS, IPS, HoneyPots)
- да ни ги прикаже отворените канали (порти) за комуникација помеѓу мрежните уреди

Класификација на средствата на информативниот систем на банката

- **Класификацијата на системот претставува раслојување на информативниот систем спрема чуствителноста на информацијата**. Банките треба да одлучат каква ќе биде нивната класификација на информациите и како ќе бидат заштитени.

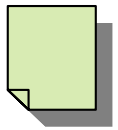
- **Рангирањето и вреднувањето на документите треба да се направи заедно со вработените во банката кои непосредно ракуваат со нив**. Вработените ја знаат вистинската загуба и можната штета која може да ја претрпи банката од неадекватното ракување со чуствителната документација.

- **Сите документи во Банката треба да се рангирани по интерен систем за класификација на документи**.

- Пример:
  - јавни, интерни, доверливи, строго доверливи средства или документи, итн;

Анализа на веројатноста на појава на ЗАКАНИТЕ и СЛАБОСТИТЕ (Дефиниции)

Средство е било кој објект во банката кој има вредност. **Слабости** претставува било каков недостаток кој може да се искористи за повреда на системот или информацијата која тој ја содржи. **Закана** претставува потенцијално нарушување на сигурноста.



Заканите спрема информативниот систем вклучуваат:

- уништување на информацијата и носителите на таа информација;
- корупција или неовластено променување на информацијата;
- кражба, изнесување или губење на информацијата и средствата;
- прекин на сервисите.

Заканите може да биде класифицирани како случајни или намерни и може да бидат активни или пасивни.

Source: ISO 7498-2 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

Анализа на веројатноста на појава на ЗАКАНИТЕ и СЛАБОСТИТЕ (Дефиниции)

Средствата се подложни на различен тип на **слабости**. **Слабостите** може да предизвикаат несакан **инцидент** кој може да го загрози системот, Банката или нејзините средства. **Заканата** може да ја искористи слабоста на средствата во смисла на успешно нанесување на штета кон средствата. Слабостите сами за себе не нанесуваат штета. Слабостите се на некој начин сет на услови кои треба да се исполнат со кои може заканата да го афектира средството или информацијата.

Ризикот претставува можноста дека дадена закана ќе искористи дадена слабост на системот и ќе предизвика штета или финасиска загуба кон Банката. **Контролите** се пракси, процедури и механизми кои се употребуваат со цел да се заштити од заканата, да се намали слабоста или да се ограничи ударот на одреден инцидент и откривање на несакани инциденти.

Ризиците обично се парцијално намалувани со имплементација на контроли. Контроли за намлување на ризикот се најчесто применувани, меѓутоа секоја имплементирана контрола ни дава поскап трошок. Ова имплицира дека секогаш ќе имаме **РЕЗИДУАЛЕН РИЗИК**. Еден начин на однесување во Банката е прифаќање на целиот резидуален ризик и тој процес е познат како **ПРИФАЌАЊЕ на РИЗИКОТ**. Постои и начин на трансфер на тој ризик кон осигурителни компании и тоа е познато како осигурување или **ТРАНСФЕР на РИЗИКОТ**.

Source: ISO/IEC WD 13335-1, Information technology - Security techniques – Guidelines for the management of IT security (GMITS) – Part 1: Concepts and models of IT security

Идентификација на ЗАКАНИТЕ и СЛАБОСТИТЕ кон системите

- **закани од** (нечесни луѓе, вработени кои случајно или намерно може да направат штета како и надворешни влијанија (земјотрес, поплава, пожар, недостапност на телекомуникации и електрична енергија)
- **интерни слабости** (слаба поддршка од РО, лош и слаб тренинг, неадекватна екипираност со луѓе, неадекватни или никакви процедури)
- **технички слабости**
- **слаба документираност** на моменталните контроли и сигурносни процеси кои се присутни во ИТ
- нови сигурносни **препораки и барања на регулаторните органи**
- **одржување на процесот** на проценка на ризик и собирање на информациите за нови закани и слабости и ревидирање на политиката за ИС

Идентификација на заканите спрема значајните средства

Предизвикувач на заканата	Може да ја искористи слабоста	РЕЗУЛТАТ
Вирус	Недостаток на Антивирус софтвер	Инфекција со вирус
Хакер	Доста моќни сервиси се подигнати	Неавторизиран пристап до доверливи податоци
Корисници	Недостаток на добра централна политика	Доделување на несоодветни привилегии
Пожар	Недостаток на ПП заштита	Оштетување на опрема и податоци, а можна е загуба на човечки животи
Напаѓач	Апликација со слаби контроли	Buffer overflow
Напаѓач	Недостаток на обезбедување	Крадење на компјутерска опрема (а вероватно и новчаниците на колешките)
Напаѓач	Недостаток на јака и централна конфигурација на огнениот ѕид	DoS, DDoS

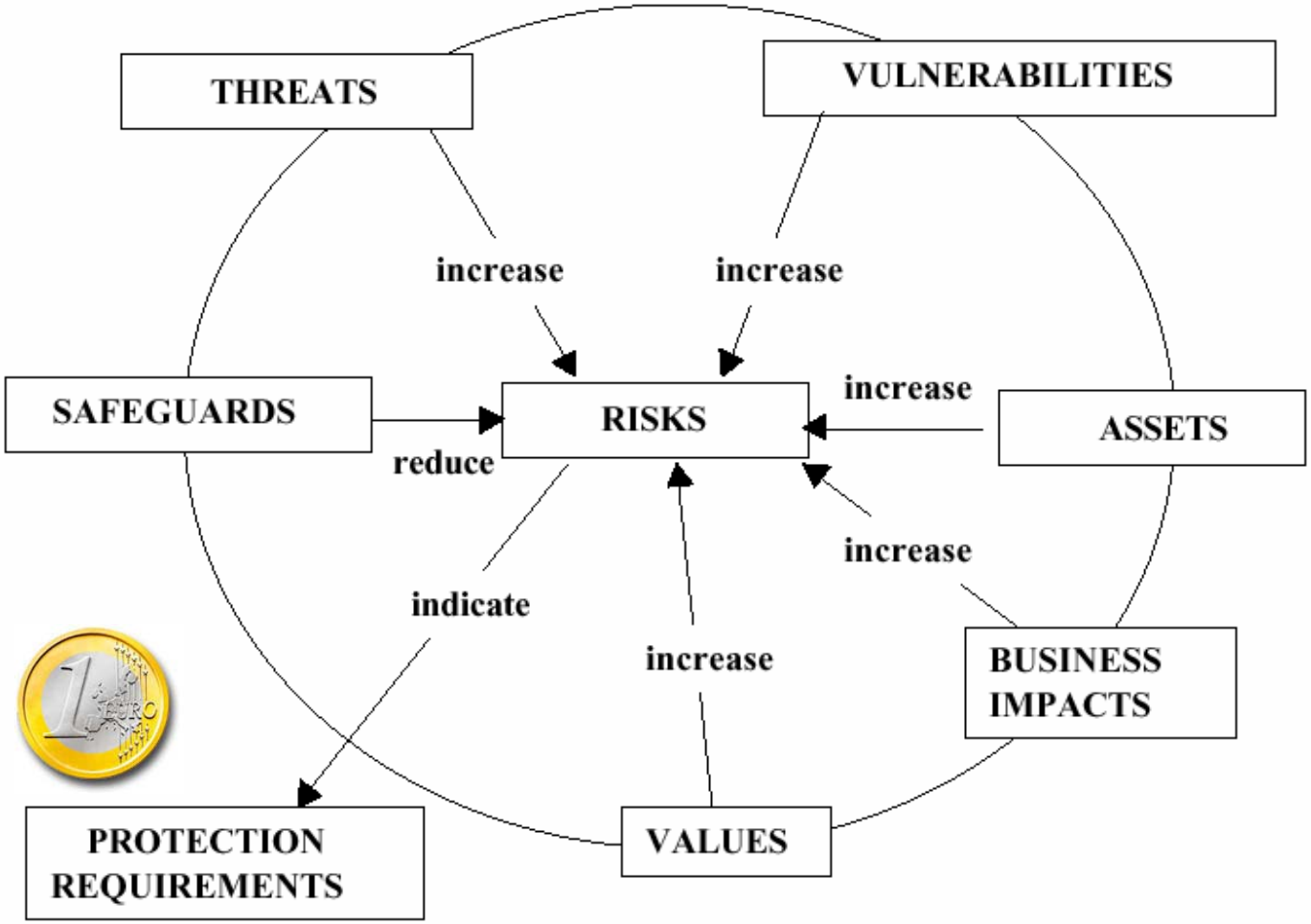
Анализа на веројатноста на појава на заканите и можните последици по банката

- Работоводниот орган треба да ги искористи податоците обработени во претходните чекори и да изврши анализа на средствата и ризиците кои се асоцирани со нив.
- Анализа на заканата на скала:
  - **многу веројатно** - заканата мошне веројатно може да се оствари;
  - **веројатно** - заканата може да се појави, меѓутоа постојат некои заштитни механизми;
  - **неверојатно** - заканата многу тешко може да се појави, бидејќи постојат адекватни заштитни механизми.

- Анализата на појавата на одредени закани треба да ги земе предвид:
  - **намерно** предизвикани закани;
  - **ненамерно** (случајно) предизвикани закани.

- **Ненамерни закани** опфаќаат инциденти од неадекватни интерни системи на контрола и неадекватни процедури во работењето, неадекватни контроли на пристап и недостаток на физичка сигурност или од природни катастрофи.
- **Намерните закани** обично се изведени од високо мотивиран напаѓач (платен од конкуренција, поранешен вработен итн) кој може да ги искористи слабостите на информативниот систем на банката.

Методи за мерење на ризикот



Source: ISO/IEC WD 13335-1, Information technology - Security techniques – Guidelines for the management of IT security (GMITS) – Part1: Concepts and models of IT security

Методи за мерење на ризикот

Начелно постојат два општо прифатени метода на мерење на ризикот и тоа:

- **КВАНТИТАТИВНА метода** и (настојува да добие вредности во $, €, денари и на тој начин да се добие листа со приоритети – потребна е статистика)

- **КВАЛИТАТИВНА метода**. (настојува во тимска работа врз база на искуство да се направи проценка на ризикот – потребно е градење на тим и искуство)

КВАНТИТАТИВНА метода

- **ЗЕН** -(**Загуба од единечна појава на настанот**) -претставува загуба изразена во денари која банката ќе ја претрпи од појава на настанот.
- **ВС** -(**Вредноста на средството**)
- **ФИ** -(**Фактор на изложеност**) -претставува процент на загуба што ќе ја предизвика заканата по вредноста на средтвото;

Со дефинирањето на овие коефициенти се добива следната равенка:

- **ЗЕН** = **ВС x ФИ**

Пример: Доколку некој сервер на банката вреди 1.000.000 денари (**ВС**=1.000.000) и се појави пожар на местото каде што е сместен. Се проценува дека оштетувањето од пожарот на серверот е 25% (**ФИ**=25%). Овој коефициент варира доколку банката има (нема) имплементирано адекватни физички контроли. (на пр.: противпожарни средства). Во тој случај, загубата од единечна појава на настанот би била:

ЗЕН = **ВС x ФИ** = 250.000 **денари**.

КВАНТИТАТИВНА метода

- **ГФП** -(**Годишна фреквенција на појава на настанот**) претставува фреквенција на појава на настанот во рамка од една година. Рангот се протега од 0.00 (никогаш) до 1.00 (секогаш) (**статистички параметар**)

- **ГЗН** -(**Годишна загуба од настанот**) претставува годишната загуба од појава на настанот согласно предвидените коефициенти на појава на настанот (ГФП)

Од горенаведеното се заклучува дека:

- **ГЗН** = **ЗЕН x ГФП**

Во продолжение на примерот треба да се дефинира коефициентот ГФП, односно доколку во регионот може да се случи пожар еднаш во десет години (статистички), тогаш ГФП=0.1 и може да се пресмета дека:

ГЗН = **ЗЕН x ГФП** = 250.000**x**0.1 = 25.000 **денари**.

Квалитативна анализа

- Анализа на различни видови сценарија и можни ризици по стабилноста и сигурното работење на банката.
- **Тимска работа на искусни луѓе** кои имаат познавање на работењето на целата банка и имаат големо познавање на ризиците кои може да се појават.
- Сценаријата се разработуваат од страна на ОСИС пред тимот и се **предлагаат или се нудат решенија** кои можат да придонесат за превентивно избегнување на заканата.
- Метод ја **рангира сериозноста на заканата и врши рангирање на можни решенија за намалување на ризикот** (**Банката може да изгради интерна скала** (**нсв**), (1,2,3,4,5)).
- Кога тимот ќе заврши со рангирањето на сериозноста на заканата и ризикот и соодветното рангирањето на ефикасноста на поединечните контроли, треба да подготви **извештај до работоводниот орган**,

Квалитативна анализа

Пример сценарио: Банката била нападната од надворешна трета страна и дека при нападот од надвор биле украдени неколку кредитни досиеја на кредитните референти.

Закана: Хакер добива пристап до доверливи информации на банката(кредитни досиеја)	Големина на заканата	Веројатност да се случи	Загубата по банката	**Контрола1:** Ефикасност на огнен ѕид (Firewall)	**Контрола2:** Ефикасност на систем за детекција на напад (IDS)
ИТ директор	4	2	4	4	3
Администратор	4	4	4	3	2
Програмер	2	3	3	4	3
Директор на Дирекција (кредити)	5	4	3	4	3
Референт (кредитен)	4	4	4	4	3
РЕЗУЛТАТИ	**3.8**	**3.4**	**3.6**	**3.8**	**2.8**

Доделување на приоритет

- Добиената анализа на ризиците треба да послужи за подготовка на **листа на приоритети** во решавање од страна на работоводниот орган
- За ризиците кои можат да предизвикаат голема штета по банката ќе биде потребна **промптна реакција** од страна на работоводниот орган или **одредување на временска рамка** во која тие ќе се намалат .
- Работоводниот орган може да реши да ги **прифати ризици** од помал степен и да не воведува контроли за намалување на истите .
- **Во овој чекор се врши селекција на нивото кое ја подразбира границата помеѓу контрола на ризиците и прифаќање на ризиците од страна на работоводниот орган .**

Политика за сигурност на информативниот систем

- Политиката за сигурност на информативниот систем претставува почетна точка во градењето на процесот на информативна сигурност.
- Политиката за сигурност на информативниот систем треба да биде поставена по принципот од најгоре па до најдолу во банката ("top-down" пристап). **Затоа, ПОЧЕТНО МЕСТО за започнување на процесот на информативна сигурност е работоводниот орган на банката.**

Стандарди, упатства и процедури

- **Стандардите ги дефинираат активностите, претставени како правила и ограничувања, со кои ќе се обезбеди постигнување на дефинираните цели со политиката за информативна сигурност.**

- **Упатствата содржат подетални насоки за активностите кои треба да се преземат и применуваат и даваат оперативни насоки за корисниците на системот.**

- **Процедурите претставуваат детални чекори што треба да се преземат за да се постигнат одредени цели од политиката.** Процедурите може да бидат упатени кон крајните корисници, вработените кои треба да направат одредени активности за подобрување на сигурноста на ниво на целата банка.

- Пример: доколку се декларира дека правењето "бекап" е стандард во банката, процедурите треба детално да го разработат правењето "бекап", во кој временски рамки, каде ќе се чува...

Клучни фактори кои влијаат на успехот на политиката за информативна сигурност

- добивање поддршка и активно учество на работоводниот орган;
- спроведување комплетна анализа на ризиците по информативниот систем на банката;
- успешна класификација на информативниот систем;
- имплементација на сигурносни контроли со цел контрола и управување со ризикот;
- воспоставување на сет од прецизно дефинирани морални и етички вредности на однесување на вработените во поглед на сигурноста на информативниот систем;
- добивање изјава (потврда) од сите вработени дека ја прочитале и ја разбрале политиката за информативна сигурност, особено делот за прифатливо користење на информативните системи на банката;
- обезбедување соодветна обука и едукација на сите вработени за сигурност на информативниот систем;
- спроведување на годишно ревидирање на политиката, а промените да бидат утврдени од страна на Управниот одбор.

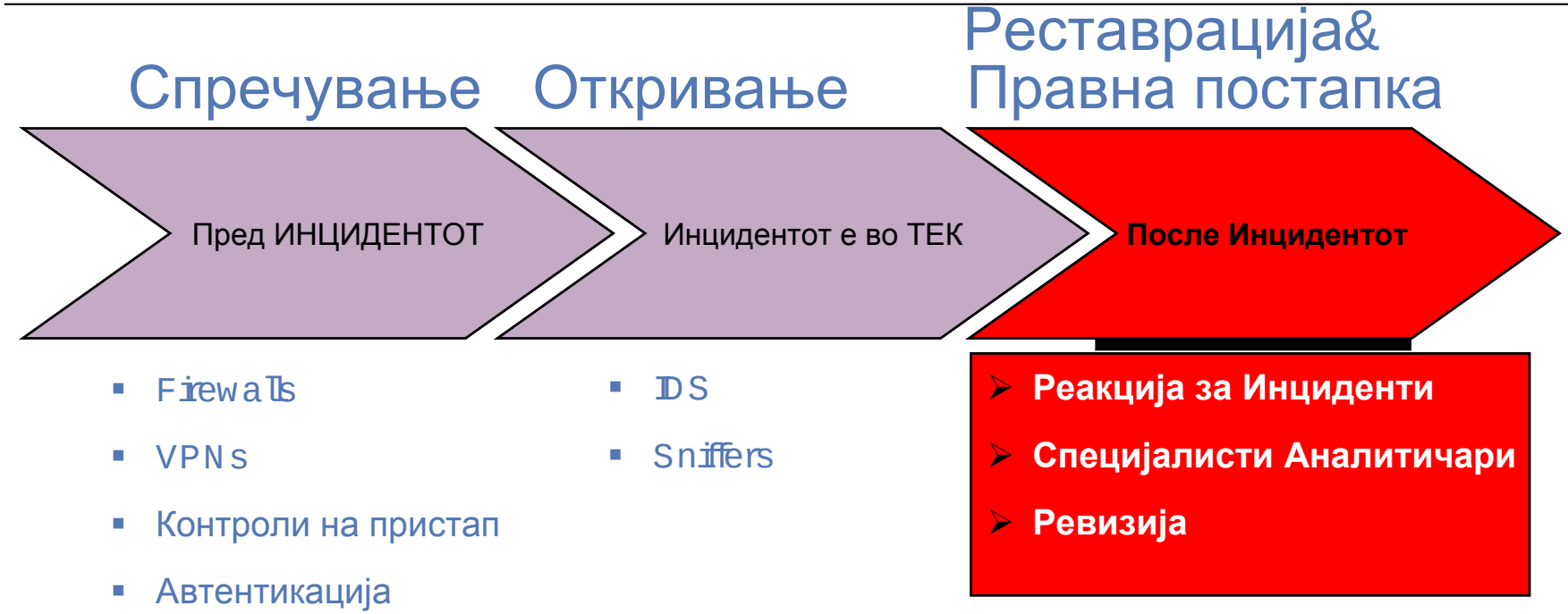
Основни компоненти на политиката за сигурност на информативниот систем

- Класификација на информацијата
- Обука на вработени во однос на правилно (прифатливо) користење на информативниот систем на банката
- Дефинирање на улогата на внатрешната и надворешната ревизија од аспект на обезбедување на сигурноста на информативниот систем;
- Дефинирање на односот со обезбедувачите на ИТ сервиси на банката.
- Дефинирање на контрола на пристап до одредени ресурси на банката (начинот на контрола и идентификација на корисник);
- Следење на конфигурации (сигурносни надградби, надградби на нови верзии, промени во параметри и кодови на апликации, подготовка и мигрирање на апликацијата во продукција); Поставување на План за континуитет во работењето (во понатамошниот текст ПКР) на сите деловни функции на банката;
- Воспоставување на антивирусна заштита;
- Дефинирање на телекомуникации (модеми, огнени ѕидови, системи за набљудување, алармирање и евидентирање на неавторизиран пристап до информативниот систем, енкрипција);

Основни компоненти на политиката за сигурност на информативниот систем

- Ограничување на физичкиот пристап (забрана за неавторизиран физички пристап до одредени области во банката); Пример: Поделба на банката на сигурносни зони. Секоја сигурносна зона може да се има свои специфични контроли за физички пристап.
- Воспоставување на дополнителни безбедносни механизми (противпожарна заштита, заштита од поплава, набљудување, сензори, аларми);
- Заштита на инвентарот од кражба или неовластено изнесување на медиуми, хардвер или софтвер надвор од банката и слично;
- Дефинирање на соодветни активности коишто ќе се преземат во случај кога банката се сомнева или утврдила инцидент во поглед на сигурноста на информативната сигурност, за што треба да се известуваат Народна банка на Република Македонија и Министерството за Внатрешни работи. Банките треба да го достават известувањето до Народна банка на Република Македонија во рок од пет дена по утврдениот сигурносен инцидент.

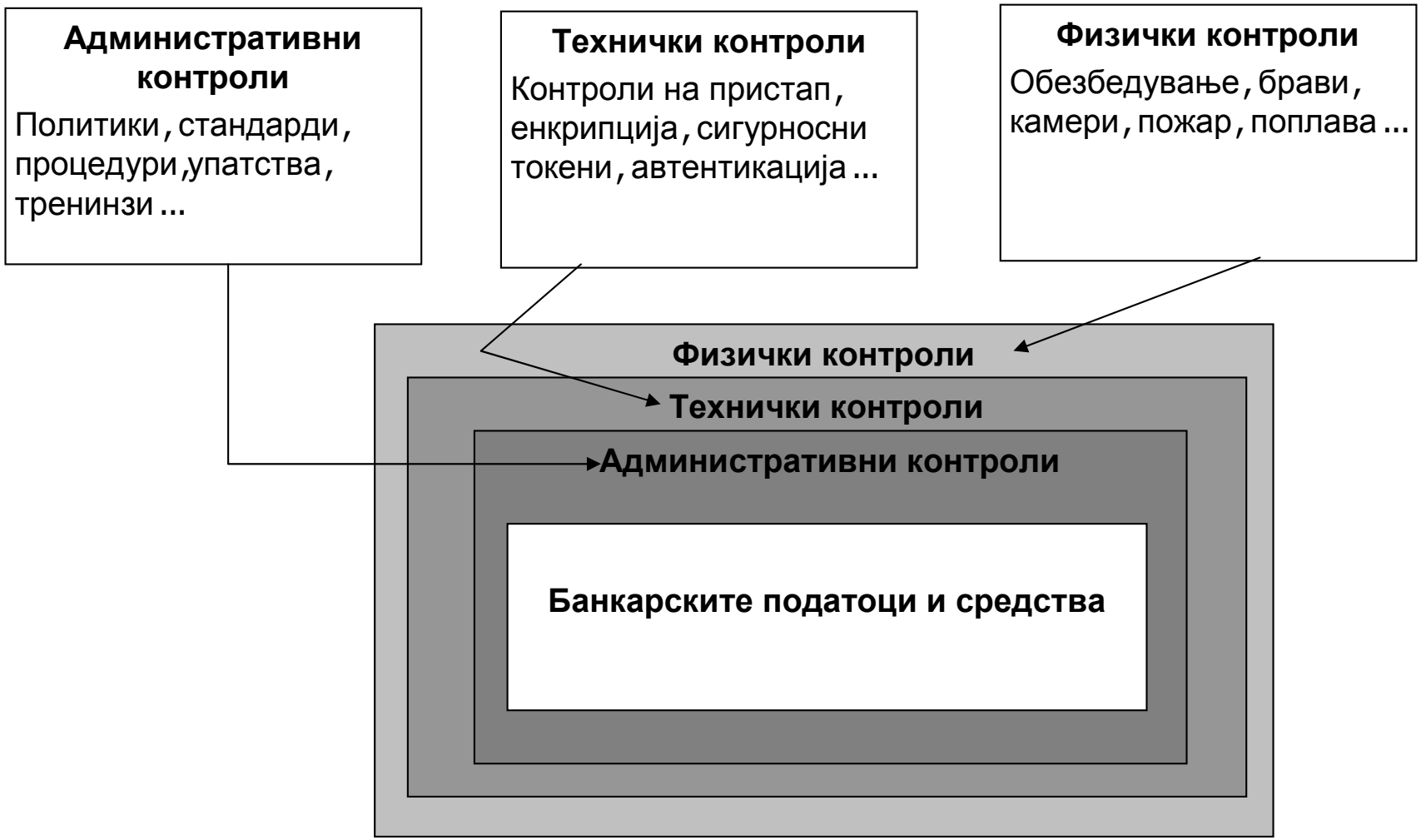
Постапки при нарушување на СИГУРНОСТА



Имплементација на сигурносни контроли

	Административни	Технички	Физички
Спречување	X	X	X
Откривање	X	X	X

Имплементација на сигурносни контроли



Физички контроли за спречување

- Заштита на податоци
- Ограда
- Чуварска служба
- Беџеви
- Брави и клучеви
- Генератори на електрична енергија
- Избор на локација (Примарна или алтернативна)
- Противпожарни средства

Физички контроли за откривање

- Детектори на движење
- Детектори на чад и оган
- C C TV системи
- Сензори и аларми

Технички контроли за спречување

- контролни листи за пристап
- антивирус
- корисничко име и лозинка
  - Начин на дистрибуција до крајните корисници;
  - Можноста за погодување на лозинката;
  - Број на дозволени погрешни обиди.
  - Препораки за управување со лозинките:
    - важност :120 дена на обични корисници;
    - важност :60 дена привилегирани корисници;
    - важност :30 дена сигурносни лица;
  - Корисникот самиот да може да ја менува лозинката пред да истече;
  - Водење на ревизорски траги на промените на лозинките.
- смарт-картички
- биометрија
- шифрирање (енкрипција)
- Контроли за далечински пристап

Техничките контроли за откривање

- Ревизорска трага - **Овие извештаи треба да се следат на редовна основа, да бидат надгледувани од Одговорниот за сигурност на информативниот систем (во понатамошниот текст ОСИС) со цел да се изврши анализа на неавторизиран пристап**

- Системи за спречување и откривање напад - **Овие системи треба да се имплементираат особено во делот кој пристапува кон интернет или сервисите на електронското банкарство**

Административни контроли за спречување

- Регистрација на корисникот за работа на системот - Пред регистрацијата, корисникот треба да е запознаен и согласен за кои операции смее, а кои операции не смее да ги извршува на информативниот систем.
- Процедури за прием на нов вработен и отпуштање
- Договори за работа
- Тренинзи за сигурност
- Сегрегација на должности
- План за континуитет во работењето (ПКР)
- Сигурносни политики, стандарди, упатства и процедури

Административни контроли за откривање

- Тестирање (ревизии) на сигурноста
- Ротација на должности на вработените

Тестирање на сигурноста

- Во тестирањето на сигурноста важна улога има службата за внатрешна ревизија и надворешната ревизија и тоа во улоги на активни тестери на сигурноста на информативниот систем.
- Генерално постојат два типа системи, и **тоа со висок и низок ризик**.
- Системите со висок степен на ризик треба да бидат пофреквентно проверувани и тестирани. Постои широк ранг тестови со цел добивање слика за сигурноста.
- Во рангот на овие тестови Управниот одбор треба да одлучи кои тестови може да ги спроведе и дали тестовите ги имале задоволителните резултати.

Набљудување и надградба

- Статичната политика на информативна сигурност застарува со тек на времето
- Се добива чуство на т.н. ЛАЖНА СИГУРНОСТ кога имаме статичка политика за информативна сигурност
- Банките треба континуирано да собираат информации и да вршат анализа на ризиците земајќи ги во предвид новите закани и слабости, актуелните напади и нови вируси кон банките и другите установи. Тие треба да ги користат овие информации, а доколку е потребно, и да се надгради процесот на проценка на ризиците, политиката за информативна сигурност и имплементираните контроли
- Управниот одбор треба да бара извршување тестови и ревизии за да се направи оценка на усогласеноста на банката со политиката на информативна сигурност

Супервизорски циркулар 9

1	Дефиниција на сигурноста на информативниот систем
2	Процес на информативна сигурност
3	**Место и улога на УО, РО и ревизијата**
4	Одговорен за сигурноста на информативниот систем
5	План за континуитет во работењето
6	Управување со обезбедувачите на ИТ сервиси
7	Утврдување на динамика на имплементација

МЕСТО, УЛОГИ И ОДГОВОРНОСТИ НА УО, РО И РЕВИЗИЈАТА ВО ПОГЛЕД НА СИГУРНОСТА И ЕФЕКТИВНО УПРАВУВАЊЕ СО ИТ

Улогата на Управниот одбор за сигурност на информативниот систем

- Управниот одбор е одговорен за управување, имплементација и унапредување на политиката за сигурност на информативниот систем на банката.
- Управниот одбор ја утврдува политика за сигурност на информативниот систем и врши нејзино унапредување најмалку еднаш годишно.
- Управниот одбор треба да му даде насоки и препораки на работоводниот орган за обезбедување на сигурен информативен систем преку:
  - барање за воспоставување централен надзор и координација;
  - дефинирање на соодветни улоги и одговорности;
  - мерење на ризикот;
  - набљудување и тестирање;
  - известување;
  - идентификување, следење и контрола на ризиците.

МЕСТО, УЛОГИ И ОДГОВОРНОСТИ НА УО, РО И РЕВИЗИЈАТА ВО ПОГЛЕД НА СИГУРНОСТА И ЕФЕКТИВНО УПРАВУВАЊЕ СО ИТ

Улогата на Работоводниот орган за сигурност на информативниот систем

- **Однесувањето на менаџментот спрема сигурноста на информативниот систем влијае на однесувањето на сите вработени кон сигурноста.**
- Работоводниот орган треба да назначи еден или повеќе лица одговорни за сигурност на информативните системи (ОСИС).
- Работоводниот орган, исто така, има одговорност да обезбеди интегрирање на контролите за сигурност на информативниот систем во комплетниот систем на банката. За да ја обезбеди интеграцијата, работоводниот орган треба да:
  - обезбеди поткрепа на процесот на сигурност со интерни политики и процедури кои се применуваат;
  - обезбеди усогласеност со политиката за информативна сигурност на континуиран и урамнотежен начин низ целата банка;
  - обезбеди тестирање на спроведените контроли на сигурноста на информативниот систем.

МЕСТО, УЛОГИ И ОДГОВОРНОСТИ НА УО, РО И РЕВИЗИЈАТА ВО ПОГЛЕД НА СИГУРНОСТА И ЕФЕКТИВНО УПРАВУВАЊЕ СО ИТ

Улогата на Работоводниот орган за сигурност на информативниот систем

- Работоводниот орган треба да ги земе предвид и улогата и одговорностите на надворешните трети лица. Обезбедувачите на ИТ сервиси на банката, корисниците и други лица кои имаат пристап до информациите или средствата на банката, треба исто така да имаат одговорност за сигурноста, која треба да е јасно дефинирана и определена во договорите за користење на нивните сервиси.

МЕСТО, УЛОГИ И ОДГОВОРНОСТИ НА УО, РО И РЕВИЗИЈАТА ВО ПОГЛЕД НА СИГУРНОСТА И ЕФЕКТИВНО УПРАВУВАЊЕ СО ИТ

Улогата на вработените за сигурност на информативниот систем

- Вработените треба да знаат, да разбираат и да бидат одговорни за исполнување на нивните обврски кон сигурноста
- Вработените треба да имаат потпишани изјави за прифатливо користење на информативниот систем
- Банките треба да работат на подигање на свеста на вработените во поглед на информативната технологија
- Банките треба да обезбедат тренинзи на своите вработени за работа со апликациите и адекватни тренинзи за сигурност

Улогата на Одборот за ревизија, Службата за внатрешна ревизија и Надворешната ревизија

Банката е должна да изврши тестирање на системите и процедурите за контрола, кои се дел од политиката на информативниот систем на банката, од страна на независен и соодветно обучен тим (РЕВИЗИЈА).

Ревизиите треба да се вршат при воспоставувањето на политиката за информативна сигурност, како и периодично, а особено во случај на позначајни измени на политиката за информативна сигурност

Неопходно е службата за внатрешна ревизија и надворешната ревизија во поглед на ИТ да ги следи професионалните стандарди за вршење на овој тип на ревизија, како што се Standards for the Professional Practice of Internal Auditing издадено од Institute for Internal Auditors (IIA) или пак тие кои се издадени од асоцијацијата Information System Audit and Control Association (ISACA). Овие стандарди ги обработуваат независноста, етиката, професионалните вештини, делокругот на работа, изведувањето на ревизијата и контрола на квалитетот на извршената ревизија.

Улогата на Одборот за ревизија, Службата за внатрешна ревизија и Надворешната ревизија

Улогата на УО и Одборот за ревизија

- Проверка на ефикасноста на воспоставените интерни контролни механизми од страна на Работоводниот орган

- Во спроведувањето на оваа функција, покрај Управниот одбор и работоводниот орган, се вклучени и посебни тела во банката: Служба за внатрешна ревизија и Одборот за ревизија.

- Голем број внатрешни контроли се составен дел од информативниот систем на банката. За да може УО да се осигура дека РО воспоставил ефикасни внатрешни контроли може да бара:
  - Вработување на ИТ ревизор во службата за внатрешна ревизија на банката;
  - Извршување на ИТ ревизија од страна на надворешна ревизија;
  - Користење на комбинирана метода.

- Ревизија на сигурноста на информативниот систем се врши и од страна на Народна банка на Република Македонија како супервизорски орган во земјата.

Улогата на Одборот за ревизија, Службата за внатрешна ревизија и Надворешната ревизија

Управниот одбор и Одборот за ревизија треба да ги разгледуваат следните ризици кои се однесуваат на технологијата:

- Неадекватни внатрешни контроли поставени на информативниот систем на банката;
- Нетестирани, неадекватни и неефективни ПКР;
- Финансиски загуби и губење на репутација поврзана со падови на информативните системи (на пр. неработење на шалтери);
- Неавторизирано објавување на доверливи податоци;
- Нерасположиви или скапи имплементации на ИТ решенија;
- Неадекватност на ИТ системите за потребите на банката;
- Неадекватна анализа и неадекватни договори со обезбедувачите на ИТ сервиси на банката;
- Неадекватни системи за набљудување на системите за обработка на трансакциите и системите за чување на податоците;
- Неефективни тренинзи на вработените и корисниците на системите;
- Недостаток на процедури и контроли спрема крајните корисници за работа со информативниот систем (на пр. вработените)

Улогата на Службата за внатрешна ревизија

- **вршење на општи контроли** за кои не е потребно специјалистичко познавање
- **вработување на ИТ ревизор** за вршење на специјалистички т.н. апликативни контроли
- Доколку во Службата за внатрешна ревизија не постои специјализиран ИТ ревизор, тогаш **контролата од страна на Службата за внатрешна ревизија треба да се врши комбинирано со ангажирање на надворешна ИТ ревизија**
- Службата за внатрешна ревизија треба да ја врши контролата на сигурноста на информативниот систем врз основа на **годишен план за ревизија**, одобрен од страна на Управниот одбор. Планот треба да се ревидира во зависност од потребите
- **Методолошки, планот за вршење на ИТ ревизии треба да се заснова на проценка на сите ризици на работењето**, што воедно претставува потврда дека Службата за внатрешна ревизија има разбирање за значајните активности на банката и ризиците што ги носат тие активности.

Улогата на Службата за внатрешна ревизија

Најважни фактори кои може да помогнат во градење на ефикасен систем на проценка на ризици на Службата за внатрешна ревизија во поглед на ИТ се:

- Адекватноста на системите на внатрешни контроли;
- Адекватноста на системите за набљудување од страна на работоводниот орган;
- Претходните забелешки од страна на ревизијата и способноста на работоводниот орган да ги отстрани недостатоците;
- Физичката и логичката сигурност на информативниот систем (опрема и објекти);
- Староста на информативниот систем и банкарските апликации;
- Оперативниот ризик во поединечни организациони единици во банката;
- Фреквенцијата на промени во начинот на извршување на операциите (планирани конверзии на податоци, мигрирање на нови системи, потенцијална финасиска штета);
- Вработени, искуството на работоводниот орган и вработените, техничката компетентност.
- Службата за внатрешна ревизија треба да ги има предвид и наведените фактори, воведувањето на нови активности, производи и иновации, како и ризиците што ги носат новите активности, промената на опкружувањето, унапредувањето на информативните системи и др. Исто така, треба да се земат предвид обемот, природата и фрекфенцијата на задачите што треба да се извршат, периодот од последната ревизија, невообичаените и некарактеристичните промени и други податоци и информации.

Улогата на Службата за внатрешна ревизија

- **Извештаите од извршените ИТ ревизии се доставуваат до Управниот одбор**, Одборот за ревизија, како и до работоводниот орган, директорот на организациониот дел
- **Ревизијата треба да ја следи реакцијата на работоводниот орган** за одредена неправилност и да воспостави соодветен систем за следење на отстранувањето на неправилностите и недостатоците во дадените временски рамки.
- **Службата за внатрешна ревизија може да побара набавка на специјализиран софтвер** за поефикасно вршење на својата функција или пак во соработка со ИТ организационата единица да развие сопствен ревизорски софтвер
- **Службата за внатрешна ревизија не треба да се инволвира во дневните активности на банката**, но нејзините вработени може да учествуваат во постојани и повремени работни комисии како консултанти, набљудувачи и претставници без право на глас.
- **Службата за внатрешна ревизија има право на пристап до сите податоци и документи**, без разлика на начинот и местото каде се чуваат и степенот на нивната доверливост, до сите информативни системи и влез во сите деловни простории без разлика на начинот на кој тие се обезбедени.

Улогата на надворешната ревизија

- Обемот на работа на надворешната ИТ ревизија треба да биде дефинирана во писмото за нивно ангажирање (engagement letter).
- Надворешната ИТ ревизија треба да биде извршена од независен и квалификуван тим, заради постигнување на основната цел за нивно ангажирање. Квалификувани ИТ ревизори претставуваат ревизори кои имаат меѓународни или домашни акредитирани сертификати за вршење на оваа функција.
- За проверка на одредени генерални и апликативни контроли, надворешната ревизија може да користи специјализирани ревизорски софтвери за таа намена. (т.н. COMPUTER ASSISTED AUDIT TECHNIQUES - CAATs).
-
- Како посебен тип на тестирање кое може да се побара од надворешните ИТ ревизори е тестирање на отпорноста на ИТ системот на напади однадвор или одвнатре **т.н. тестови за пенетрација на ИТ системот**.
  - нов engagement letter со точно прецизирани услови и цели
  - на редундантна околина

УПРАВУВАЊЕ СО ИТ

- **Одбор за надгледување на ИТ** - Целта на овој Одбор е да му помага на Управниот одбор во носењето на одлуките во врска со ИТ . Банката треба да води записници
- **Организација на ИТ** – централизиран и децентрализиран пристап
- **Управување со проекти**
- **Менаџмент информативен систем**
- **ПЛАНИРАЊЕ и СТРАТЕГИЈА**
  - Стратешки ИТ планови
  - Оперативни ИТ планови
  - Буџет за ИТ

Управување со проекти

- Ефективно управување со проектите е клучен фактор за добро управувани ИТ операции и успешно следење на конфигурациите.
- Управувањето со проекти зависи од големината и комплексноста на банката, како и од големината и комплексноста на задачата.
- Генерално во секој проект постојат фази како што се:
  - започнување,
  - планирање,
  - извршување,
  - контрола и
  - затворање на проектот, а крајните корисници обука за промените.
- **Менаџментот треба да ја користи оваа техника за да ги контролира проектите кои се од голема важност за банката и кои може да предизвикаат висок оперативен ризик** (надградба и развој на системите, конверзија на податоците од стар систем на нов, воведување на нови инфраструктурни компоненти (нови сервери), воведување нови типови продукти и сервиси, како и подобрување на одредени банкарски апликации или сервиси и др.).

Стратешки ИТ планови

- Стартешките ИТ планови треба да се фокусираат на период од **три до пет години** и треба да се усогласат со деловната долгорочна стратегија на банката

- При дефинирањето на стратешките планови за ИТ, УО и РО треба да ги имаат предвид:
  - позицијата на пазарот;
  - трендовите на развој на банката;
  - технологијата и стандардите;
  - барањата на регулаторните тела;
  - намалувањето на трошоците;
  - подобрувањето на процесите;
  - оптималната инфраструктура за иднината;
  - способноста за прифаќање и интеграција на нови технологии.

Оперативни ИТ планови

- Оперативните ИТ планови треба логички да произлегуваат од стартешкиот ИТ план
- Управниот одбор треба да ги разгледува на годишно ниво

- Потребна е координација на ИТ ресурсите:
  - Инфраструктура
  - Апликативен софтвер
  - Оперативен софтвер
  - Хардвер
  - Вработени

Супервизорски циркулар 9

1	Дефиниција на сигурноста на информативниот систем
2	Процес на информативна сигурност
3	Место и улога на УО, РО и ревизијата
4	**Одговорен за сигурноста на информативниот систем**
5	План за континуитет во работењето
6	Управување со обезбедувачите на ИТ сервиси
7	Утврдување на динамика на имплементација

Одговорен за сигурноста на информативниот систем (ОСИС)

- **ОСИС е одговорен за обезбедување сигурен информативен систем на банката.**
- Да врши анализа и проценка на ризиците кон информативниот систем на банката во согласност со процесот на информативна сигурност;
- Креирање, имплементација и развој на целокупен процес за информативна сигурност
- Креирање, имплементација, унапредување и развој на Планот за континуитет во работењето и Планот за санација на катастрофа
- Да предлага до Управниот одбор политики, стратегии, процедури и упатства со кои се постигнува сигурноста на информативниот систем;
- Координирање на сите сигурносни активности на системот на банката;
- Дава одобрение за вршење на промени кои се изведуваат на информативниот систем на Банката;
- Дава одобрение за привилегиран пристап до системот;

Одговорен за сигурноста на информативниот систем (ОСИС)

- Предлага програма за ревизии во поглед на сигурноста на информативниот систем на банката;
- Врши ревизија на инциденти поврзани со нарушувања на сигурноста на информативниот систем, слабостите и грешките на системот на банката, вклучувајќи и соработка со МВР/НБРМ;
- Соработка/координација со чуварската служба;;
- Дава спецификација на сигурносните услови кои треба да се вметнат во договорите со трети лица во врска со сигурноста на информативниот систем на банката;
- Работи на подигање на свеста за сигурност на информативниот систем и организација на тренизи и обука на вработените за сигурност;
- Помага при извршувањето на ревизии и проверки на сигурноста на информативниот систем, врши оценка и управува со имплементацијата на корективната акција на системот на банката;
- Ги прегледува сите ревизорски траги (аудит логс) и контролни дневници (логс) кои се водат на ниво на банка за одреден период и да гарантира дека тие редовно се одржуваат;
- Ја извршува својата работа во согласност со регулативата и меѓународните стандарди за сигурност на информативните системи;
- Ги разјаснува сите нејаснотии во поглед на сигурноста на информативниот систем на лицата кои работат на системот на банката, врши обука и тренизи во поглед на сигурноста.

Одговорен за сигурноста на информативниот систем (ОСИС)

- Високо образование (Електротехнички факултет-отсек за компјутерска техника или Економски факултет);
- Искуство од банкарско работење;
- Интегритет на личноста;
- Способност да влева доверба и сигурност;
- Добри познавања за информативните системи, закани и ризици;
- Способност да планира и да имплементира промени;
- Способност да објаснува и да ги документира новите концепти и проекти;
- Познавање на системите и процесите кои се случуваат на ниво на цела банка;
- Способност да размислува стратешки;
- Добри организациски способности;
- Добра способност да носи одлуки;
- Добра комуникациска способност ;
- Способност да организира и да води тимска работа.

Одговорен за сигурноста на информативниот систем (ОСИС)

ОСИС треба да го известува управниот одбор на банката најмалку двапати годишно, за статусот на процесот на информативна сигурност.

Извештаите што се доставуваат до Управниот одбор треба да содржат:

- податоци за идентификуваните ризици и нивната контрола,
- информации за договорите со обезбедувачите на ИТ сервиси,
- резултати од извршените тестирања,
- нарушувања во сигурноста на информативниот систем и соодветната реакција од страна на менаџментот,
- како и препораки и иницијативи за промени во политиката за сигурност на информативниот систем на банката, од аспект на нејзино унапредување и модернизирање.

- **ОСИС не треба да биде вработен во ИТ организационата единица, туку за своето работење директно одговара пред работоводниот орган.**

Супервизорски циркулар 9

1	Дефиниција на сигурноста на информативниот систем
2	Процес на информативна сигурност
3	Место и улога на УО, РО и ревизијата
4	Одговорен за сигурноста на информативниот систем
5	**План за континуитет во работењето**
6	Управување со обезбедувачите на ИТ сервиси
7	Утврдување на динамика на имплементација

ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО

- Целта на Планот за континуитет во работењето е минимизирање на финасиската загуба на банката, реставрација и продолжување на сервисноста кон клиентите и намалување на негативните ефекти кои може да влијаат на остварување на стратешките планови на банката (репутација, оперативност, ликвидност, пазарна позиција, и др.).

- Банката треба да овозможи идентификација на критичните операции, вклучувајќи ги и тие каде што банката зависи од надворешни обезбедувачи или трети лица. Банката треба:

  - да идентификува алтернативни механизми за континуитет во деловните процеси во случај на прекин на примарните механизми;
  - да ја идентификува можноста за реставрирање на податоците кои се потребни за продолжување на деловниот процес;
  - податоците да се заштитени на секундарна локација која ќе биде на адекватна далечина од примарната локација, за да се избегне и да се минимизира ризикот двете локации да бидат истовремено недостапни.

ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО

- При развој на Планот за континуитет во работењето банките треба да ги имаат предвид следните цели:
  - планирањето за континуитет служи за одржување, продолжување и реставрација на целиот банкарски процес, а не само за реставрација на технологијата;
  - планирањето за континуитет треба да биде на ниво на цела банка, а не само за информатичкиот дел;
  - темелна анализа на заканите и проценка на ризиците се основа за градењето на ефективен план;
  - ефикасноста на планот може да се верифицира само со тестирање;
  - планот и резултатите од тестот треба да бидат предмет на независна контрола и резултатите треба да бидат разгледани од управниот одбор;
  - повремено треба да се вршат измени во планот како реакција на настанатите промени во банката (нетехнички или технички).

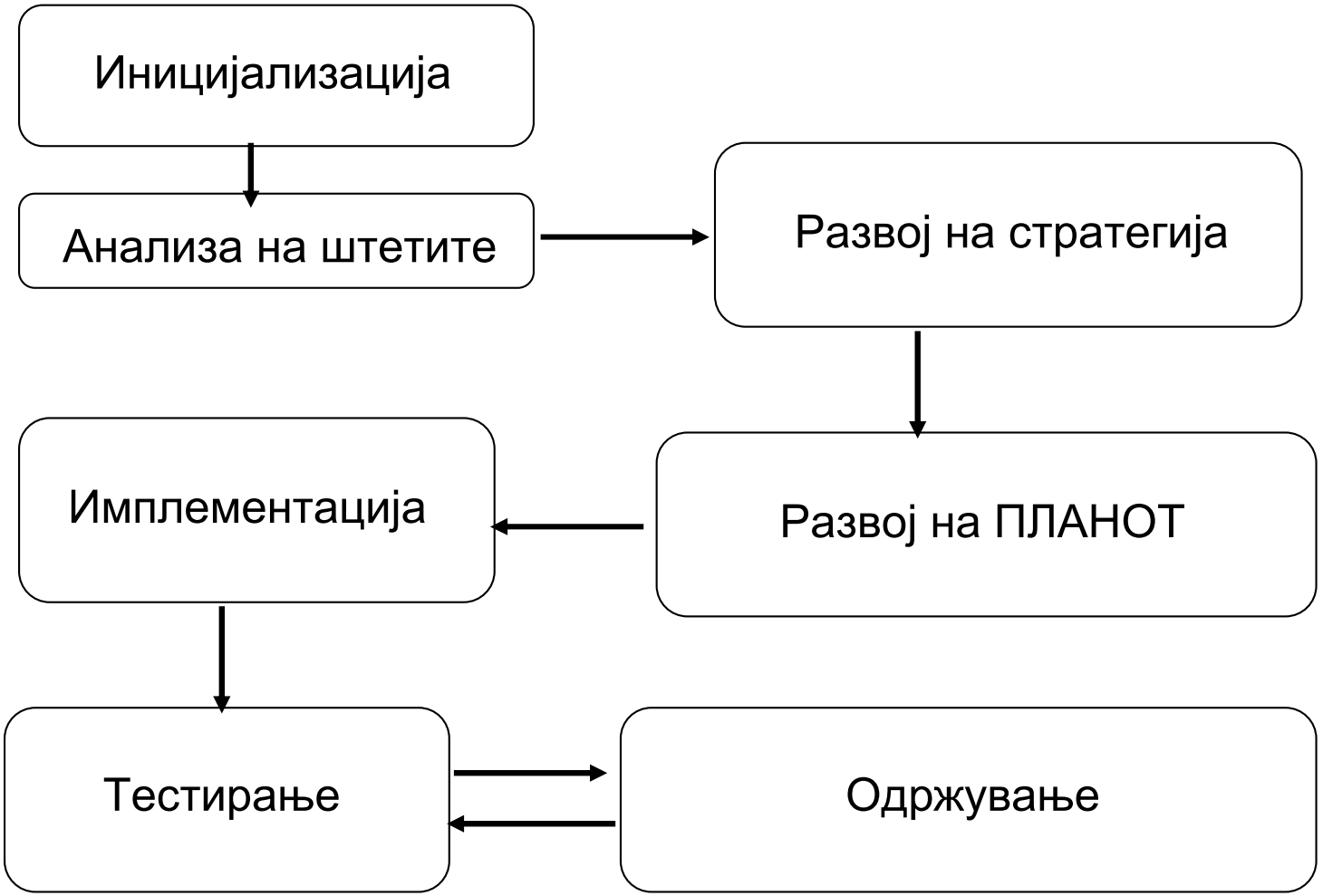
- Отсуството на развиен план за континуитет во работењето значи дека банката во случај на прекин нема да може да ги услужи своите коминтенти на задоволително ниво, **односно дека информативниот систем на банката не го задоволува стандардот за расположивост на системот и оценката за целокупниот информативен систем е НЕСИГУРЕН**.

ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО

Планирањето на континуитет во работење ги опфаќа следните чекори по редослед:

- **Анализа на штетите;**
- **Проценка на ризикот;**
- **Управување со ризикот;**
- **Набљудување.**

Процеси за успешен ПКР



ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО
Анализа на штетите

Анализата на штетите претставува првиот чекор во развој на ПКР. Потребното време за изведување на овој чекор зависи од големината и комплексноста на банката. Анализата на штетите треба да вклучи:

- идентификација на потенцијалната штета од неконтролирани настани на банкарските операции;
- земање предвид на сите банкарски операции, а не само на операциите кои се изведуваат со помош на информатичка опрема;
- определување на коефициент на максимално дозволено време на нефункционирање на системот (MTD-Maximum Tolerable Downtime) и евентуалната финансиската загуба на банката.

ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО
Анализа на штетите

Проценката на максимално дозволеното време на нефункционирање на системот може да се движи во следните граници:

вид на операција		**МТД**
▪ критични операции	=	минути до часови
▪ итни операции	=	24 часа
▪ важни операции	=	72 часа
▪ нормални операции	=	7 дена
▪ неважни операции	=	30 дена

- **На овој начин**, банката ќе согледа кои се критичните системи и операции без кои не може да опстане и колку долго може да го толерира нивното нефункционирање.

ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО
Анализа на штетите

При одредување на критичноста на операции во одредена организациона единица треба да се земе во предвид:

- Дали во вашата организациона единица има некоја специјализирана опрема и како се користи?
- Како ќе работи вашата организациона единица, доколку не работи главниот сервер на податоци, или е во прекин компјутерската мрежа?
- Како зависи вашата организациона единица од работата на други организациони единици во банката или од надворешни трети лица?
- Дали постојат слабости во одделот и кои се ризиците поврзани со тоа?
- Дали за извршување на критичните операции се потребни обезбедувачи на услуги од областа на информативната технологија?
- Кој е минималниот број на вработени и колкав простор ќе ви биде потребен на алтернативната локација? (организационата единица да продолжи со работа на секундарна локација)
- Какви комуникациски уреди ќе бидат обезбедени на алтернативната локација?
- Дали вработените имаат тренинг и знаење за извршување на други задолженија во вашата организациона единица?

ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО
Управување со ризик

Специфичните сценарија треба да предвидат како ќе реагира банката доколку:

- клучните вработени не се достапни;
- критичните објекти и згради не се достапни;
- настане дефект на опремата (хардверска, телекомуникациска);
- програмите или податоците не се достапни или се со грешка;
- поддршката од обезбедувачот на ИТ сервиси е недостапна;
- прекин на електрична енергија и телекомуникации;
- критична документација или податоци не се достапни.
- Банките треба да предвидат дека нивните објекти може да бидат недостапни или тешко оштетени, а клучните луче (на пример: работоводниот орган на банката) нема да бидат достапни веднаш, по прекинот на операциите.

- **Банките треба да предвидат дека нивните објекти може да бидат недостапни или тешко оштетени, а клучните луче (на пример: работоводниот орган на банката) нема да бидат достапни веднаш, по прекинот на операциите.**

ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО
Набљудување на ризиците и тестирање

Набљудувањето на ПКР претставува континуиран процес. Ефикасноста на ПКР треба да се осигура преку:

- **тестирање на ПКР најмалку еднаш годишно**;
- ПКР и резултатите да бидат разгледувани од Службата за внатрешна ревизија;
- континуирано одржување на планот како се менува Банката и условите

- Работоводниот орган треба да ги дефинира функциите, системи и процеси ќе бидат тестирани и кои се целите кои сака да ги постигне. Работоводниот орган треба да **припреми пишан план за тест на ПКР**. Целта на тестирањето е да се обезбеди дека ПКР е точен, релевантен и функционален и покрај "тешките околности" кои може да предизвикаат тежок прекин на деловните процеси.

- **Пишаниот план за тестирање на ПКР** треба да има предвид:
  - Да не го загрози нормалното работење на банката;
  - Да се зголемува систематски комплексноста и бројот на вклучени вработени, функции и сервиси;
  - Откриените неадекватности да бидат променати и поправени

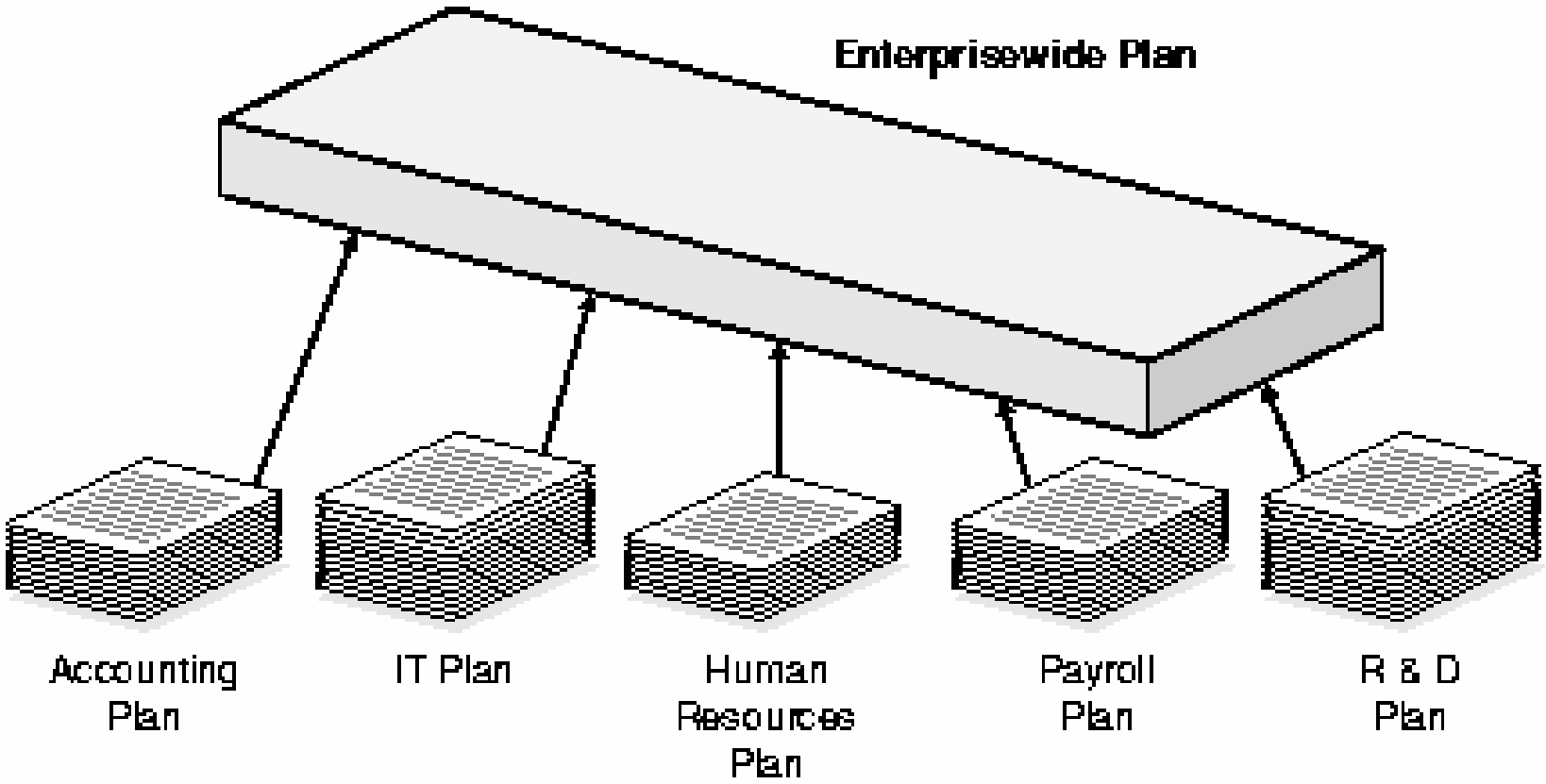
ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО
Набљудување на ризиците и тестирање

- Надзорот од страна на Службата за внатрешна ревизија ќе обезбеди валидност на процесот на тестирање и независност во известувањата до Управниот одбор.

- Успешен тест ќе биде оној во кој резултатите од тестот се анализирани и споредени со однапред дефинирани цели во Планот за тест на ПКР. Работоводниот орган треба да го извести Управниот одбор за резултатите од тестот и за начинот на кој ќе ги решава недостатоците.

- **Управниот одбор треба да го ревидира ПКР најмалку еднаш годишно.**

ПЛАН ЗА КОНТИНУИТЕТ ВО РАБОТЕЊЕТО
може да биде составен од поединечни планови на ПКР



Приоритети

Број 1 приоритет при иницирање на Планот за континуитет во работењето е

- Безбедноста на луѓето

Број 1 појава после секоја катастрофа е:

- Кражби и вандализам

Супервизорски циркулар 9

1	Дефиниција на сигурноста на информативниот систем
2	Процес на информативна сигурност
3	Место и улога на УО, РО и ревизијата
4	Одговорен за сигурноста на информативниот систем
5	План за континуитет во работењето
6	**Управување со обезбедувачите на ИТ сервиси**
7	Утврдување на динамика на имплементација

Управување со обезбедувачите на ИТ сервиси

- **Банките треба да вршат набљудување на квалитетот на сервисот и финансиската ситуација на надворешната компанија која им овозможува извршување на критични ИТ операции.**

- Како Обезбедувачи на сервиси за банките најчесто се јавуваат компании, меѓутоа може да бидат и други финасиски установи (пример: НБРМ со системите за платен промет, КИБС, Процесинг центар за картично работење, и др.).

- **Банките треба да обезбедат тековна информација од нивните Обезбедувачи на сервиси за да можат да направат целосна анализа на бонитетот и финансиската ситуација на своите обезбедувачи најмалку еднаш годишно.** Обврската за доставување на финасиските извештаи (пожелно е финасиските извештаи да се независно ревидирани) треба да биде дел од обврските во дефинирани во договорот за соработка.

Договори со обезбедувачот на ИТ сервиси

Банките треба да направат писмен договор кој треба да содржи и податоци за:

- оптималните перформанси на сервисот и неговата сигурност и доверливост;
- обврската за доставување на финансиски извештаи;
- обврските кои треба да ги исполни обезбедувачот на ИТ сервиси, со цел банката да биде усогласена со прописите, политиките и процедурите за обезбедување на информативната сигурност;
- линиите на комуникација и известување помеѓу банката и обезбедувачот на ИТ сервиси.

Управување со обезбедувачот на ИТ сервиси

Банките треба да ги дефинираат условите за работа со обезбедувачите на ИТ сервиси преку:

- Дефинирање на единствени принципи на избор на обезбедувачи и следење на финасиските извештаии на своите обезбедувачи на ИТ сервиси;
- Договорите помеѓу банката и обезбедувачот на ИТ сервиси да имаат вградени заштитни механизми за имплементација на политиката за информативна сигурност;
- Обезбедувачите на ИТ сервиси треба да работат во согласност со одредени стандарди за сигурност на информативниот систем, за да можат банките со кои работат тие да се усогласат со стандардите пропишани од страна на Народна Банка на Република Македонија.
- Да се дефинира обврска за неоткривање на информациите и чување на банкарската тајна и на соодветните лица од обезбедувачот на ИТ сервиси кои имаат пристап до информативниот систем на банката (на пр.: лицата кои имаат пристап од страна на обезбедувач на ИТ сервиси треба да имаат потпишана изјава за прифатливо користење на информативниот систем на банката пред да им се даде пристап до системот на банката);

Управување со обезбедувачот на ИТ сервиси

- Банката треба да бара од својот обезбедувач на ИТ сервиси да врши независни тестирања на сигурноста од стручни тимови или службата на внатрешна ревизија да има пристап до организационата единица на обезбедувачот каде што банката го изнајмува ИТ сервисот;

- Банките треба да бараат од сопствените обезбедувачите на ИТ сервиси да развијат сопствени ПКР и коишто треба да се во координација со ПКР на банката. Банката треба да ги добива резултатите од извршените тестови или извршени ревизии на ПКР за да направи промени во сопствениот ПКР и да воспостави поефектни процеси за тестирање. **Планот за ПКР на банката доколку е зависен од ПКР на обезбедувачите на ИТ сервиси треба да вклучи и контакти кои банката ќе може да ги оствари на примарната и алтернативната локација на обезбедувачот на ИТ сервиси**

- Банката треба да реагира при сигурносни инциденти во координација со обезбедувачот на ИТ сервисите доколку банката била алармирана преку системите за набљудување дека инцидентот доаѓа од страна на обезбедувачот на ИТ сервиси. Банката треба да го пријави инцидентот во НБРМ, најдоцна пет дена после неговото случување;

Договори за одржување на информативниот систем

- Доколку поддршката на системот не може да се обезбеди преку локална експертиза во самата банка или не може да одговори на деловните барања на одредени организациони единици (на пр. минимално време на одзив од моментот на настанување на проблемот), тогаш банката треба да склучи договор за одржување на системот со реномирана компанија со седиште во РМ.

- Банката може да склучи договор за одржување со реномирана меѓународна компанија која е надвор од РМ, меѓутоа треба да обезбеди сигурен електронски начин на поврзување и теледијагностика на проблемите и ефектен начин на нивно решавање. **Доколку поддршката на системот не може да се реализира ефикасно и сигурно преку електронска врска со банката, обезбедувачот кој се избира за ИТ одржување на системот кои се од редот на реномирани фирми, МОРА да има седиште или претставништво во РМ.**

Супервизорски циркулар 9

1	Дефиниција на сигурноста на информативниот систем
2	Процес на информативна сигурност
3	Место и улога на УО, РО и ревизијата
4	Одговорен за сигурноста на информативниот систем
5	План за континуитет во работењето
6	Управување со обезбедувачите на ИТ сервиси
7	**Утврдување на динамика на имплементација**

Утврдување на динамика на имплементација

- Почетната обврска на сите банки е да назначат ОСИС. ОСИС треба да бидат лица со познавање на технологијата на банката, познавање на сите процедури и упатства кои важат во банката и соодветната законската регулатива. Банките требаше да назначат ОСИС заклучно со декември 2004 година согласно со точка 22 од Одлуката за дефинирање на стандардите за изготвување и спроведување на сигурноста на информативниот систем.

- Во наредната фаза треба да се направи почетниот чекор во имплементација на политиката, а тоа е општа и целосна АНАЛИЗА и ОЦЕНКА на РИЗИЦИТЕ на информативниот систем на банката. Оваа материја треба да ги опфати сите можни сценарија по средствата на информативниот систем на банката. (**август/септември** 2005).

- Врз база на оваа спроведена анализа на ризиците, банката треба да воспостави адекватни политики, стандарди, упатства и соодветни процедури за да се комплетира програмата за сигурност на информативниот систем (**ноември** 2005).

- Целокупниот материјал на спроведената анализа и оценка на ризиците, формалната политиката за сигурност на информативниот систем и адекватните останати политики, стандарди, упатства и процедури да се достават за согласност во НБРМ заклучно со **ноември** 2005 **година**.

Утврдување на динамика на имплементација

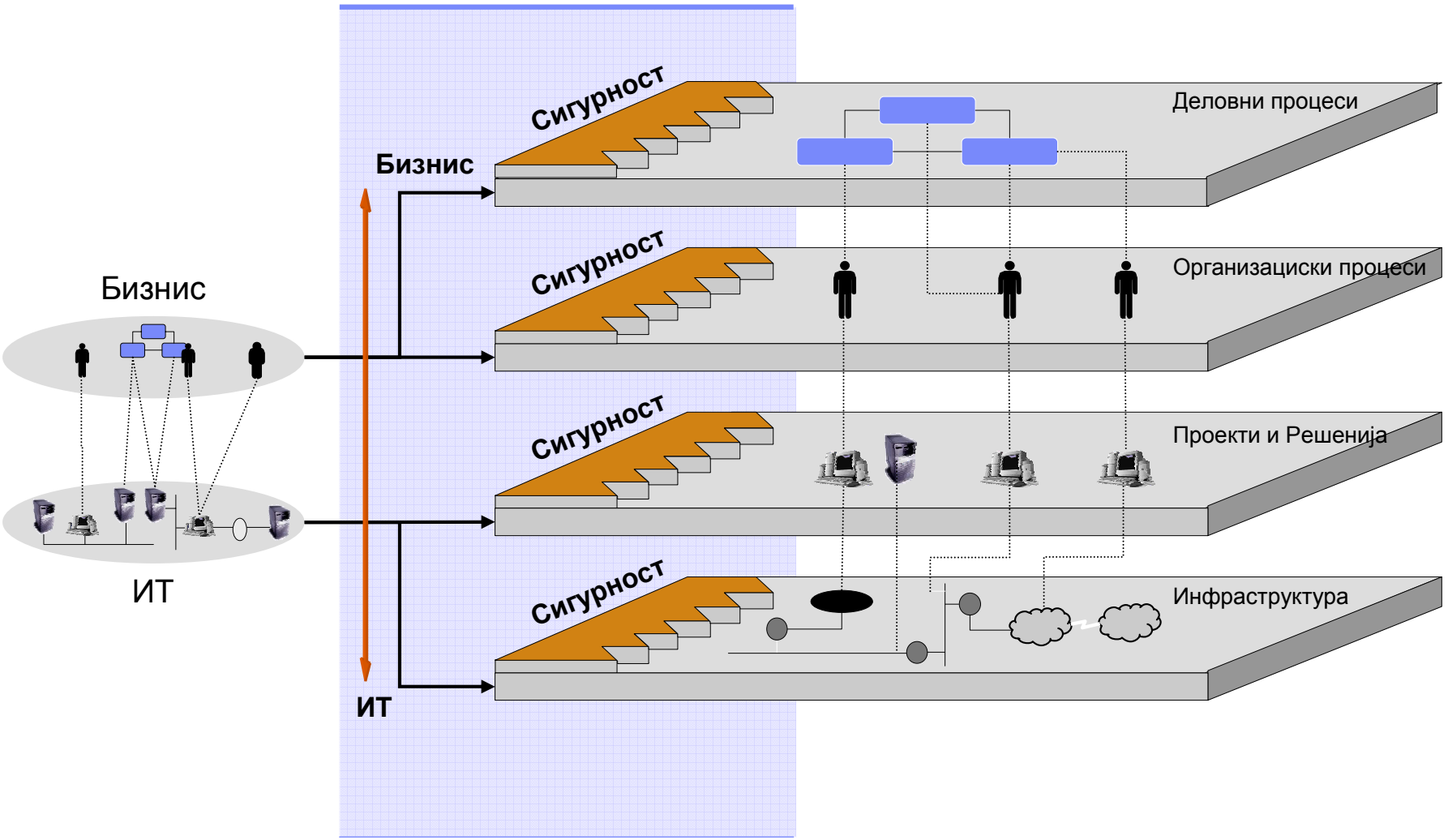
- Секундарната локација на банката **не мора да биде во посед на банката**, туку овие услуги може и да се изнајмуваат од адекватен обезбедувач на ИТ сервиси.

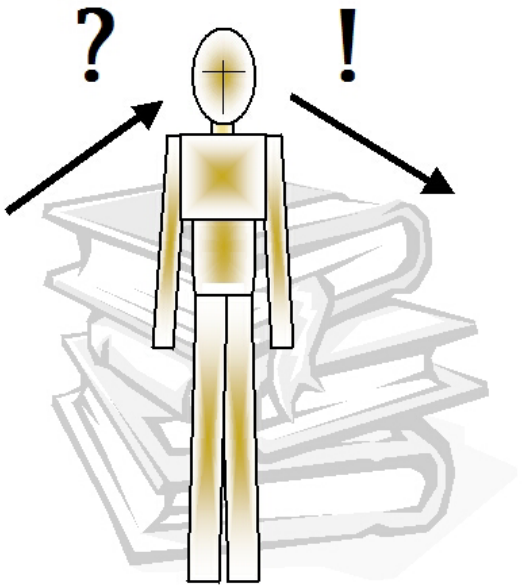
- **За банката е важно да има можности непречено да врши тестирање на ПКР**, како и при случај на тежок прекин на деловните процеси да може да се префрли во избраната локација и да ги реставрира во најкус можен рок своите операции.

- **Планот за континуитет во работењето** согласно со инфраструктурните решенија на банката, соодветните тимови и политики, процедури, упатства во поглед на ова прашање треба да бидат завршени до **ноември** 2005 **година** и да се достават заедно со материјалот за политиката за информативна сигурност за добивање на согласност во НБРМ.

- При одбирањето на алтернативната локација, треба да се внимава таа да е на адекватна оддалеченост од примарната локација, за да не може двете локации да бидат оштетени од истата закана. Се препорачува алтернативната локација да биде оддалечена **најмалку** 30 **километри** од примарната локација за да се обезбеди максимална заштита во случаи на регионални несреќи и катастрофи.

ИТ - ОПЕРАТИВЕН РИЗИК ВО BASEL II





КОНТАКТ

Горан Јанкоски, CISSP,
самостоен супервизор

Дирекција за
Супервизија

тел.: +389 23 108241

факс.: +389 23 108348

jankoskig@nbrm.gov.mk
supervizija@nbrm.gov.mk