Direkcija za supervizija

CIRKULAR ZA SIGURNOSTNA INFORMATIVNIOT SISTEM NA BANKATA

juli, 2005

Sodr`ina

Voved

Voobi~aen na~in na tolkuvawe na odredeni novini i pra{awa od domenot na bankarski praktiki i standardi e preku izrabotka na supervizorski cirkulari. Ovie cirkulari sodr`at odredeni nasoki i preporaki koi se rezultat na sumirawe na soznanijata na Narodna banka na Republika Makedonija za primenata na me|unarodnite supervizorski standardi, kako i karakteristikite na bankarskiot sistem i bankarskata regulativa vo Republika Makedonija.

Za razlika od supervizorskite standardi koi se reguliraat so zakonskata i podzakonskata ramka i imaat zadol`itelen karakter, supervizorskite cirkulari se vo nasoka na obezbeduvawe poefikasen na~in za ispolnuvawe na propi{anite supervizorski standardi, odnosno ispolnuvawe na odredni zakonski obvrski. Imeno, so izmenite na Zakonot za bankite izvr{eni vo tekot na juni 2002 godina, Narodna banka na Republika Makedonija e obvrzana da propi{uva standardi za izgotvuvawe i sproveduvawe na sigurnosta na informativniot sistem na bankite. Vrz osnova na vakvite odredbi, vo dekemvri 2003 godina, Sovetot na Narodna banka na Republika Makedonija donese Odluka za definirawe na standardite za izgotvuvawe i sproveduvawe na sigurnosta na informativniot sistem na bankite ("Slu`ben vesnik na RM" br. 77/2003) so koja podetalno se opredeluvaat standardite za upravuvawe i kontrola na rizicite zna~ajni od aspekt na sigurnosta na informativniot sistem, kako i standardite za obezbeduvawe na kontinuitet vo raboteweto na bankite. Taka, osnovot za donesuvawe na ovoj supervizorski cirkular proizleguva od to~ka 22 od Odlukata za definirawe na standardite za izgotvuvawe i sproveduvawe na sigurnosta na informativniot sistem na bankite. Pri izrabotkata na ovaa Odluka, kako i pri izrabotkata na ovoj cirkular, se koristea preporakite i nasokite sodr`ani vo Me|unarodniot standard za upravuvawe so sigurnosta na informativniot sistem (***BS7799-2:2002,*** odnosno ***ISO/IEC17799:2000E***) i Bazelskiot dokument za upravuvawe so operativniot rizik[1].

Narodna banka na Republika Makedonija e zainteresirana za vospostavuvawe na solidni standardi vo pogled na sigurnosta na informativnite sistemi. So primena na ovie standardi }e se obezbedi zgolemena bezbednost na informaciite koi se ~uvaat vo informativniot sistem i povisok stepen na integritet na podatocite pri razli~ni vidovi obrabotki. Neophodno e informativniot sistem na bankite da im e raspolo`iv odnosno dostapen na vrabotenite i na komintentite za nepre~eno odvivawe na bankarskite operacii, kako i na organite na upravuvawe za nosewe prudentni odluki, vo ramkite na svoite delovni potrebi i dozvoleni avtorizacii.

Ovoj cirkular nema ambicii da gi pokrie site aspekti na upravuvawe so sigurnosta na informativniot sistem, tuku pred se, da slu`i kako nasoka vo definiraweto i vospostavuvaweto na adekvatni standardi za obezbeduvawe sigurnost na informativniot sistem, definirawe na pravata i odgovornostite na licata koi se nositeli na sigurnosta na informativniot sistem i vrz taa osnova da ovozmo`i sledewe na utvrdenite zakonski normi za sigurnosta na informativniot sistem od strana na bankite vo Republika Makedonija.

[1] Sound Practices for the Management and Supervision of Operational Risk (Basle Committee Publications No.96 – February 2003)

Cirkularot e struktuiran vo slednite segmenti:

1. **Definicija na sigurnosta na informativniot sistem**
2. **Proces na upravuvawe i kontrola na rizicite od aspekt na sigurnosta na informativniot sistem (vo ponatamo{niot tekst: Proces na informativna sigurnost);**
3. **Mesto, uloga i odgovornosti na Upravniot odbor, rabotovodniot organ i revizijata;**
4. **Odgovoren za sigurnosta na informativniot sistem (OSIS);**
5. **Plan za kontinuitet na raboteweto;**
6. **Upravuvawe so obezbeduva~ite na servisi od oblasta na IT;**
7. **Utvrduvawe na dinamika na implementacija.**

1. DEFINICIJA na sigurnosta na informativniot sistem

CEL

Celta za vospostavuvawe na standardite za sigurnost na informativniot sistem e da se obezbedi neprekinatost na delovnite operacii i minimizirawe na eventualnata {teta koja bi ja pretrpela bankata so aktivna i preventivna implementacija na kontroli so koi }e se namalat rizi~nite efekti koi mo`at da bidat predizvikani so pojava na sigurnosni incidenti.

DEFINICIJA

Informacijata e sredstvo koe e od golemo zna~ewe za bankite i zatoa treba da bide soodvetno za{titena. Obezbeduvaweto na sigurnosta na informativniot sistem }e ja {titi informacijata od razli~ni tipovi na zakani za da se obezbedi deloven kontinuitet, da se minimizira {tetata pri raboteweto i da se maksimizira prihodot od davaweto bankarski uslugi.

Informacijata mo`e da postoi vo mnogu formi. Taa mo`e da bide pe~atena ili napi{ana na hartija, da se ~uva vo kompjuter da se prenesuva preku po{ta ili so koristewe na elektronski sredstva, da se prika`e na filmovi ili da se ka`e vo razgovor.

Informativnite sistemi se pove}e se soo~uvaat so zakani i izlo`enost na rizici od razni izvori, vklu~uvaj}i izmami so pomo{ na kompjuter, {piona`a, hakerstvo, a novite virusi se se po~esti, poambiciozni i se posofisticirani.

Bez ogled na formata na informacijata ili sredstvata preku koi se prenesuva ili se ~uva, taa treba sekoga{ da bide soodvetno za{titena.

Sigurnosta na informativniot sistem se definira kako obezbeduvawe na:

1. **Doverlivost**- informacijata ime dostapna samo na onie koi{to imaat ovlasten pristap do nea. Bankata e dol`na da vospostavi procesi, proceduri i kontroli koi }e se upotrebuvaat za da se za{titat informaciite od neavtoriziran pristap;

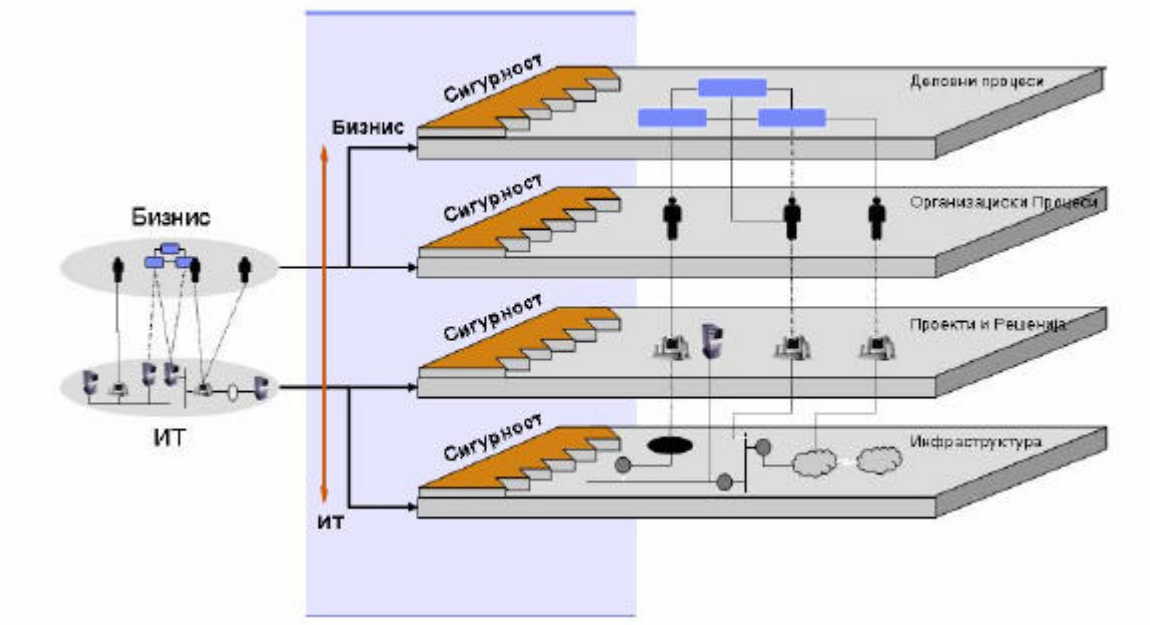
2. **Integritet**- za{tita na to~nosta i kompletnosta na informacijata i na metodite na obrabotka. Bankata e dol`na da vospostavi procesi, proceduri i kontroli koi }e se koristat so cel da se spre~i menuvawe na infomacijata na neovlasten na~in i so neavtorizirano rakuvawe so sistemite, koe mo`e da ja naru{i to~nosta, kompletnosta i verodostojnosta na informacijata;

3. **Raspolo`ivost**- ovlastenite korisnici imaat pristap do informacijata i do drugite pridru`ni sredstva potrebni za nejzina prezentacija, koga za toa ima delovna potreba. Bankata e dol`na da vospostavi procesi, proceduri i kontroli koi }e se primenuvaat za da mo`at ovlastenite korisnici da imaat pristap do informacijata i sistemite koga za toa imaat delovna potreba.

Doverlivosta, integritetot i raspolo`ivosta na informaciite mo`at da bidat od su{tinsko zna~ewe za odr`uvawe na konkurentnosta, likvidnosta, profitabilnosta, pravnata usoglasenost i na reputacijata na bankata.

Dokolku eden od ovie principi e neispolnet ili e naru{en se smeta deka informativniot sistem na bankata NE E SIGUREN.

Za da se obezbedi sigurnost na informativniot sistem, treba da se izgradi KONTINUIRAN PROCES za informativna sigurnost i da se dade SILNA poddr{ka od strana na organite na upravuvawe na bankata. Vo procesot treba da se obezbedi adekvatno u~estvo na site vraboteni i istiot da se sprovede na nivo na celata banka, bidej}i sigurnosta na informativniot sistem NE MO@E da se postigne samo so tehni~ki sredstva.



Slika 1. Sigurnosta na informativniot sistem vo bankata ne mo`e da se postigne samo so tehni~ki sredstva

2. PROCESNA INFORMATIVNA SIGURNOST

Bankata treba da vospostavi KONTINUIRAN proces za informativna sigurnost i da gi opredeli ulogite i odgovornostite na organite na upravuvawe i vrabotenite.

Procesot za informativna sigurnost e metodologija {to }e ja koristi bankata za implementacija i realizacija na celite so koi se postignuva sigurnosta na informativniot sistem. Procesot treba da e dizajniran na na~in {to }e ovozmo`i da se identifikuvaat, merat, kontroliraat i da se sledat rizicite, povrzani so doverlivosta, integritetot i raspolo`ivosta na sistemite i podatocite.

Ovoj proces treba da gi sodr`i slednite celini (subprocesi):

1. **Procenka na rizikot-** Bankata e dol`na da izgradi kontinuiran proces na identifikacija na slabostite i zakanite kon svoite informativni sistemi. Procesot treba da ja identifikuva mo`nosta i frekvencijata na pojavuvawe na zakanite za da se utvrdi eventualnata {teta koja bi nastanala dokolku istite se slu~at;
2. **Politika za sigurnost na informativnite sistemi-** Bankata e dol`na da donese politika za sigurnost na informativniot sistem koja }e pretstavuva **STRATEGIJA** (plan) na menaxmentot za upravuvawe so identifikuvanite rizici (od prethodniot ~ekor) za sigurnosta na informativniot sistem na bankata;
3. **Implementacija na sigurnosni kontroli-** Bankata e dol`na da vospostavi administrativni, fizi~ki i tehni~ki kontroli so koi }e se izvr{i za{tita na sigurnosta na informaciite i sistemite na pove}e nivoa;
4. **Testirawe na sigurnosta-**Bankata e dol`na da vospostavi proces na profesionalno, nezavisno i objektivno testirawe na efikasnosta i adekvatnosta na implementiranite kontroli sodr`ani vo politikata za informativna sigurnost.
5. **Nabquduvawe i nadgradba-**Bankata e dol`na da vospostavi proces na kontinuirano pribirawe i analiza na informacii od aspekt na novite zakani i slabosti, aktuelni napadi kon bankata ili kon drugite finansiski institucii kombinirani so efikasnosta na postojnite sigurnosni kontroli. Nabquduvaweto i nadgradbata }e go napravat procesot na informativna sigurnost

2.1. Procenka na rizik

Bankata mora da odr`uva kontinuiran proces na procenka na rizicite kon informativnata tehnologija, koj gi podrazbira slednite ~ekori:

- **Identifikacija** na sredstvata na informativniot sistem na bankata (vidovi informacii i tipovi sistemi za prenos na informaciite);
- **Klasifikacija** na sredstvata na informativniot sistem na bankata (dodeluvawe na vrednost na sredstvata);
- **Analiza na verojatnosta na pojava na zakanite i slabostite na sistemot i koi se mo`nite posledici** po informativniot sistem na bankata;
- **Dodeluvawe prioritet** vo zavisnost od goleminata na rizikot.

**Procenkata na rizikot kon sigurnosta na informativniot sistem e ~ekor na identifikacija na rizicite kon doverlivosta, integritetot i raspolo`ivosta na informativnite sistemi.** Procesot na procenka na rizik e neophoden ~ekor za formirawe na strategija i politika za sigurnost na informativnite sistemi. Po~etnata procenka na rizik mo`e da bara zna~itelen ednokraten napor, me|utoa vo natamo{niot period taa treba da se odviva vo kontinuitet.

2.1.1. Identifikacija na sredstvata na informativniot sistem na bankata

Sredstvata na informativniot sistem se va`ni za bankata. Zatoa, tie treba da bidat soodvetno za{titeni za da se obezbedat kontinuirani i to~ni bankarski operacii.

Identifikacijata na sredstvata koi se del od informativniot sistem na bankata opfa}a analiza na {irok spektar informacii koi se va`ni za funkcioniraweto na bankata. Sekoe sredstvo koe e del od informativniot sistem na bankata vo ovoj ~ekor treba da bide jasno identifikuvano, a negovata pripadnost definirana.

Kako primeri na sredstva na informativniot sistem na bankata, vo smisla na ovoj cirkular, mo`e da bidat:

- **Elektronska dokumentacija**-sistemska dokumentacija, upatstva za koristewe, operativni proceduri, planovi, treninzi;
- **Pi{ana dokumentacija**-dogovori, upatstva, pi{ani kreditni dosieja, dokumenti koi sodr`at va`ni i doverlivi podatoci za bankata;
- **Softverski sredstva**-aplikacii, sistemski programi, razvojni alatki;
- **Fizi~ki sredstva**-kompjuteri i komunikaciska oprema, magnetni mediumi(kaseti i diskovi), druga tehni~ka oprema (agregati, erkondi{ni), mebel;
- **^ove~ki faktor**-vrabotenite;
- **Servisi**-kompjuterski i telekomunikaciski servisi {to gi koristi bankata, vklu~uvaj}i i elektri~na energija i telekomunikaciski povrzuvawa;

Rezultat od ovoj ~ekor treba da bide t.n."informativna kniga" so site sredstva koi se smetaat za glavni delovi na informativniot sistem na bankata, nivnata lokacija i nivnata pripadnost.

Del od ovaa celosna informativna kniga treba da pretstavuva TEHNI^KATA INFORMATIVNA KNIGA koja }e gi opfati celosniot hardverski, softverski i telekomunikaciski inventar na bankata, kako i nejziniot mre`en dijagram.

Rabotovodniot organ mora da ima osnovno poznavawe na najva`nite komponenti na sistemot i na~inot na prenos i tek na informaciite niz sistemot.

Primer za korisni informacii koi mo`e da se skladiraat vo **hardverskata informativna kniga**:

- **za serveri**
  - proizvoditel i model
  - kapacitet na procesorot vo milioni instrukcii vo sekunda (MIPS)
  - glavna memorija (RAM)
  - memorija (HDD, lenti, silosi na lenti, ...)
  - mre`na povrzanost
  - funkcija
  - lokacija

- **za personalni kompjuteri (desktop)**
  - proizvoditel i model
  - koj go ima (poseduva) i so koja cel
  - mre`na povrzanost
  - povrzuvawe so nadvore{ni mre`i (modem ili bez`i~na karti~ka)
  - lokacija

- **za mre`ni uredi**
  - proizvoditel i model
  - tip
  - IP adresa

Postojat najmalku tri tipa na podelbi na **softverskiot inventar** i toa: **operativni sistemi, aplikativen softver i t.n. back-office softver**.

Aplikativniot softver gi opfa}a glavnite bankarski programi, kako i glavnite aplikacii koi se koristat vo bankata za rabota na personalnite kompjuteri. Vo t.n. back-office softver treba da se smestat site ostanati aplikacii koi se koristat vo slu~aj na poddr{ka na primarnite aplikacii (primer: softver za upravuvawe so bazata, softver za za{tita na podatoci, antivirus softver, internet serveri i softver za poddr{ka na aplikaciite i softver za kontrola na gre{ki i nepravilnosti i itn.).

Primer za korisni informacii koi mo`e da se skladiraat vo **softverskata informativna kniga**:

- ime na aplikacijata (pr. Glavna kniga, naselenie,...)
- proizvoditel ili nabavuva~
- seriski broj
- verzija na aplikacijata (Version level)
- verzija na nadogradbata (Patch level)
- Broj na instalirani kopii
- Broj na poseduvani licenci
- Tip na licenca

Mre`nata infrastruktura na bankata e od va`nost za neprekinato odvivawe na delovnite operacii. **Bankata mora da poseduva mre`en dijagram na svojot informativen sistem, koj vo celost }e go prika`uva povrzuvaweto na site komponenti na informativniot sistem**. Mre`nata povrzanost treba da sodr`i dovolno detali za:

- identifikuvawe na site vnatre{ni i nadvore{ni povrzuvawa (vklu~uvaj}i go internet, modemi, bez`i~no povrzuvawe,...)

- da go opi{e na~inot i tipot na povrzuvawe (DSL, ADSL, dialup, wireless)
- da ni go prika`e kapacitetot na vrskata pome|u povrzuvawata (bandwith)
- identifikuvawe na enkriptiranite kanali ili na drug na~in kanali za sigurna komunikacija
- da ni go prika`e tipot i kapacitetot na mre`nite povrzuva~i (switches, routers, hubs)
- da ni gi prika`e glavnite komponenti za sigurnost na informativnite sistemi (ogneni yidovi-"firewalls", sistemi za detekcija i prevencija na napad-"Intrusion Detection&Prevention Systems" i t.n. "honey pots"-sistemi za namamuvawe, dokolku se instalirani)
- da ni gi prika`e otvorenite kanali (porti) za komunikacija pome|u mre`nite uredi (**NAPOMENA: vo bankite treba da se otvoreni samo kanlite(portovite) za komunikacija za koi ima delovna potreba, a site ostanati treba da se ZATVORENI. Obratete vnimanie deka golem broj tehni~ki uredi fabri~ki se ispora~uvaat so otvoreni kanali (portovi) za komunikacija**).

2.1.2 Klasifikacija na sredstvata na informativniot sistem na bankata

Klasifikacijata i vrednuvaweto na sredstvata e najva`niot faktor vo sproveduvaweto na uspe{na analiza na rizici.

Za taa cel treba da se identifikuvaat osnovnite kriti~ni komponenti na sistemot, odnosno da **se prepoznaat negovite granici, da se utvrdi ~ustvitelnosta i va`nosta na hardverot i softverot, informaciite koi se ~uvaat, procesiraat i se transportiraat.**

Klasifikacijata na sistemot pretstavuva raslojuvawe na informativniot sistem sprema ~ustvitelnosta na informacijata. Bankite treba da odlu~at kakva }e bide nivnata klasifikacija na informaciite i kako }e bidat za{titeni. Dokolku ne postoi vrednuvawe na ~ustvitelnosta na sredstvata i informaciite, toga{ }e se smeta deka site sredstva i informacii se od najvisok rang na ~ustvitelnost i za site niv treba da se primenat soodvetni sigurnosni kontroli.

Klu~en del vo klasifikacijata na sredstvata e **rangirawe na podatocite, dokumentite i sistemite** spored nivnoto zna~ewe za uspe{no izvr{uvawe na operaciite na bankata i od mo`nata {teta koja mo`e da se predizvika koga ~ustvitelna informacija ne se ~uvala na adekvaten na~in, kako na primer:

- delovna tajna, slu`bena tajna;
- javni, interni, doverlivi, strogo doverlivi sredstva ili dokumenti, itn;

Rangiraweto i vrednuvaweto na dokumentite treba da se napravi zaedno so vrabotenite vo bankata koi neposredno rakuvaat so niv. Vrabotenite ja znaat vistinskata zaguba i mo`nata {teta koja mo`e da ja pretrpi bankata od neadekvatnoto rakuvawe so ~ustvitelnata dokumentacija.

Vrednosta {to }e im se dodeli na sredstvata na informativniot sistem treba da bide vo korelacija so tro{okot od nabavka i odr`uvawa na sredstvoto i udarot koj mo`e da se predizvika so zaguba na doverlivosta, integritetot i raspolo`ivosta na sredstvoto kon bankata. Bankata treba da izgradi sopstvena skala na vrednosti za sredstvata na informativniot sistem koi }e ni ja pretstavuvaat zagubata na bankata od naru{enost na doverlivosta, integritetot i raspolo`ivosta, kako na primer:

- mala, sredna i visoka ili
- mnogu mala, mala,sredna, visoka, mnogu visoka.

Bankata treba da gi definira svoite vrednuvawa i limiti za uspe{no izvr{uvawe na klasificiraweto na sredstvata na informativna sigurnost.

Kako rezultat na ovoj ~ekor vo "informativnata kniga" treba da se dodade za sekoe identifikuvano sredstvo, negovata klasifikacija i vrednuvaweto spored sekoj od kriteriumite (doverlivost, integritet, raspolo`ivost).

2.1.3. Analiza na verojatnosta na pojava na ZAKANITE i SLABOSTITE

2.1.3.1. Identifikacija na ZAKANI i SLABOSTI kon sistemite

Zakana pretstavuva mo`en nesakan nastan koj mo`e da im nanese {teta na stabilnoto rabotewe na informativniot sistem, a so toa i na stabilnoto rabotewe i na samata banka.

Slabostite se povrzani so odredeni sredstva na informativniot sistem. Slabostite na sistemot sami po sebe ne predizvikuvaat {teta. **Zakanite po sigurnosta na informativniot sistem gi koristat slabostite na odredeni sredstva za da predizvikaat nestabilnost na sistemot na bankata.** Zakanite se identifikuvaat i se merat preku kreirawe i analiza na scenarija.

Potrebno e da se napravi identifikacija na slabostite na informativniot sistem na bankata koi mo`e da bidat od razli~na priroda:

- fizi~ka priroda-nedostatok od fizi~ko obezbeduvawe;
- administrativna priroda-nedostatok od adekvatno obu~eni vraboteni, nedostatok od proceduri vo nivnoto rabotewe;
- tehni~ka priroda-neadekvatnost na tehni~kata konfiguracija

odnosno, treba da se napravi:

- identifikacija na slabite interni sistemi na kontrola i organizaciskite slabosti (pr. slaba poddr{ka od rabotovodniot organ, neadekvaten trening na vrabotenite, neadekvatna stru~nost i ekipiranost, neadekvatni proceduri i politiki za rabota);
- identifikacija na tehni~kite slabosti (pr. slabosti vo postoe~kiot hardver i softver, slaba (osnovna) konfiguracija na serverite, mre`ata i {alterite);
- identifikacija na neadekvatna i nedovolna fizi~ka sigurnost na bankata;

- identifikacija na novite sigurnosni preporaki i barawa na zakonskata regulativa;
- identifikacija na zakanite sprema informativniot sistem, koi bi nastanale od lu|e so ne~esni nameri, vraboteni i ostanati koi slu~ajno i nenamerno mo`e da napravat {teta, kako i nadvore{ni vlijanija koi se nadvor od kontrola na bankata (pr. zemjotres, poplava, po`ar, nedostapnost na telekomunikacii ili elektri~na energija itn.);

So ovoj ~ekor na identifikacija se pravi lista na slabosti od razli~en tip po odredeno sredstvo na informativniot sistem i zakanata koja mo`e da se asocira so odredena slabost.

Zakana	Potencijalna slabost	Rizik
Virus	Nedostatok od antivirusna za{tita	Zarazuvawe so virus
Haker	Slaba (osnovna) konfigu-racija na serverot na bankata	Neavtoriziran pristap do doverliva informacija
Vraboteni	Nepravilna konfi-guracija na {alterite	Gre{ka vo sistemot
Ogan	Nedostatok od aparati za gasewe na po`ar	O{tetuvawe na zgradata i opremata
Vraboteni	Neadekvatni kontroli na pristap do aplikacija	Neavtoriziran pristap do doverliva informacija

(**Tabela 1** - Primeri za zakani po sredstvata na informativniot sistem na bankata)

2.1.3.2. Analiza na verojatnosta na pojava na zakanite i mo`nite posledici po bankata

Rabotovodniot organ treba da gi iskoristi podatocite obraboteni vo prethodnite ~ekori i da izvr{i analiza na sredstvata i rizicite koi se asocirani so niv. Analizata treba da gi identifikuva razli~nite nastani i zakani koi mo`e negativno da vlijaat od ostvaruvawe na strate{kite i operativnite celi na bankata.

Analizata na verojatnost mo`na zakana da nanese eventualna {teta na bankata preku upotreba na odredena slabost treba da se rangira na soodvetna skala:

- mnogu verojatno-zakanata mo{ne verojatno mo`e da se ostvari;
- verojatno-zakanata mo`e da se pojavi, me|utoa postojat nekoi za{titni mehanizmi;
- neverojatno-zakanata mnogu te{ko mo`e da se pojavi, bidej}i postojat adekvatni za{titni mehanizmi.

Analizata na pojavata na odredeni zakani treba da gi zeme predvid:

- namerno predizvikani zakani;
- nenamerno (slu~ajno) predizvikani zakani.

Nenamerni zakani opfa}aat incidenti od neadekvatni interni sistemi na kontrola i neadekvatni proceduri vo raboteweto, neadekvatni kontroli na pristap i nedostatok na fizi~ka sigurnost ili od prirodni katastrofi.

Namernite zakani obi~no se izvedeni od visoko motiviran napa|a~ (platen od konkurencija, porane{en vraboten itn) koj mo`e da gi iskoristi slabostite na informativniot sistem na bankata.

Analizata na verojatnost i mo`nite {teti koi mo`e da gi ima bankata treba da se analiziraat so koristewe na scenarija. Scenarijata treba da podrazbiraat napadi kon fizi~kata sigurnost, tehni~kata sigurnost, kako i opfa}awe na scenarija kade {to vrabotenite ne se pridr`uvaat kon sopstvenite administrativni proceduri za rabota. Naj~esto napa|a~ite od t.n. tip **"socijalen in`inering"** podrazbiraat napadi kon bankata koi sakaat da dobijat informaciii za koi nemaat potrebna avtorizacija, so manipulacija na doverbata na vrabotenite vo bankata. Vo toj slu~aj treba redovno da se testira adekvatnosta i efikasnosta na pridr`uvaweto kon sigurnosnite proceduri na vrabotenite vo bankata, a osobeno na onie koi rabotat so ~ustvitelna dokumentacija. ^estopati za napa|a~ot e polesno da dobie ~ustvitelna dokumentacija ili pristapni {ifri i lozinki na ovoj na~in, namesto preku nadvore{en napad na informativniot sistem (pr. preku internet).

2.1.3.3. Metodi za merewe na rizikot

Na~elno postojat dva op{to prifateni metoda na merewe na rizikot i toa:

- KVANTITATIVNA metoda i
- KVALITATIVNA metoda.

Idejata za vospostavuvawe na ovie metodi za merewe na rizikot e so cel da se oformi lista na mo`ni zakani i realni finasiski {teti po bankata. Od dobienata lista rabotovodniot organ treba da podgotvi strategija za namaluvawe na visokite rizici so gradewe na prioritetni listi na aktivnosti za implementacija na adekvatni kontroli i prifa}awe na site drugi rizici.

2.1.3.3.1. Kvantitativna analiza na rizikot

Ovoj metod dodeluva vrednosti koi se od domenot na verojatnosta, taka {to sekoga{ treba da se ima vo predvid da se dodelat {to porealni brojki na soodvetnite koeficienti. Za ovoj pristap treba da se definiraat osnovnite koeficienti kako: vrednosta na sredstvoto, frekvencija na pojava na zakanata, efikasnosta na kontrolite, verojatnosta na pojava na zakanata i itn. Za ovoj pristap treba dobro poznavawe na site ovie pokazateli za da mo`at da se vnesat vo ravenka i da se napravi uspe{no merewe na rizikot. Vo ovoj pristap treba da se definiraat:

- **ZEN**-(**Z**aguba od **e**dine~na pojava na **n**astanot)-pretstavuva zaguba izrazena vo denari koja bankata }e ja pretrpi od pojava na nastanot.
- **VS**-(**V**rednosta na **s**redstvoto);

- **FI**-(**F**aktor na **i**zlo`enost)-pretstavuva procent na zaguba {to }e ja predizvika zakanata po vrednosta na sredtvoto;

So definiraweto na ovie koeficienti se dobiva slednata ravenka:

ZEN = VS h FI

Primer: Dokolku nekoj server na bankata vredi 1.000.000 denari (**VS=1.000.000**) i se pojavi po`ar na mestoto kade {to e smesten. Se procenuva deka o{tetuvaweto od po`arot na serverot e 25% (**FI=25%).** Ovoj koeficient varira dokolku bankata ima (nema) implementirano adekvatni fizi~ki kontroli. (na pr.: protivpo`arni sredstva). Vo toj slu~aj, zagubata od edine~na pojava na nastanot bi bila:

ZEN = VS h FI = 250.000 denari.

Vo prodol`enie, gi definirame slednite koeficienti:

- **GFP**-(**G**odi{na **f**rekvencija na **p**ojava na nastanot) pretstavuva frekvencija na pojava na nastanot vo ramka od edna godina. Rangot se protega od 0.00 (nikoga{) do 1.00 (sekoga{)
- **GZN**-(**G**odi{na **z**aguba od **n**astanot) pretstavuva godi{nata zaguba od pojava na nastanot soglasno predvidenite koeficienti na pojava na nastanot(**GFP**)

Od gorenavedenoto se zaklu~uva deka:

GZN = ZEN h GFP

Vo prodol`enie na primerot treba da se definira koeficientot GFP, odnosno dokolku vo regionot mo`e da se slu~i po`ar edna{ vo deset godini (statisti~ki), toga{ **GFP**=0.1 i mo`e da se presmeta deka:

GZN = ZEN h GFP = 250.000h0.1 = 25.000 denari.

Ovaa vrednost (**GZN**) ni ja definira maksimalnata godi{na vrednost koja bi mo`el da ja potro{i rabotovodniot organ za za{tita na sredstvoto (serverot) od odredenata zakana (po`ar). Dokolku rabotovodniot organ na godi{no nivo tro{i pove}e od ovaa maksimalna godi{na vrednost, toga{ nema ekonomska opravdanost za investiciite za implementacija na tie kontroli, bidej}i realno predizvikanata {teta }e bide pomala od potro{enite sredstva za kontrola na nastanuvawe na tie {teti.

Sigurnosnite kontroli za namaluvawe i kontrola na rizicite pred da se implementiraat treba da se sogleda dali istite imaat ekonomska opravdanost. Bankata NE TREBA da investira vo kontrolni mehanizmi za za{tita koi }e se poskapi od vkupnata vrednost na sredstvoto za bankata.

Vo ovoj tip na analiza na rizik treba da se dodelat {to porealni koeficienti i vrednosti za da se dobie porealna i kvantitativna pretstava za zagubite od pojava na razli~nite zakani pred menaxmentot.

2.1.3.3.2. Kvalitativna analiza na rizikot

Ovoj metod na analiza na rizikot se sostoi od razrabotka i analiza na razli~ni vidovi scenarija i mo`ni rizici po stabilnosta i sigurnoto rabotewe na bankata. Ovoj metod se zasnova na timska rabota na iskusni lu|e koi imaat poznavawe na raboteweto na celata banka i imaat golemo poznavawe na rizicite koi mo`e da se pojavat. Mo`nite scenarija se razrabotuvaat od strana na OSIS pred timot i se predlagaat ili se nudat re{enija koi mo`at da pridonesat za preventivno izbegnuvawe na zakanata. Ovoj metod ja rangira **serioznosta na zakanata** i vr{i **rangirawe na mo`ni re{enija za namaluvawe na rizikot (rangirawe na efikasnosta na odredeni mo`ni sigurnosni kontroli)**. Sekoj ~len od timot ja rangira serioznosta na zakanata i potencijalnata zaguba na bankata. **Bankata treba da izgradi interna skala za rangirawe koja mo`e da bide opisna (niska, sredna, visoka) ili numeri~ka (1,2,3,4,5).** Koga timot }e zavr{i so rangiraweto na serioznosta na zakanata i rizikot i soodvetnoto rangiraweto na efikasnosta na poedine~nite kontroli, treba da podgotvi izve{taj do rabotovodniot organ, so cel donesuvawe dobra odluka vo odnos na obezbeduvaweto na poefikasna kontrola za obezbeduvawe na posiguren informativen sistem.

Primer: Zemame scenario deka bankata bila napadnata od nadvore{na treta strana i deka pri napadot od nadvor bile **ukradeni nekolku kreditni dosieja na kreditnite referenti.** Timot koj u~estvuva vo ovie scenarija treba da e iskusen i da gi znae postavenite kontroli i proceduri koi va`at na nivo na cela banka. Pritoa, tie go vrednuvaat so ocenki od 1 do 5 (1-najmala, 5-najvisoka) kakva e goleminata na zakanata i verojatnosta taa da se slu~i. Kakvi bi bile posledicite po bankata i kakvi se mo`nite implikacii vrz idnoto rabotewe na bankata? Na krajot se rangiraat i efikasnosta na odredeni kontroli koi treba da se ponudat kako soodvetni re{enija za namaluvawe na nivoto na rizik od zakanata.

Sumarnite rezultati treba da im se prezentiraat na rabotovodniot organ koj treba vrz baza na ovoj izve{taj da zaklu~i deka ovaa zakana e od dosta visok intenzitet za bankata i deka najsoodvetno re{enie za namaluvawe na ovoj rizik e instalacija i konfigurirawe na ognen yid (Tabela 2).

Zakana: Haker dobiva pristap do doverlivi informacii na bankata(kreditni dosieja)	Golemina na zakanata	Verojatnost da se slu~i	Zagubata po bankata	**Kontrola1**: Efikasnost na ognen yid (**Firewall**)	**Kontrola2**: Efikasnost na sistem za detekcija na napad (**IDS**)
IT direktor	4	2	4	4	3
Administrator	4	4	4	3	2
Programer	2	3	3	4	3
Direktor na Direkcija (krediti)	5	4	3	4	3
Referent (krediten)	4	4	4	4	3
REZULTATI	**3.8**	**3.4**	**3.6**	**3.8**	**2.8**

Tabela2. Primer na kvalitativna analiza na rizikot

Rizikot od sekoe scenario e funkcija od verojatnosta nastanot da se slu~i i eventualnata {teta {to }e ja pretrpi bankata.

Kako rezultat na ovoj ~ekor treba da se napravi analiza na verojatnosta deka odredena zakana mo`e da iskoristi dadena slabost na odredeno sredstvo na informativniot sistem i koi bile {tetite (kvantitativni ili kvalitativni) na bankata od naru{uvawe na doverlivosta na informacijata, naru{uvawe na integritetot ili nedostapnost na delovi od informativniot sistem na bankata.

2.1.4. Dodeluvawe na prioritet

Ovoj ~ekor go rangira rizikot (verojatnosta i {tetata) od razli~nite scenarija so cel da se prezentira rizikot i rezultatite od niv vo analiti~ka forma. Dobienata analiza na rizicite treba da poslu`i za podgotovka na lista na prioriteti vo re{avawe od strana na rabotovodniot organ. Za rizicite koi mo`at da predizvikaat golema {teta po bankata }e bide potrebna promptna reakcija od strana na rabotovodniot organ ili odreduvawe na vremenska ramka vo koja tie }e se namalat. Rabotovodniot organ mo`e da re{i da gi prifati rizici od pomal stepen i da ne voveduva kontroli za namaluvawe na istite. Vo ovoj ~ekor se vr{i selekcija na nivoto koe ja podrazbira granicata pome|u **kontrola na rizicite** i **prifa}awe na rizicite od strana na** rabotovodniot organ.

Rizicite koi baraat akcija treba da se razrabotat vo politikata za informativna sigurnost.

2.2. Politika za sigurnost na informativniot sistem

Politikata za sigurnost na informativniot sistem pretstavuva **TEMEL** na gradeweto na procesot na informativna sigurnost. Voedno, politikata treba da obezbedi dovolen prostor za razrabotka na dopolnitelni temi od aspekt na sigurnosta. Procedurite, standardite i upatstvata {to }e proizlezat vrz osnova na politikata }e pridonesat za podetalno, postepeno razrabotuvawe na site aspekti za obezbeduvawe na posiguren i neprekinat informativen sistem.

Politikata za sigurnost na informativniot sistem treba da bide postavena po principot od najgore pa do najdolu vo bankata (**"top-down"** pristap). Zatoa, **PO^ETNO MESTO** za zapo~nuvawe na procesot na informativna sigurnost e rabotovodniot organ na bankata. Rabotovodniot organ treba da elaborira kako }e bide postaven procesot na informativna sigurnost vo bankata, koi se negovite celi (strate{ki) i da objasni kako }e bide sprovedena na razli~ni nivoa vo bankata. Politikata treba da ja definira metodologijata {to }e se primenuva za procenka na rizikot i koli~estvoto na rizik {to }e go prifati rabotovodniot organ, a voedno i na~inot na upravuvaweto so visokiot rizik. Vo politikata treba da stoi i koi se soodvetnite politiki koi proizleguvaat od ovaa politika za sigurnost na informativnite sistemi.

2.2.1. Standardi, upatstva i proceduri

Politikata za sigurnost na informativna sigurnost treba da se gradi so izrabotka na dopolnitelni sigurnosni politiki i prifa}awe na standardi, kako i izrabotka na upatstva i proceduri za nivno doobjasnuvawe i razrabotka.

Standardite gi definiraat aktivnostite, pretstaveni kako pravila i ograni~uvawa, so koi }e se obezbedi postignuvawe na definiranite celi so politikata za informativna sigurnost. Primer: Dokolku sakame da postigneme celata doverliva dokumentacija da bide {ifrirana, toga{ bankata mora da go specificira standardot {to }e go koristi za {ifrirawe za da se postigne posiguren informativen sistem.

Bankata mora da navede koi standardi }e gi sledi i po~ituva.

Upatstvata sodr`at podetalni nasoki za aktivnostite koi treba da se prezemat i primenuvaat i davaat operativni nasoki za korisnicite na sistemot. Site preporaki od strana na menaxmentot treba da se navedat vo upatstvata.

Procedurite pretstavuvaat detalni ~ekori {to treba da se prezemat za da se postignat odredeni celi od politikata. Procedurite mo`e da bidat upateni kon krajnite korisnici, vrabotenite koi treba da napravat odredeni aktivnosti za podobruvawe na sigurnosta na nivo na celata banka. **Procedurite, prakti~no, ka`uvaat kako }e se implementiraat politikite, standardite i upatstvata vo bankata.** Primer: dokolku se deklarira deka praveweto "bekap" e standard vo bankata, procedurite treba detalno da go razrabotat praveweto "bekap", vo koj vremenski ramki, kade }e se ~uva...

slika2 (Prika`ana e piramidata na gradewe na politikata za IS so razvoj na standardi, upatstva i proceduri za informativna sigurnost)

Klu~ni faktori koi {to vlijaat na uspehot na politikata za informativna sigurnost se:

- **dobivawe poddr{ka i aktivno u~estvo na rabotovodniot organ;**
- sproveduvawe kompletna analiza na rizicite po informativniot sistem na bankata;
- uspe{na klasifikacija na informativniot sistem;
- implementacija na sigurnosni kontroli so cel kontrola i upravuvawe so rizikot;
- vospostavuvawe na set od precizno definirani moralni i eti~ki vrednosti na odnesuvawe na vrabotenite vo pogled na sigurnosta na informativniot sistem;
- dobivawe izjava (potvrda) od site vraboteni deka ja pro~itale i ja razbrale politikata za informativna sigurnost, osobeno delot za prifatlivo koristewe na informativnite sistemi na bankata;
- obezbeduvawe soodvetna obuka i edukacija na site vraboteni za sigurnost na informativniot sistem;
- sproveduvawe na godi{no revidirawe na politikata, a promenite da bidat utvrdeni od strana na Upravniot odbor.

Osnovni elementi na politikata za sigurnost na informativniot sistem koi treba da se razrabotat so dopolnitelni politiki, standardi, upatstva i proceduri se:

- **Klasifikacija na informacijata** vo smisla na ovoj Cirkular podrazbira rangirawe na informaciite vo bankata i toa spored stepenot na nivnata ~ustvitelnost. **(primer: javno, doverlivo, strogo dovererlivo...)**
- **Obuka na vraboteni** vo odnos na **pravilno (prifatlivo) koristewe na informativniot sistem na bankata** (pravilna rabota so bankarskite programi, pravilno koristewe na internet i elektronska po{ta za delovni potrebi). Bankata treba da gi definira koi aktivnosti ne treba da se izveduvaat so informativniot sistem na bankata (na pr.: zabrana za instalacija na hardver i softver so koj mo`e da se naru{i sigurnosta na celokupniot sistem, modemi, bez`i~na komunikacija, virusi). **Ovaa politika treba da bide distribuirana do site vraboteni i site koi imaat pristap i delovna potreba od informativniot sistem (vraboteni, obezbeduva~i na IT servisi...), koi{to treba da imaat potpi{ana izjava deka ja pro~itale i ja razbrale;**
- Definirawe na **ulogata na vnatre{nata i nadvore{nata revizija** od aspekt na obezbeduvawe na sigurnosta na informativniot sistem; **Da se definira ulogata na Slu`bata na vnatre{na revizija od aspekt na testirawe i ocenka na efikasnosta na implementiranite kontrolni sistemi vo odnos na sigurnosta na informativniot sistem. Voedno, Slu`bata za vnatre{na revizija treba aktivno da zeme u~estvo vo definiraweto na potrebnite revizorski i kontrolni tragi koi }e bidat ~uvani vo odreden vremenski rok;**
- Definirawe na **odnosot so obezbeduva~ite na IT servisi na bankata. Da se definira na~inot na pristap na obezbeduva~ot na IT servisi do bankata i da se definiraat pravnite normativi vo dogovorite so obezbeduva~ite i edinstvenite pravila na izbor na obezbeduva~i na IT servisi;**
- Definirawe na kontrola na pristap do odredeni resursi na bankata (na~inot na kontrola i identifikacija na korisnik);
- Sledewe na konfiguracii (sigurnosni nadgradbi, nadgradbi na novi verzii, promeni vo parametri i kodovi na aplikacii, podgotovka i migrirawe na aplikacijata vo produkcija); **Da se definira na~inot na nadgradba na sistemot i toa na operativnite sistemi, aplikaciite na bankata i vr{ewe konverzii na podatoci. Preporaka e rabotovodniot organ da gi organizira ovie zada~i vo postauvavawe na proektni timovi so to~no definirani celi i rokovi za zavr{uvawe na istite;**
- **Postavuvawe na Plan za kontinuitet vo raboteweto** (vo ponatamo{niot tekst **PKR**) na site delovni funkcii na bankata;
- Vospostavuvawe na antivirusna za{tita;
- Definirawe na telekomunikacii (modemi, ogneni yidovi, sistemi za nabquduvawe, alarmirawe i evidentirawe na neavtoriziran pristap do informativniot sistem, enkripcija); **Tehnikite i sistemite za interni kontroli koi }e bidat upotrebeni so cel da se obezbedi funkcionalnosta na odreden servis (na pr.: internet, elektronska po{ta, elektronsko bankarstvo). Celta na tehnikite i sistemite na interni kontroli e da se spre~i ili da se otkrie eventualen napad odvnatre ili odnadvor i da se vospostavat procesi na reakcija pri eventualen napad na informativniot sistem na bankata.**

- Ograni~uvawe na fizi~kiot pristap (zabrana za neavtoriziran fizi~ki pristap do odredeni oblasti vo bankata); Primer: **Podelba na bankata na sigurnosni zoni. Sekoja sigurnosna zona mo`e da se ima svoi specifi~ni kontroli za fizi~ki pristap.**
- Vospostavuvawe na dopolnitelni bezbednosni mehanizmi (protivpo`arna za{tita, za{tita od poplava, nabquduvawe, senzori, alarmi);
- **Za{tita na inventarot od kra`ba ili neovlasteno iznesuvawe na mediumi, hardver ili softver nadvor od bankata i sli~no;** Pokraj fizi~koto obezbeduvawe, za postignuvawe na ovie celi treba da se vovedat i sistemi na interni kontroli, vo smisla na vospostavuvawe efikasni sistemi na evidentirawe, ~uvawe i prenos i na otpi{uvawe na delovi od informativniot sistem.
- Definirawe na soodvetni aktivnosti koi{to}e se prezemat vo slu~aj koga bankata se somneva ili utvrdila incident vo pogled na sigurnosta na informativnata sigurnost, za{to treba da se izvestuvaat Narodna banka na Republika Makedonija i Ministerstvoto za Vnatre{ni raboti. Bankite treba da go dostavat izvestuvaweto (vo prilog na ovoj Cirkular Aneks 2), do Narodna banka na Republika Makedonija vo rok od pet dena po utvrdeniot sigurnosen incident.

Ovie predlo`eni elementi mo`at da se smetaat za **po~etna pozicija za razvoj na politikata za informativna sigurnost**. **Mo`e da bide potrebno razvoj i na dopolnitelni elementi koi ne se vklu~eni vo sodr`inata na ovoj Cirkular, a se bitni za sigurnosta na informativniot sistem za bankata.**

2.3. Implementacija na sigurnosni kontroli

Sigurnosta na informativniot sistem mo`e da se obezbedi preku pove}e nivoa na kontroli: fizi~ki, tehni~ki i administrativni.** Ovie tri kategorii mo`e dopolnitelno da bidat podeleni na **kontroli za spre~uvawe i onie za otkrivawe.

Kontrolite za spre~uvawe imaat za zada~a da **spre~at** pojava na nesakani nastani, dodeka **kontrolite za otkrivawe** nastojuvaat da go otkrijat nastanot po negovoto slu~uvawe.

Treba da se prezemat soodvetni fizi~ki, tehni~ki i administrativni kontroli za da se obezbedi sakanoto nivo na sigurnost na informativniot sistem, kako i balans pome|u kontrolite za spre~uvawe i otkrivawe za ostvaruvawe na celite na politikata na informativna sigurnost.

Kombinaciite od fizi~kite, tehni~kite i administrativnite kontroli koi najdobro odgovaraat na specifi~na okolina, mo`e da bide identifikuvano samo so sproveduvawe na kompletna analiza na rizicite.

Ne postoi univerzalna {ema koja mo`e da se preslika od drugi banki.

2.3.1. Fizi~ki kontroli

Fizi~kite kontroli slu`at za obezbeduvawe na adekvatna fizi~kata sigurnost vo bankata. Kako primeri na fizi~ki kontroli se upotrebata na bravi, ~uvarskata slu`ba, bexevi, alarmi i sli~ni merki za kontrola na pristapot do informativnite sistemi na bankata. Ovie merki imaat za cel da spre~at mo`ni zakani od tipot na {piona`a, otu|uvawe i uni{tuvawe ili o{tetuvawe od nesre}en slu~aj ili prirodna katastrofa (poplava, zemjotres...).

2.3.1.1 Fizi~ki kontroli za spre~uvawe

Fizi~ki kontroli za spre~uvawe se upotrebuvaat za da se spre~i neavtoriziran pristap do informativnite sistemi i za za{tita od prirodni katastrofi. Ovie kontroli mo`at da bidat:

- **Za{tita na podatocite**-dokolku se slu~i namerno ili nenamerno uni{tuvawe na podatocite ili dokumentacijata, treba **za{titenite podatoci da bidat dostapni i to~ni.** Za{titenite podatoci treba da bidat ~uvani na sigurna lokacija konstruirana od nezapalivi materijali. **Za{titenite podatoci treba da se nao|aat na adekvatna dale~ina za da se izbegne rizikot od uni{tuvawe na originalnite i za{titenite podatoci i sistemi od istiot sigurnosen incident.** Za{titenite podatoci koi se od ~uvstvitelna priroda treba da imaat isto nivo na za{tita kako i originalnite podatoci;
- **Ograda**-Ogradata mo`e da bide dopolnitelno nadgleduvana so kameri ili osigurana so alarmni uredi;
- **^uvarska slu`ba**- e stacionirana na vlezot vo zgradata i imaat zada~a da dozvolat pristap na avtorizirani lica vo prostoriite na bankata. ^uvarite se dosta efektivni dokolku imaat proceduri za toa koi sredstva mo`e, a koi ne mo`e da se iznesat nadvor od bankata bez prethodna avtorizacija. Efikasnosta na ~uvarskata slu`ba mo`e da bide dosta pogolema, dokolku e poddr`ana so alarmni pomagala i predupreduva~ki indikatori koi mo`e da gi sledat;
- **Bexevi**-Fizi~kata bezbednost mo`e da bide kontrolirana ednostavno so izdavawe soodvetni bexevi koi va`at za soodvetna sigurnosna zona na fizi~ki pristap;
- **Bravi i klu~evi**-naj~esto koristeni za kontrola na pristapot vo restriktivnite oblasti. Bidej}i e te{ko da se kontrolira kopiraweto na klu~evite, pove}eto banki gi izbegnuvaat obi~nite bravi i klu~evi. Se prepora~uva koristeweto kodirani bravi (na pr.: soodvetna kombinacija na brojki koja se pritiska vo odreden redosled, so {to se otvora vratata);
- **Generatori na elektri~na energija**-se dobiva visok stepen na raspolo`ivost na informativnite sistemi, duri i pri prekini vo elektri~noto napojuvawe. Obi~no ova se postignuva so kombinacija na **generatori (bazirani) na baterija** t.n. (**UPS**) i **generatori na elektri~na energija (bazirani) na benzin, dizel, kerozin ili nekoj priroden gas**. Rabotovodniot organ treba da se osiguri deka generatorite bazirani na baterija se pravilno konfigurirani niz

celata banka, kako i rabotata na centralniot generator na elektri~na energija. Nivnata rabota treba da e sinhronizirana, odnosno pri nedostatok na elektri~na energija prvo treba da se vklu~at elektri~nite generatori (bazirani) na baterija (vreme vo milisekundi), a za toa vreme treba da se podigne i proraboti centralniot generator na elektri~na energija. Sistemite **UPS** treba da obezbedat dovolno energija za adekvaten vremenski period i neprekinatost na rabotata na informativnata oprema dodeka ne dojde do pravilno vra}awe na elektri~na energija ili do prezemawe na celokupnata rabota od strana na generatorot na struja. **Generatorot na elektri~na energija treba da bide vo mo`nost da obezbedi neprekinato rabotewe na bankata od dva do tri rabotni dena. Bankata treba da vr{i periodi~no testirawe na generatorot na elektri~na energija so cel verificirawe na negovata funkcionalnost**;

- **Izbor na lokacija** (Primarna ili alternativna)-treba da se izvr{i vnimatelno za da se izbegnat o~iglednite predvidlivi rizici vo oblasta kade {to se nao|a. (na pr.: Da se izbegnat rizicite od poplava, zemjotresi ili po`ari vo oblasta. Da se izbegnat lokaciite vo blizina na aerodromi ili `eleznica so cel da se izbegnat vibraciite koi mo`e da predizvikaat {teta na elektronskata oprema);
- **Protivpo`arni sredstva**-pretstavuvaat sredstva ~ija namena e spre~uvawe i lokalizirawe eventualen po`ar koj mo`e da nastane vo bankata. Celta e da se spre~i katastrofa, zaguba na ~ove~ki `ivoti i zaguba na infrastrukturata na bankata. Informativniot sistem e va`en del od infrastrukturata na bankata i zatoa treba da bide soodvetno za{titen od mo`en po`ar. Informativnite sistemi treba da se lociraat podaleku od potencijalni predizvikuva~i na po`ar (kujni, bife...). Mebelot vo kompjuterskata sala treba da bide od nezapaliv materijal. Aparatite za gasewe na po`arot treba da bidat soodvetno rasporedeni vo bankata so za da bidat pri raka vo slu~aj na po`ar. Vrabotenite treba da bidat obu~eni i trenirani za da se znae rakuvaweto so ovie sredstva i da se zapoznaat so procedurite koi treba da se sledat vo slu~aj na po`ar. Obi~no, vo plafonot na kompjuterskiot centar se vgraduvaat avtomatski gasna~i na po`ar. Rizikot od gasneweto so voda vo kompjuterskiot centar e daleku pogolem otkolku samiot po`ar. Dokolku se gasi so voda ili pena, toga{ vo salata treba da ima posebni vodootporni prekriva~i so koi }e se pokrie kriti~nata oprema pred da se vr{i lokalizacija na po`arot. Se prepora~uva upotreba na specijalni gasovi koi go izvlekuvaat kislorodot, a na toj na~in i go lokaliziraat po`arot, na mesta kade {to ne se prisutni vraboteni ili koi{to mo`e mnogu brgu da se evakuiraat.

2.3.1.2 Fizi~ki kontroli za otkrivawe

Fizi~kite kontroli za otkrivawe gi predupreduvaat odgovornite vo procesot na sigurnost na informativniot sistem deka fizi~kite merki na za{tita se naru{eni. Ovie kontroli mo`at da bidat:

- **Detektori na dvi`ewe**-se postavuvaat vo kompjuterski sali vo koi nema prisustvo na lu|e, ili mo`e da se vklu~uvaat na nivo na cela banka posle rabotnoto vreme na personalot. Detektorite na dvi`ewe mora da bidat konstantno nabquduvani od ~uvarskata slu`ba;
- **Detektori na ~ad i ogan**-treba da bidat rasoporedeni na tavanot i vo dupliot pod. So napredokot na tehnologijata se pojavuvaat sistemi t.n. **VESDA** koi pretstavuvaat rani detektori na po`ar. Ovie detektori se daleku posofisticirani i podobri od klasi~nite detektori na po`ar. Tie zemaat primerok na vozduh od prostorijata vo kontinuitet i lesno mo`e da otkrijat nagoren kabel ili `ica u{te vo rana faza i da go alarmiraat menaxmentot. Bankata treba da vr{i redovna kontrola i testirawe na site detektori na ~ad i ogan vo nivnata to~nost;
- **CCTV monitori**-celta e da se dobie audio i video nadzor nad oblasti koi treba da bidat pod neprekinato nabquduvawe (na pr: kompjuterskata sala celosno, glavniot server na bankata, vlezovi ili izlezi itn.);
- **Senzori i alarmi**-treba da vr{at neprekinat monitoring na rabotnata okolina na opremata i da se osigura deka se postignati rabotnite temperaturi na vozduh i vla`nost vo prostorijata spored onaa specificirana i prepora~ana od proizveduva~ot.

2.3.2. Tehni~ki kontroli

Tehni~kite kontroli se kontroli koi se vgradeni vo informativnata oprema, aplikativniot softver, komunikaciskata oprema i pridru`nite uredi od strana na proizveduva~ot na opremata. **Tehni~kite kontroli u{te se nare~eni i logi~ki kontroli**.

2.3.2.1. Tehni~ki kontroli za spre~uvawe

Tehni~kite kontroli za spre~uvawe se koristat za da se spre~at lica, programi ili procesi da dobijat pristap do informativni resursi za koi nemaat adekvatna avtorizacija:

- **kontrolni listi za pristap**-Bankata treba da vospostavi kontrola na pristapot do odredeni informativni resursi. Vo pove}eto sistemi, pristapot do podatocite i programite e so implementirani **kontrolni listi za pristap** (**access lists**) do resursite na informativniot sistem. Tie listi ovozmo`uvaat pristap do odredeni resursi samo na avtorizirani i registrirani korisnici;
- **antivirus**-Bankata mora da poseduva antivirus re{enie na nivo na cela banka. Treba da se istakne va`nosta na ova re{enie, bidej}i zazema epidemiolo{ki proporcii vo informati~kiot svet. Rizicite koi se povrzani so virusite se mo{ne visoki, bidej}i mo`no e da predizvikaat prekini vo raboteweto na bankata i gubewe na podatoci. Ovoj softver obi~no se **"osve`uva"** na dnevna osnova so cel prezemawe na novite definicii na virusite koi sekojdnevno se pojavuvaat;

- **korisni~ko ime i lozinka (user/password)-Korisni~kite imiwa na informativniot sistem treba na edinstven na~in da gi identifikuvaat korisnicite na sitemot.** Treba da se izbegnuva otvorawe korisni~ki imiwa na sistemot na bankata so koi ne mo`e da se izvr{i edinstvena identifikacija na korisnicite. Ne se prepora~uvaat otvorawe na korisni~ki imwa od tipot na: banka, imiwa na organizacioni edinici, imiwa na obezbeduva~i, i drugi op{ti imiwa so koi ne mo`e so preciznost da se identifikuva koj bil korisnikot {to rabotel na sistemot i dali go poseduval potrebnoto nivo na avtorizacija.

  Za izbor na lozinkite nema nekoe magi~no pravilo i zavisi od sredinata i nivoto na sigurnost koe saka da se postigne.

  Ova se samo nekoi razmisluvawa vo vrska so lozinkite:
  - Tro{oci na zamena na lozinkite;
  - Rizik od probivawe na lozinkite (vidi tabela 1);
  - Na~in na distribucija do krajnite korisnici;
  - Mo`nosta za pogoduvawe na lozinkata;
  - Broj na dozvoleni pogre{ni obidi.

  Preporaki za upravuvawe so lozinkite:
  - va`nost : 120 dena na obi~ni korisnici;
  - va`nost : 60 dena privilegirani korisnici;
  - va`nost : 30 dena sigurnosni lica;
  - Korisnikot samiot da mo`e da ja menuva lozinkata pred da iste~e;
  - Vodewe na revizorski tragi na promenite na lozinkite.

Tip na lozinka	dol`ina	mo`ni kombinacii	potrebno vreme za probivawe
bukvi (mali ili golemi)	6 karakteri	308,915,776	pomalku od minuta
bukvi (mali i golemi)	6 karakteri	19,770,609,664	1 den
bukvi (mali i golemi) i brojki	6 karakteri	56,800,235,584	3 dena
bukvi (mali i golemi), brojki i spec. znaci	6 karakteri	606,355,001,344	5 nedeli
bukvi (mali i golemi), brojki i spec. znaci	9 karakteri	472,161,363,286,556,672	77 iljadi godini

tabela 1. Vidovi lozinki i potrebno vreme za probivawe so dosega{nata mo} na informativnata tehnologija

- **smart-karti~ki**-plasti~ni karti~ki so vgraden kompjuterski ~ip (memorija/procesor). ^ipot mo`e da bide ili mikroprocesor so vnatre{na memorija ili samo memorija. Vo memorijata na smart karti~kata mo`e da se nao|aat {ifrirani podatoci koi mo`e da poslu`at za proverka (avtentikacija) na korisnikot. **Vo kombinacija so PIN broj verifikacija nudat sigurna proverka (avtentikacija) na dve nivoa.** Nivnata upotreba se prepora~uva za pristap do dokumentacija koja za bankata e od naj~ustvitelna priroda. Voedno upotrebata na smart karti~ki mo`e da poslu`i za potrebite na elektronsko upravuvawe so dokumentacija i elektronsko potpi{uvawe na dokumenti soglasno zakonskata regulativa za elektronski potpis i za celite na elektronskoto bankarstvo;
- **{ifrirawe (enkripcija)**-pretstavuva transformacija na ~istiot tekst vo t.n. nerazbirliv ({ifriran) tekst upotrebuvaj}i kriptografski tehniki. Se prepora~uva upotreba na {ifrirawe pri prenos na ~ustvitelni informacii. Postojat dva na~ina na {ifrirawe, i toa hardverski i softverski;
- **Kontroli za dale~inski pristap**-pretstavuvaat sistem na interni tehni~ki kontroli koi se sproveduvaat za namaluvawe na rizikot od neavtoriziran pristap na nadvore{ni lica vo informativniot sistem na bankata. Dokolku postoi dale~inski pristap do sistemot na bankata, toj treba da bide pod neprekinato nabquduvawe i sledewe na kontrolnite tragi. Bankata mora da gi prezeme site neophodni kontroli za da se zgolemi sigurnosta na tipot na re{enieto (callback, VPN, {ifrirawe, Access serveri, itn).

2.3.2.2. Tehni~kite kontroli za otkrivawe

Ovie kontroli se koristat za da se otkrijat naru{enite tehni~ki kontroli za spre~uvawe koi bile instalirani vo sistemot i da izvr{at alarmirawe na sistemite za za{tita i kontrola. Mo`e da bidat:

- **Revizorska traga (Audit trails)**-pretstavuvaat snimki od sistemskite aktivnosti so koi mo`e da se izvr{i rekonstrukcija i revizija na sekvencite vo slu~aj na transakcija, od po~etokot do nejzinoto izvr{uvawe. Na ovoj na~in se obezbeduva **zna~aen dokaz** i traga vo obidot za naru{uvawe na vospostavenata politika na informativen sistem. Ovie izve{tai treba da se sledat na redovna osnova, da bidat nadgleduvani od **O**dgovorniot za **s**igurnost na **i**nformativniot **s**istem (vo ponatamo{niot tekst **OSIS**) so cel da se izvr{i analiza na neavtoriziran pristap;
- **Sistemi za spre~uvawe i otkrivawe napad (Intrusion Prevention & Detection System)**-**Bankata treba da poseduva sistemi za da se spre~i ili da se otkrie incidentot ili naru{uvawata na sigurnosnata politika vo tekot na nivno slu~uvawe, a ne posle nivnoto nastanuvawe**. Site neavtorizirani dejstvija se alarmiraat do OSIS koj prezema koordinirana reakcija. Ovie sistemi treba da se implementiraat osobeno vo delot koj pristapuva kon internet ili servisite na elektronskoto bankarstvo (nezavisno od tipot na

sistemot zatvoren/otvoren). Na toj na~in }e se sprovede eden efektiven, brz i siguren sistem na predupreduvawe vo slu~aj na poseriozni naru{uvawa na definiranata politika za sigurnost na informativniot sistem na bankata.

2.3.3. Administrativni kontroli

Administrativnite kontroli vklu~uvaat vospostavuvawe proceduri, upatstava, strategii i sigurnosni politiki so koi na vrabotenite koi imaat pristap do informativniot sistem, im se ovozmo`uva potrebnata avtorizacija za izvr{uvawe na svoite delovni procesi i imaat jasna slika za aktivnostite vo pogled na obezbeduvawe na posiguren informativen sistem.

2.3.3.1. Administrativni kontroli za spre~uvawe

Ovie kontroli vo najgolem del se orientirani kon kontrolirawe na odnesuvaweto na vrabotenite za da se obezbedi doverlivosta, integritetot i raspolo`ivosta na informativnite sistemi. Tie mo`at da bidat:

- **Registracija na korisnikot za rabota na sistemot**-So ova formalno se postignuva vrabotenite da imaat soodvetni prava i privilegii za rabota na sistemot so cel vr{ewe na svoite delovni aktivnosti. **Pred registracijata, korisnikot treba da e zapoznaen i soglasen za koi operacii smee, a koi operacii ne smee da gi izvr{uva na informativniot sistem. Bankata treba da poseduva izjavi na site vraboteni potpi{ani od nivna strana deka se zapoznati so na~inot na prifatlivo (adekvatno) koristewe na informativniot sistem na bankata.** Vo izjavite treba da se navede koi se nivnite odgovornosti od aspekt na obezbeduvawe pogolema sigurnost na sistemot i koi se merkite {to }e se prezemat, dokolku predizvikaat sigurnosen incident;
- **Proceduri za priem na nov vraboten i otpu{tawe**-Bankata treba da ima proceduri za priem na vraboteni. Treba da ima proceduri i za otpu{tawe na vraboteni, bez ogled na na~inot na koj mu prekinuva rabotniot odnos, za na~inot na zatvorawe i blokirawe na profilot na vraboteniot koj e otvoren na sistemo,t kako i primopredavawe na site klu~evi, bexevi, laptop-kompjuteri ili drugi sredstva koi gi poseduva toj. Korisni~kiot profil treba da bide izbri{an (onevozmo`en) ili prilagoden i dodelen na novata zamena na vraboteniot.
- **Dogovori za rabota**- Vo ovoj kontekst, bankata treba da obrati osobeno vnimanie na posledici na Zakonot za avtorskoto pravo i srodnite prava (“Slu`ben vesnik na RM“ br. 47/96, 3/98 i 98/02) vo koj se regulira poimot za avtorsko pravo, negovoto koristewe i prenesuvawe, za{titata na pravata, nadzorot na primenata na Zakonot i sankciite vo slu£aj na postapuvawe vo sprotivnost so negovite odredbi. Toa pred se va`i za banki koi poseduvaat izvorni

kodovi na svoite bankarski aplikacii i koi poseduvaat programerski timovi za razvoj na svoite aplikacii.

- **Treninzi za sigurnost**-Bankata treba da napravi treninzi za adekvatno koristewe na aplikativnite programi i pridru`nite aplikacii koi se potrebni za efikasno izvr{uvawe na delovnite procesi. Ovie treninzi se za da se podigne nivoto na svest vo bankata vo pogled na potrebata za sigurnosta na informativnite sistemi. Krajnite korisnici treba da gi razberat merkite i kontrolite koi se vospostavuvaat na nivo na cel sistem. Dokolku vrabotenite ne go razberat zna~eweto na vospostavenite kontroli, tie mo`e da ne gi primenuvaat ili, so drugi zborovi, }e go oslabnat celokupniot program za sigurnost. Generalno, site vraboteni treba da se zapoznati so na~inot na koj mo`e da izvr{at za{tita na odredeni ~ustvitelni podatoci, da imaat poznavawe za virusite i na~inot na nivnoto {irewe i kogo treba da alarmiraat vo slu~aj na pojava na odredeni gre{ki ili sigurnosni incidenti;
- **Segregacija na dol`nosti**-Procesot e razdvoen na osnovni delovi, kade razli~ni vraboteni se odgovorni za razli~ni delovi od procesot. Ova se pravi za da se namali rizikot eden ~ovek da ima kontrola vrz celokupniot tek na izvr{uvawe na bankarskata operacija. Vo toj slu~aj, toj bi mo`el da izvr{i manipulacija ili izmama za da se zdobie so li~na profit ili dobivka. **(primer: kreirawe i verifikacija na nalozi vo platen promet vo zemjata od `iro smetka na bankata vodi kon visok operativen rizik koj mo`e da dovede do pojava na likvidnosen rizik. Bankata mora da vospostavi proces na dvojna kontrola pri kreiraweto, potpi{uvaweto i pra}aweto na ovie nalozi vo sistemite na platen promet).**
- **Nadgleduvawe** od neposredniot rakovoditel-Se pravi za da se zabele`at nevoobi~eni promeni vo odnesuvaweto na vrabotenite, koi ponatamu mo`at da vodat do somnitelni transakcii. Pretpostavenite od taa strana mora da bidat zapoznati so procedurite, pravilata i so na~not na koj se izvr{uvaat tie od strana na vrabotenite i da obezbedi segregacija na dol`nosti dokolku e potrebno za izveduvawe na nekoja ~ustvitelna operacija.
- **Organizacija na bankata i kontinuitet na klu~nite lu|e**-Bankata mora da vospostavi organizaciona struktura koja }e obezbedi adekvatna dvojna kontrola i podelba na dol`nostite. **Visokata stapka na zaminuvawe na vraboteni od bankata mo`e da vlijae na samata banka i mo`e da vodi kon degradacija na servisite i namaluvawe na kvalitetot kako i zgolemuvawe na tro{ocite za trening na novite vraboteni.** Rabotovodniot organ treba da vlijae za namlauvawe na ovaa stapka.
- **Sigurnosni politiki, standardi, upatstva i proceduri**-soodvetni politiki, standardi upatstva i proceduri koi treba da bidat vospostaveni za da se implementira politikata za informativna sigurnost.
- **Plan za kontinuitet vo raboteweto (PKR)**-pretstavuva plan vo koj se sodr`ani proceduri za vrabotenite vo slu~aj na delumna ili kompletna zaguba ili te`ok prekin na informativnite sistemi. Primarnite celi na ovie planovi se da obezbedat razumni garancii

deka bankata mo`e da gi prodol`i svoite kriti~ni operacii vo naru{eni uslovi i da se vrati vo normalen tek vo razumno vreme.

2.3.3.2. Administrativni kontroli za otkrivawe

Ovie kontroli slu`at za procenka na kvalitetot i stepenot na implementacija na politikata na informativna sigurnost. Tie mo`at da bidat:

- **Testirawe (revizii) na sigurnosta i efikasnosta na implementiranite kontroli-** mo`e da obezbedat informacija koi politiki i proceduri se slabi i koi ne se sproveduvaat zadovolitelno. Vklu~enosta na rabotovodniot organ so korektivna akcija posle izvr{enite revizii i testirawa ja poka`uva negovata poddr{kata za voveduvawe efikasna politika za informativna sigurnost.
- **Rotacija na dol`nosti-**slu`i za namaluvawe na operativniot rizik i detekcija na izmama ili nepo~ituvawe na procedurite za sigurnost na informativniot sistem. **Rotacijata na dol`nosti pomaga i bankata da ne bide zavisna vo izveduvawe na svoite operacii samo od eden ~ovek.**

2.4. Testirawe na sigurnosta

Sigurnosta na informativnite sistemi e integriran proces koj gi namaluva rizicite povrzani so informativnata tehnologija na prifatlivo nivo. Celiot proces, vklu~uvaj}i go testiraweto, e voden od procenka na rizicite. Kolku e pogolem rizikot tolku e pogolema potrebata od proverka na efikasnosta na implementiranite kontroli.

Generalno postojat dva tipa sistemi, i toa so visok i nizok rizik. Sistemite so visok stepen na rizik treba da bidat pofrekventno proveruvani i testirani. Postoi {irok rang testovi so cel dobivawe slika za sigurnosta. Nekoi od niv se so cel da se verificiraat nekoi izolirani kontroli i procesi (pr.: lozinka i nejzinata silina). Nekoi od niv se odnesuvaat na tehni~ka konfiguracija (pr.: konfiguracija na serverot za elektronsko bankarstvo). Nekoi testovi imaat za cel da se predvidat odredeni slabosti na sistemot. Nekoi testovi mo`e da se napravat za da se simuliraat akciite na mo`nite napa|a~i. Vo rangot na ovie testovi **Upravniot odbor treba da odlu~i koi testovi mo`e da gi sprovede** i dali testovite gi imale zadovolitelnite rezultati.

Vo testiraweto na sigurnosta va`na uloga ima slu`bata za vnatre{na revizija i nadvore{nata revizija i toa vo ulogi na aktivni testeri na sigurnosta na informativniot sistem. Ulogata na testirawe na sigurnosta so soodvetnite ulogi i odgovornosti podetalno e razrabotena vo glava: **3.2. Ulogata na Odborot za revizija, slu`bata za vnatre{na revizija i nadvore{nata revizija.**

2.5. Nabquduvawe i nadgradba

Stati~nata politika na informativna sigurnost zastaruva so tek na vremeto.

Upravniot odbor i rabotovodniot organ na bankata treba da sozdadat uslovi za razvoj i prilagoduvawe na politikata za sigurnost na informativniot sistem vo soglasnost so promenite vo tehnologijata, promenite na ~ustvitelnosta na informacijata na korisnicite, vnatre{nite ili nadvore{nite rizici na koi e izlo`ena taa informacija, a osobeno pri promenite vo funkcioniraweto ili organiziraweto na samata banka(pr.: statusni promeni na bankata).

Bankite treba kontinuirano da sobiraat informacii i da vr{at analiza na rizicite zemaj}i gi vo predvid novite zakani i slabosti, aktuelnite napadi i novi virusi kon bankite i drugite ustanovi. Tie treba da gi koristat ovie informacii, a dokolku e potrebno, i da se nadgradi procesot na procenka na rizicite, politikata za informativna sigurnost i implementiranite kontroli.

Efektivnoto nabquduvawe na postaveniot proces na informativna sigurnost treba da zeme predvid izvori od netehni~ka i od tehni~ka priroda.

Netehni~ki izvori pretstavuvaat organizaciski promeni na bankata, pojava na novi proizvodi i servisi, zgolemena ~ustvitelnost na odredeni informacii, zaminuvawe na odredeni klu~ni lu|e od bankata itn.

Tehni~ki izvori pretstavuvaat pojava na novi tehni~ki sistemi, novi obezbeduva~i na IT servisi, novi aplikacii, novi sistemi na telekomunikacisko povrzuvawe i za{tita.

Vo ovoj proces treba da se vklu~at slednite aktivnosti:

- Vidliva poddr{ka i anga`iranost na rabotovodniot organ za implementacija na politikata za informativna sigurnost na nivo na celata banka. Direktorite na poedine~nite organizacioni edinici imaat odgovornost za odr`uvawe na sigurnosta na sistemite i informaciite vo ramkite na nivnata edinica;
- **OSIS treba kontinuirano da go razviva procesot na sigurnost na informativniot sistem, da vr{i identifikacijata na novite trendovi i zakani koi se asocirani so novata tehnologija, kako i da gi sledi otkrienite slabosti vo implementiranite kontroli**.
- OSIS treba da gi nadgleduva nadvore{nite izvori na netehni~ki i tehni~ki slabosti i da u~estvuva vo razvoj na soodvetni re{enija za nivna kontrola. (na pr.: osve`uvawe na bazata so definicii na virusi so tekovniot datum, osve`uvawe na definiciite na poznati napadi kaj sistemite za spre~uvawe i otkrivawe na napadi (Intrusion prevention&detection system), proces na nadgleduvawe na obezbeduva~ite na IT servisi);

- Upravniot odbor treba da bara izvr{uvawe testovi i revizii za da se napravi ocenka na usoglasenosta na bankata so politikata na informativna sigurnost

Spored informaciite {to gi poseduvaat, bankite treba da odlu~at kakvi unapreduvawa treba da im se izvr{at na razli~nite komponeneti vo procesot na informativna sigurnost, soglasno so izvr{enata procenka na rizik po bankata.

3. MESTO, ULOGI I ODGOVORNOSTI NA UPRAVNIOT ODBOR, RABOTOVODNIOT ORGAN I REVIZIJATA VO POGLED NA SIGURNOSTA I EFEKTIVNO UPRAVUVAWE SO INFORMATIVNATA TEHNOLOGIJA VO BANKATA

3.1. MESTO, ULOGA I ODGOVORNOST

Efektivnoto upravuvawe so informativnata tehnologija e od osobeno zna~ewe za upotrebata na novite servisi i tehnologii vo ostvaruvaweto na strategiskite celi na bankata. IT pretstavuva integralen i centralen del od procesot na izvr{uvawe na najgolemiot broj bankarski operacii. Upravuvaweto so IT ne pretstavuva samo upravuvawe so tro{ocite koi se napraveni pri izvr{uvaweto na bankarskite operacii i kontrola na nivnoto sproveduvawe, bidej}i napredokot vo tehnologijata mo`e da rezultira so ponuda na novi servisi i proizvodi, koi mo`at da zna~at zgolemuvawe na izlo`enosta na rizicite na bankata.

Sigurnosta na informativniot sistem e odgovornost za sekogo vo bankata.

Upravniot odbor, rabotovodniot organ i vrabotenite imaat razli~ni ulogi vo razvojot i implementacijata na efektiven sigurnosen proces.

3.1.1. Ulogata na Upravniot odbor i rabotovodniot organ za sigurnost na informativniot sistem

Upravniot odbor e odgovoren za upravuvawe, implementacija i unapreduvawe na politikata za sigurnost na informativniot sistem na bankata.

Upravniot odbor ja utvrduva politika za sigurnost na informativniot sistem i vr{i nejzino unapreduvawe najmalku edna{ godi{no.

Upravniot odbor treba da mu dade nasoki i preporaki na rabotovodniot organ za obezbeduvawe na siguren informativen sistem preku:

- barawe za vospostavuvawe centralen nadzor i koordinacija;
- definirawe na soodvetni ulogi i odgovornosti;
- merewe na rizikot;
- nabquduvawe i testirawe;
- izvestuvawe;
- identifikuvawe, sledewe i kontrola na rizicite.

Odnesuvaweto na menaxmentot sprema sigurnosta na informativniot sistem vlijae na odnesuvaweto na site vraboteni kon sigurnosta. Vo bankata da ima vospostaveno idealen sistem na kontroli, dobri politiki i proceduri, no ako nivne gi po~ituva rabotovodniot organ, toga{ te{ko deka }e mo`e toa da se o~ekuva i od vrabotenite. Zatoa, va`no e rabotovodniot organ, preku svoeto odnesuvawe, da dava signal do vrabotenite za va`nosta na informativnata sigurnost.

Rabotovodniot organ treba da nazna~i eden ili pove}e lica odgovorni za sigurnost na informativnite sistemi (OSIS). OSIS e odgovoren i vodi smetka za sigurnosta na informativnite sistemi. OSIS treba da ima dobro poznavawe na

informativniot sistem i rizicite koi se pridru`eni kon IT, kako i dobra organizaciska postavenost za da bide vo mo`nost da gi izvede site zada~i koi se o~ekuvaat od nego.

Rabotovodniot organ treba da ja primeni politikata na informativna sigurnost na nivo na cela banka so jasna diferencijacija na odgovornostite i soodvetni dol`nosti za sigurnosta na informativniot sistem na odredeni lica. Odgovornostite za sigurnost na informativniot sistem treba da bidat raspredeleni od IT organizacionata edinica do razli~nite sektori vo bankata, vo zavisnost od goleminata, kompleksnosta, vidot na operacii koi se izvr{uvaat vo bankata.

Rabotovodniot organ, isto taka, ima odgovornost da obezbedi integrirawe na kontrolite za sigurnost na informativniot sistem vo kompletniot sistem na bankata. Za da ja obezbedi integracijata, rabotovodniot organ treba da:

- obezbedi potkrepa na procesot na sigurnost so interni politiki i proceduri koi se primenuvaat;
- obezbedi usoglasenost so politikata za informativna sigurnost na kontinuiran i uramnote`en na~in niz celata banka;
- obezbedi testirawe na sprovedenite kontroli na sigurnosta na informativniot sistem.

Rabotovodniot organ treba da gi zeme predvid i ulogata i odgovornostite na nadvore{nite treti lica. Obezbeduva~ite na IT servisi na bankata, korisnicite i drugi lica koi imaat pristap do informaciite ili sredstvata na bankata, treba isto taka da imaat odgovornost za sigurnosta, koja e jasno definirani i opredelena vo dogovorite za koristewe na nivnite servisi.

Vrabotenite treba da znaat, da razbiraat i da bidat odgovorni za ispolnuvawe na nivnite obvrski kon sigurnosta. Ovie odgovornosti bankata treba da gi definira vo politikata za informativna sigurnost. Bankite treba da rabotata na podigawe na svesta na vrabotenite vo pogled na informativnata tehnologija i obezbeduvawe na sigurno rabotewe. Vrabotenite treba da imaat treninzi za rabota so aplikaciite i treninzi za sigurnost.

3.1.2. Ulogata na Odborot za revizija, Slu`bata za vnatre{na revizija i Nadvore{nata revizija

Bankata e dol`na da izvr{i testirawe na sistemite i procedurite za kontrola, koi se del od politikata na informativniot sistem na bankata, od strana na nezavisen i soodvetno obu~en tim (REVIZIJA). Reviziite treba da se vr{at pri vospostavuvaweto na politikata za informativna sigurnost, kako i periodi~no, a osobeno vo slu~aj na pozna~ajni izmeni na politikata za informativna sigurnost.

**Celta na revizijata vo bankata e da dade nezavisna i objektivna ocenka za raspolo`ivosta, doverlivosta i integritetot na informativniot sistem na bankata i efikasnosta na implementiranite kontroli.** Ovie ocenki mo`at da pomognat za odr`uvaweto i podobruvaweto na efikasnosta na upravuvaweto so rizikot na bankata i unapreduvaweto na vnatre{nite kontroli.

Neophodno e slu`bata za vnatre{na revizija i nadvore{nata revizija vo pogled na IT da gi sledi profesionalnite standardi za vr{ewe na ovoj tip na revizija, kako {to se **Standards for the Professional Practice of Internal Auditing** izdadeno od

Institute for Internal Auditors (IIA) ili pak tie koi se izdadeni od asocijacijata **Information System Audit and Control Association (ISACA)**. Ovie standardi gi obrabotuvaat nezavisnosta, etikata, profesionalnite ve{tini, delokrugot na rabota, izveduvaweto na revizijata i kontrola na kvalitetot na izvr{enata revizija.

3.1.2.1 Ulogata na Odborot za revizija

Rabotovodniot organ na bankata e dol`en da vospostavi adekvatni sistemi na vnatre{na kontrola. Upravniot odbor, od svoja strana, vodi smetka dali rabotovodniot organ vospostavil soodvetni sistemi na vnatre{na kontrola. Vo sproveduvaweto na ovaa funkcija, pokraj Upravniot odbor i rabotovodniot organ, se vklu~eni i posebni tela vo bankata: **Slu`ba za vnatre{na revizija i Odborot za revizija**. **Golem broj vnatre{ni kontroli se sostaven del od informativniot sistem na bankata.** Za da mo`e Upravniot odbor da se osigura deka rabotovodniot organ vospostavil efikasni vnatre{ni kontroli mo`e da bara:

- Vrabotuvawe na IT revizor vo slu`bata za vnatre{na revizija na bankata;
- Izvr{uvawe na IT revizija od strana na nadvore{na revizija;
- Koristewe na kombinirana metoda.

Revizija na sigurnosta na informativniot sistem se vr{i i od strana na Narodna banka na Republika Makedonija kako supervizorski organ vo zemjata.

Upravniot odbor i Odborot za revizija treba da bidat zapoznati so rizicite i kontrolnite mehanizmi koi se prisutni vo izveduvaweto na bankarskite operacii, vklu~uvaj}i gi rizicite koi proizleguvaat od pojavata na novi proizvodi i servisi, implementacija na novi tehnologii i informativni sistemi i voveduvawe internet i elektronsko bankarstvo.

Upravniot odbor i Odborot za revizija treba da gi razgleduvaat slednite rizici koi se odnesuvaat na tehnologijata:

- Neadekvatni vnatre{ni kontroli postaveni na informativniot sistem na bankata;
- Netestirani, neadekvatni i neefektivni PKR;
- Finansiski zagubi i gubewe na reputacija povrzana so padovi na informativnite sistemi (na pr. nerabotewe na {alteri);
- Neavtorizirano objavuvawe na doverlivi podatoci;
- Neraspolo`ivi ili skapi implementacii na IT re{enija;
- Neadekvatnost na IT sistemite za potrebite na bankata;
- Neadekvatna analiza i neadekvatni dogovori so obezbeduva~ite na IT servisi na bankata;
- Neadekvatni sistemi za nabquduvawe na sistemite za obrabotka na transakciite i sistemite za ~uvawe na podatocite;
- Neefektivni treninzi na vrabotenite i korisnicite na sistemite;
- Nedostatok na proceduri i kontroli sprema krajnite korisnici za rabota so informativniot sistem (na pr. vrabotenite).

3.1.2.2. Ulogata na Slu`bata za vnatre{na revizija

Slu`bata za vnatre{na revizija ima za zada~a da se gri`i za postojana i celosna kontrola na adekvatnosta i efikasnosta na vospostavenite sistemi za vnatre{na kontrola. Za da ja sprovedat ovaa glavna funkcija na nivo na cela banka, Slu`bata za vnatre{na revizija treba da vr{i kontrola na postavenosta i adekvatnosta na postavenite vnatre{ni kontroli na informativniot sistem na nivo na cela banka. Soglasno so ~len 10, ~len 11 stav 4 i ~len 18 od Odlukata za definirawe na standardite za izgotvuvawe i sproveduvawe na sigurnosta na informativniot sistem, bankite treba da vr{at revizija i na sigurnosta na informativniot sistem i revizija na usoglasenosta na svoite obezbeduva~i na IT servisi so vospostaveniot proces na informativna sigurnost vo bankata. Za vr{ewe na ovaa funkcija so potrebnoto nivo na profesionalna kompetentnost, bankite mo`at vo Slu`bata za vnatre{na revizija da vrabotat IT revizor. IT revizorot treba da poseduva znaewe i iskustvo za vr{ewe kontrola na celokupniot informativen sistem vo bankata, kako i na podobnosta na obezbeduva~ite na IT servisi od aspekt na ispolnuvawe na kriteriumite za sigurnost na informativniot sistem. IT revizorot treba da e vo tek so sekojdnevnite promeni na revizorskite tehniki i rizicite koi se povrzani so voveduvaweto na novi finansiski aktivnosti.

Dokolku vo Slu`bata za vnatre{na revizija ne postoi specijaliziran IT revizor, toga{ kontrolata od strana na Slu`bata za vnatre{na revizija treba da se vr{i kombinirano so anga`irawe na nadvore{na IT revizija. Imeno, Slu`bata za vnatre{na revizija }e vr{i kontrola na **generalnite (op{tite) kontroli,** koi vklu~uvaat dokumentiranost na procedurite za rabota na IT organizacionata edinica, kontrola na otvorenite korisnici na informativniot sistem i nivni privilegii za rabota, za{tita na podatoci i kontrola na uspe{nosta na za{titata, nabquduvawe na testiraweto na PKR itn. Nadvore{na IT revizija }e vr{i aplikativni kontroli, za da se postigne potrebnoto nivo na pokrivawe na kompletniot informativen sistem. Soglasnost za izborot na nadvore{nata revizija na predlog na Upravniot odbor dava Sobranieto na bankata.

Ottuka proizleguva deka bankata ne mora da ima IT revizor koj }e bide vraboten vo Slu`bata za vnatre{na revizija, tuku deka mo`e da ima k**ombiniran pristap** na kontrola na sigurnosta informativniot sistem.

Slu`bata za vnatre{na revizija treba da ja vr{i kontrolata na sigurnosta na informativniot sistem vrz osnova na godi{en plan za revizija, odobren od strana na Upravniot odbor. Planot treba da se revidira vo zavisnost od potrebite.

Metodolo{ki, planot za vr{ewe na IT revizii treba da se zasnova na procenka na site rizici na raboteweto, {to voedno pretstavuva potvrda deka Slu`bata za vnatre{na revizija ima razbirawe za zna~ajnite aktivnosti na bankata i rizicite {to gi nosat tie aktivnosti. Direktorot na ovaa Slu`ba treba ?? vospostavi principi za procenka na rizicite vo forma na pi{ani proceduri, koi treba postojano da se revidiraat, soglasno so promenite na sistemot na vnatre{na kontrola ili na rabotnite procesi.

Najva`ni faktori koi mo`e da pomognat vo gradewe na efikasen sistem na procenka na rizici na Slu`bata za vnatre{na revizija vo pogled na IT se:

- Adekvatnosta na sistemite na vnatre{ni kontroli;
- Adekvatnosta na sistemite za nabquduvawe od strana na rabotovodniot organ;
- Prethodnite zabele{ki od strana na revizijata i sposobnosta na rabotovodniot organ da gi otstrani nedostatocite;

- Fizi~kata i logi~kata sigurnost na informativniot sistem (oprema i objekti);
- Starosta na informativniot sistem i bankarskite aplikacii;
- Operativniot rizik vo poedine~ni organizacioni edinici vo bankata;
- Frekvencijata na promeni vo na~inot na izvr{uvawe na operaciite (planirani konverzii na podatoci, migrirawe na novi sistemi, potencijalna finasiska {teta);
- Vraboteni, iskustvoto na rabotovodniot organ i vrabotenite, tehni~kata kompetentnost.

Pri izrabotkata na planot, Slu`bata za vnatre{na revizija treba da gi ima predvid i navedenite faktori, voveduvaweto na novi aktivnosti, proizvodi i inovacii, kako i rizicite {to gi nosat novite aktivnosti, promenata na opkru`uvaweto, unapreduvaweto na informativnite sistemi i dr. Isto taka, treba da se zemat predvid obemot, prirodata i frekfencijata na zada~ite {to treba da se izvr{at, periodot od poslednata revizija, nevoobi~aenite i nekarakteristi~nite promeni i drugi podatoci i informacii.

Izve{taite od izvr{enite IT revizii se dostavuvaat do Upravniot odbor, Odborot za revizija, kako i do rabotovodniot organ, direktorot na organizacioniot del - predmet na revizija i direktorite na organizacionite delovi koi se povrzani so predmetot, preporakite ili merkite od izvr{enata revizija.

Slu`bata za vnatre{na revizija ima pravo na pristap do site podatoci i dokumenti, bez razlika na na~inot i mestoto kade se ~uvaat i stepenot na nivnata doverlivost, do site informativni sistemi i vlez vo site delovni prostorii bez razlika na na~inot na koj tie se obezbedeni.

Revizijata treba da ja sledi reakcijata na rabotovodniot organ za odredena nepravilnost i da vospostavi soodveten sistem za sledewe na otstranuvaweto na nepravilnostite i nedostatocite vo dadenite vremenski ramki.

Za vr{ewe na IT revizija ili za generalna proverka na nekoi sistemi za vnatre{na kontrola, Slu`bata za vnatre{na revizija mo`e da pobara nabavka na specijaliziran softver za poefikasno vr{ewe na svojata funkcija ili pak vo sorabotka so IT organizacionata edinica da razvie sopstven revizorski softver.

Slu`bata za vnatre{na revizija ne treba da se involvira vo dnevnite aktivnosti na bankata, no nejzinite vraboteni mo`e da u~estvuvaat vo postojani i povremeni rabotni komisii kako konsultanti, nabquduva~i i pretstavnici bez pravo na glas. **Voveduvaweto na novi proizvodi i servisi e dobar primer kade revizijata treba da bide vklu~ena, od aspekt na davawe soveti za kontroli koi odnapred treba da se implementiraat vo sistemot, a ne otkako sistemot }e se napravi. Zaradi toa {to sekoja dopolnitelna prerabotka e poskapa.**

3.1.2.3. Ulogata na nadvore{nata revizija

Obemot na rabota na nadvore{nata IT revizija treba da bide definirana vo pismoto za nivno anga`irawe (**engagement letter**). Vo ovie pisma obi~no se navedenite delokrugot na revizijata, celite koi treba da se postignat, koi resursi se potrebni, vremenskiot rok na revizijata i izve{taite koi }e bidat podgotveni.

Nadvore{nata IT revizija treba da bide izvr{ena od nezavisen i kvalifikuvan tim, zaradi postignuvawe na osnovnata cel za nivno anga`irawe. Kvalifikuvani IT revizori pretstavuvaat revizori koi imaat me|unarodni ili doma{ni akreditirani sertifikati za vr{ewe na ovaa funkcija.

Izve{tai od izvr{enite revizii na sigurnosta na informativniot sistem treba da go informiraat Upravniot odbor i rabotovodniot organ za nivoto na usoglasenost na poedine~ni organizacioni delovi so propisite, politikite i procedurite za sigurnosta na informativniot sistem. Voedno, ovie izve{tai treba da sodr`at i inforamcii za efikasnosta na vospostavenite sistemi na vnatre{na kontrola, kako i ocenka na postojniot sistem i identifikuvawe na negovite slabosti, kako i davawe preporaki za negovo podobruvawe.

Nadvore{nata revizija mo`e da bide anga`irana za revizija na generalnite kontroli, kako i za revizija na aplikativnite kontroli. **Aplikativnite kontroli** se povrzani za specifi~ni informativni sistemi i davaat razumni veruvawa deka ~uvaweto, procesiraweto i izve{taite koi proizleguvaat od informativnite sistemi se to~ni, a implementacijata na soodvetni vnatre{ni kontroli na poedine~ni informativni sistemi e adekvatna.

Za proverka na odredeni generalni i aplikativni kontroli, nadvore{nata revizija mo`e da koristi specijalizirani revizorski softveri za taa namena. (t.n. **COMPUTER ASSISTED AUDIT TECHNIQUES - CAATs**). Celta na ovie softveri e podobruvawe na efikasnosta na revizijata, bidej}i avtomatski obrabotuvaat pogolem broj primeroci. Ovoj softver mo`e da pravi kontrola na presmetkata na kamati i provizii vo odredena organizaciona edinica, proverka na sigurnosnite postavki na opremata i drugi vidovi proverka na sistemite za vnatre{na kontrola. Izve{taite od ovie softveri se koristat kako rabotni materijali vo tekot na revizijata.

Bankata treba da obezbedi da ne se koristat specijaliziranite revizorski softveri za koj revizorite nemaat dovolna tehni~ka dokumentacija i iskustvo, bidej}i nivnata upotreba mo`e da go naru{i stabilnoto i sigurnoto funkcionirawe na informativniot sistem.** Zatoa, vo pismoto za anga`irawe na nadvore{niot revizor (engagement letter**), treba precizno da se utvrdat revizorskite softveri koi }e bidat upotrebuvani vo vr{eweto na revizijata.

Kako poseben tip na testirawe koe mo`e da se pobara od nadvore{nite IT revizori e testirawe na otpornosta na IT sistemot na napadi odnadvor ili odvnatre t.n. **testovi za penetracija na IT sistemot** (**"penetration testing"**). Za izvr{uvawe na ovoj vid testirawe treba da se sklu~i poseben dogovor so nadvore{nite revizori, vo koj isto taka }e bidat precizno utvrdeni uslovite na revizijata. Ova e potrebno zatoa {to **so neplanskoto izveduvawe na ovie testovi se zagrozuva normalnoto funkcionirawe na bankata.** Ovie testovi treba da se izveduvaat na kompletna redudantna okolina (alternativnata lokacija). Pronajdeni nedostatoci i slabosti se koregiraat prvo na sekundarnata, a podocna i na primarnata lokacija na bankata.

Bez pismena soglasnost od rabotovodniot organ, nadvore{nata IT revizija ne smee da vr{i testovi za penetracija na informativniot sistem na bankata.

3.2. UPRAVUVAWE SO IT

3.2.1. Odbor za nadgleduvawe na IT

Za efikasno nabquduvawe na IT aktivnostite na bankata, naj~esto se formira poseben odbor t.n. Odbor za nadgleduvawe na IT (IT Steering commitee). Celta na ovoj Odbor e da mu pomaga na Upravniot odbor vo noseweto na odlukite vo vrska so IT. Odborot za nadgleduvawe na IT treba da bide sostaven od eden ~len na rabotovodniot organ, pretstavnici na organizacuionite edinici od bankata koi imaat poznavawe na procedurite i upatstvata na bankata, a osobeno na onie koi se odnesuvaat na informativniot sistem. ^lenovi na ovoj Odbor mo`e da bidat i nadvore{ni specijalisti. Ovoj odbor treba da podnesuva izve{taj do Upravniot odbor za statusot na IT vo bankata i koi pra{awa se otvoreni. Odborot treba da podgotvuva adekvatna informacija do Upravniot odbor, za da mo`e da donese pravilna odluka. Odborot treba da obezbedi efektivno planirawe na IT i sledewe na kapacitetot na IT sistemot i na negovite performansi. Isto taka Odborot mo`e:

- da go nabquduva razvojot na strate{kite IT planovi;
- da odobruva anga`irawe na obezbeduva~i vo odnos na IT i da ja nabquduva nivnata finansiska sostojba;
- da gi odobruva i da gi nabquduva glavnite proekti, IT buxet, prioritetite, standardite, procedurite i performansite na sistemot;
- da gi koordinira prioritetite pome|u IT oddelot i drugite oddeli;
- da gi nabquduva adekvatnosta na IT resursi vo smisla na lu|e, oprema, dogovori so obezbeduva~i na IT servisi.

Bankata treba da vodi uredni zapisnici od odr`anite sostanoci na Odborot za nadgleduvawe na IT so cel dokumentirawe na svoite odluki i informirawe na Upravniot odbor za svoite aktivnosti na polugodi{na osnova.

3.2.2. Organizacija na IT

Organizacijata na IT e specifi~na za sekoja banka poedine~no. Prepora~livo e organizacijata na IT vo bankata da se definira po sproveduvawe na analizata na rizik vo bankata i sproveduvawe na analizi vo odnos na podobruvawe na performansite vo izveduvawe na operaciite.

Generalno, postojat dva pristapa na upravuvawe so IT i toa: **centraliziran i decentraliziran**.

Vo centraliziraniot pristap, IT e organizaciona edinica pod direkna subordinacija na rabotovodniot organ na bankata. Generalno, vo ovoj pristap vr{i nabavka, instalacija i odr`uvawe na site tehnolo{ki re{enija na nivo na cela banka. So ovoj pristap bankata ima pogolema mo`nost za nadgleduvawe i kontrola vrz celokupnata instalirana tehnologija vo bankata. Centraliziraniot pristap ni nudi zgolemena efikasnost vo izvr{uvaweto na operaciite. Direktorite na organizacionite edinici se odgovorni za sproveduvawe na internite kontroli vo ramkite na svoite organizacioni edinici.

Vo decentaliziraniot pristap, IT kako organizaciona edinica ima ~isto sovetodavna uloga vo nekoi organizacioni edinici vo pogled na nabavkata,

instalacijata i odr`uvaweto na odredeni tehnolo{ki re{enija. Ova naj~esto se slu~uva vo banki so kompleksna organizaciona struktura, so {to se vr{i transfer na odlu~uvaweto za implementiranata tehnologija kon strate{ki va`ni te organizacioni edinici na bankata. Vo toj slu~aj direktorite na ovie direkcii treba da se osiguraat deka investicijata vo tehnologijata vo nivniot oddel e konzistentna so strate{kite IT planovi na nivo na cela banka.

Vo vakov slu~aj rabotovodniot organ treba da obezbedi kompatibilnost na IT sistemite i sproveduvawe na IT politikite vo decentraliziranata okolina.

3.2.3. Upravuvawe so proekti

Upravuvaweto so IT ima dve glavni zada~i. Prvata zada~a e kontrola na raspolo`ivosta i dostapnosta na tehnologijata, operaciite i servisite vo razli~ni delovni edinici vo bankata. Vtorata zada~a e nadgleduvawe na tehnolo{kite, delovnite i operativnite **promeni** vo procesite na bankata. Upravuvaweto so proekti e tesno povrzano so ostvaruvawe na vtorata zada~a.

Efektivno upravuvawe so proektite e klu~en faktor za dobro upravuvani IT operacii i uspe{no sledewe na konfiguraciite. Upravuvaweto so proekti zavisi od goleminata i kompleksnosta na bankata, kako i od goleminata i kompleksnosta na zada~ata. Generalno vo sekoj proekt postojat fazi kako {to se: **zapo~nuvawe**, **planirawe**, **izvr{uvawe**, **kontrola** i **zatvorawe** na proektot. Menaxmentot treba da ja koristi ovaa tehnika za da gi kontrolira proektite koi se od golema va`nost za bankata i koi mo`e da predizvikaat visok operativen rizik (nadgradba i razvoj na sistemite, konverzija na podatocite od star sistem na nov, voveduvawe na novi infrastrukturni komponenti (novi serveri), voveduvawe novi tipovi produkti i servisi, kako i podobruvawe na odredeni bankarski aplikacii ili servisi i dr.). Dobroto upravuvawe so proektite od strana na bankata treba da napravi uslovi za podobro prifa}awe na promenite koi se nametnati od delovnoto opkru`uvawe i za zadovoluvawe na strate{kite celi na bankata.

Proektniot tim ima zada~a da napravi lista na proektnite zada~i i da napravi prioritetna lista. Proektniot tim treba da sogleda koi se rizicite koi se povrzani so uspe{na realizacija na proektot. Za da ima nadzor vrz proektite rabotovodniot organ treba da izgradi sistem za kontrola na statusot na proektite vo bankata (minimalniot sistem za kontrola treba da sodr`i: **datum na zavr{uvawe** na odredeni celi od proektot i **status na proektot** vo momentot). Rabotovodniot organ treba da obezbedi poddr{ka za disciplinirano upravuvawe i vodewe na proektite.

Posledna faza na proektite e nivno formalno zatvorawe. Pred formalno zatvorawe na proektite, potrebno e za site izvr{eni promeni vo sistemot, krajnite korisnici da go dobijat potrebnoto nivo na obuka i trening, a izmenite vo tehni~kata i korisni~kata dokumentacija da se a`uriraat.

3.2.4. Menaxment informativen sistem (set izve{tai do menaxmentot Management Information Sysem-MIS)

Setot izve{tai koi se nameneti za menaxmentot (MIS) koi se produciraat od informativniot sistem treba da obezbedat dovolen broj na informacii za da mo`e menaxmentot da donese pravilna delovna odluka. To~ni i navremeni podatoci vo izve{taite kon menaxmentot se osnova za nosewe na prudentni i razumni delovni odluki. Rabotovodniot organ treba da se pogri`i za obezbeduvawe na integritetot (to~nosta i kompletnosta) na ovaa informacija, kako i obezbeduvawe na raspolo`ivosta na ovoj sistem, so cel da bide dostapen vo momentite na nosewe na delovni odluki. Menaxmentot treba da se trudi da go dizajnira svojot MIS na na~in so koj }e gi izbegne ili reducira tro{ocite na napornata manuelna rabota na generirawe na ovie izve{tai prosledena so visok operativen rizik i da se celi kon avtomatizacija na istiot. Dobro vospostaveniot sistem }e obezbedi podobra komunikacija pome|u razli~nite organizacioni edinici i vrabotenite vo bankata.

MIS treba da se gradi na pove}e nivoa, i toa od operativnite rakovoditeli kon strate{kite rakovoditeli.

MIS na nivo na Upraven odbor i rabotovoden organ treba da dava informacii za nosewe na strate{ki odluki za bankata.

Napredokot vo tehnologijata nosi i pove}e vidovi informacii koi mo`e da bidat raspolo`iva za menaxmentot na bankata. Me|utoa tehnologijata go zgolemuva rizikot od nosewe odluki vrz baza na pogre{ni izve{taii. Bidej}i generiraweto na izve{taii mo`e da se bazira i na ra~no vnesuvawe brojki od razli~ni sistemi vo ramkite na bankata, rabotovodniot organ **treba da vospostavi kontrola vrz procesot na izrabotka na istite izve{taii, a Slu`bata za vnatre{na revizija da dade ocenka za efikasnosta na implementiranite kontroli na MIS.** Bidej}i ovie informacii proizleguvaat od re~isi site sistemi na bankata, rabotovodniot organ treba da se pogri`i da vospostavi kontroli za to~nosta na integritetot na podatocite niz tie poedine~ni sistemi.

3.2.5. PLANIRAWE i STRATEGIJA

Planiraweto pretstavuva proces na podgotovka na idni aktivnosti, so definirawe na celite i startegiite koi se potrebni za nivno postignuvawe. IT e integralen del od operaciite koi se odvivaat vo bankata. Zatoa, finasiskite institucii treba da izvr{at integracija na svoite resursi i investicii vo globalniot deloven plan na bankata. Golemite investicii vo IT imaat dolgoro~ni vlijanija vrz raspolo`ivosta i performansite na servisite {to gi nudi bankata. Planovite mo`e da zavisat od tipot i kompleksnosta na bankata.

Sekoja banka treba da ima proces na PLANIRAWE koj permanentno }e gi zema predvid novite rizici i }e go maksimizira efektot na instaliranata tehnologija za bankata Planovite za IT i globalniot deloven plan na bankata treba da bidat usoglaseni. So ogled na toa, pri izrabotka na planot treba da bidat vklu~eni Upravniot odbor, rabotovodniot organ i krajnite korisnici vo negovata izrabotka. Upravniot odbor treba da go odobri planot. Postojat dva tipa na planovi i toa: **strate{ki IT planovi** i **operativni (takti~ki) planovi**.

3.2.5.1. Strate{ki IT planovi

Starte{kite IT planovi treba da se fokusiraat na period od tri do pet godini i treba da se usoglasat so delovnata dolgoro~na strategija na bankata. Dokolku planot e efikasen }e se postigne balans na tro{ocite koi proizleguvaat od IT operaciite i kompetativnite barawa na organizacionite edinici niz bankata.

Starte{kite IT planovi treba da se temelat vrz ostvaruvawe na dolgoro~ni celi. Za ostvaruvawe na ovie celi treba da se obezbedat adekvatni resursi. Starte{kite planovi treba da sodr`at podatoci za buxetot, periodi~nite izve{tai kon Upravniot odbor i statusot na kontrolite za upravuvawe so rizicite. Pri definiraweto na strate{kite planovi za IT, Upravniot odbor i rabotovodniot organ treba da gi imaat predvid:

- pozicijata na pazarot;
- trendovite na razvoj na bankata;
- tehnologijata i standardite;
- barawata na regulatornite tela;
- namaluvaweto na tro{ocite;
- podobruvaweto na procesite;
- koristeweto na nadvore{ni obezbeduva~i ili koristewe na vnatre{ni timovi za razvoj na IT;
- optimalnata infrastruktura za idninata;
- sposobnosta za prifa}awe i integracija na novi tehnologii.

Odborot za nadgleduvawe na IT treba da gi usoglasuva investiciite vo IT so strate{kite i operativni celi na bankata.

Bi bilo pogre{no da se tro{at ogromni sredstva za tehnologija koja delovnite organizacioni edinici na bankata ne mo`e celosno da ja iskoristat. Od druga strana, bankite mo`e da tro{at premnogu konzervativno i da gi odlo`uvaat investiciite vo infrastruktura i novi proizvodi i servisi, so {to mo`e da go izgubat mesto na pazarot i da pretrpat zagubi vo profitot. **Nedostatokot na znaewe na novite i postojnite tehnologii mo`e da predizvika zgolemen rizik na sigurnosta na informativniot sistem.** Postojat ~etiri zna~ajni faktori za dizajnirawe dobar strate{ki plan i toa:

- **Silna poddr{ka od menaxmenot** na bankata-rabotovodniot organ na bankata treba da ima dobro poznavawe i da mu dade poddr{kata na IT strate{kiot plan i da gi odredi prioritetite;
- **Ulogata na IT**-da se razjasni koja e ulogata na IT vo bankata i dali sega{niot na~in na planirawe i organizacija vodi kon postignuvawe na zacrtanite celi;
- **Zna~eweto na IT**- Odborot za nadgleduvawe na IT treba da gi razbere povrzanosta pome|u IT infrastrukturata, aplikaciite i delovnite strate{ki planovi na bankata;
- **Vrednuvawe na prethodnite performansi**- Odborot za nadgleduvawe na IT treba da vospostavi objektivni sistemi za merewe na dobivkite/tro{ocite (**"cost/benefit"**) koi se napraveni so proektite koi se vodeni za da se postignat odredeni zacrtani celi.

3.2.5.2. Operativni IT planovi

Operativnite IT planovi treba logi~ki da proizleguvaat od starte{kiot IT plan. Upravniot odbor treba da gi razgleduva na godi{no nivo. Operativnite planovi se fokusirani na konkretni operativni aktivnosti so to~no obezbeden buxet za nivno ostvaruvawe. Rabotovodniot organ treba da se osigura deka poseduva adekvatni resursi na IT za ostvaruvawe na svoite operativni planovi. Delovnite procesi se pretstaveni kako integracija na lu|eto, tehnologijata i strogo definirani administrativni proceduri za da se ostvarat odredeni zada~i. Promenite vo delovnite procesi obi~no nosat promena vo tehnolo{kite procesi, zatoa e potrebna koordinacija so raspolo`ivite IT resursi. IT resursite koi treba da se koordiniraat vklu~uvaat:

- **Infrastruktura**-elektri~na energija, telekomunikacii, mre`na arhitektura i zgradi;
- **Aplikativen softver**-softver i negovite kontinuirani promeni{to se koristat za da se obezbedat finasiskite servisi;
- **Operativen softver**-operativni sistemi, kompajleri i alatki koi slu`at za dizajnirawe na opremata i aplikaciite da rabotat efikasno i to~no;
- **Hardver**-serveri, mre`ni serveri, personalni kompjuteri, komunikaciski uredi, uredi za arhivirawe i ostanati periferni uredi. Pri planiraweto treba da se ima vo predvid deka serverite i personalnite kompjuteri treba da poseduvaat dovolen i adekvaten kapacitet za tekovnite potrebi i da gi zadovolat idnite trendovi.
- **Vraboteni**-tuka treba da se planira potrebniot broj resursi koi treba da se posvetat na odredeni re{enija, nivniot kontinuitet vo izvr{uvaweto na operaciite i potrebata od trening i obuka.

3.2.5.3. Buxet za IT

Buxetot za IT pretstavuva finansiski plan koj treba da se koristi za kontrola na uspe{no izvr{uvawe na bankarskite operacii so informativna tehnologija. Buxetot pretstavuva va`en element vo idnite predviduvawa za tro{ocite, no i vistinska proverka za rabotovodniot organ.

Vo ramkite na novite tehnolo{ki proekti treba da se zemat predvid po~etnite tro{oci za instalacija na tehnolo{koto re{enie, kako i tro{ocite koi nastanuvaat vo periodot po implementacija. Bankata treba da pobara od svoite obezbeduva~i na IT servisi da dadat informacii za **vkupnite tro{oci za poseduvawe na sredstvoto** (**parametar: TCO – Total Cost of Ownership**) pri planirawe na negovata nabavka. Proekciite vo tehnologijata obi~no imaat i neplanirani tro{oci, kako {to se tro{ocite za konfiguracija, odr`uvawe, popravka i nadgradba i upravuvawe so tehnologijata vo tekot na nejziniot `ivoten ciklus vo bankata.

Bankata treba da sprovede finasiska analiza za IT organizaciskata edinica kako i analiza i sporedba na tro{oci i efikasnosta na sistemot. Vo zavisnost od taa analiza treba da se odlu~i dali za funkcionirawe na IT sistemot bankata }e koristi **vnatre{ni resursi** t.n.(**in-house operacii**) ili }e anga`ira **obezbeduva~ na IT servisi t.n. (outsourcing na operaciite)**.

4. Odgovoren za sigurnosta na informativniot sistem (OSIS)

OSIS treba da vr{i procenka na rizicite, analiza na verojatnosta od pojava na zakanite, predlaga unapreduvawe na politikite i procedurite za informativna sigurnost i gi predlaga na usvojuvawe do Upravniot odbor na bankata. OSIS e odgovoren za implementacija na sigurnosnite kontroli na nivo na cela banka i vr{i nabquduvawe na nivnata efikasnost. OSIS e odgovoren za efektivno funkcionirawe na procesot na informativna sigurnost na nivo na cela banka. OSIS vr{i nabquduvawe na naru{uvawata na politikite i procedurite i u~estvuva vo testirawata na efektivnosta na implementiranite kontroli. OSIS treba da go zabele`i sigurnosniot incident i da go alarmira menaxmentot so cel prezemawe koordinirana akcija za za{tita na bankata od mo`ni finansiski zagubi.

OSIS ne treba da bide vraboten vo IT organizacionata edinica, tuku za svoeto rabotewe direktno odgovara pred rabotovodniot organ. IT organizacionata edinica mo`e da ima vraboten koj sekojdnevno }e se gri`i za implementacija na politikite za sigurnosta na informativniot sistem, me|utoa tie ne smeat da davaat poedine~ni privilegii koi ne soodvestvuvaat na onie predvideni vo politikata na informativniot sistem na bankata.

OSIS e odgovoren za obezbeduvawe siguren informativen sistem na bankata. Imeno, OSIS gi ima slednive nadle`nosti:

- Da vr{i analiza i procenka na rizicite kon informativniot sistem na bankata vo soglasnost so procesot na informativna sigurnost;
- Kreirawe, implementacija i razvoj na celokupen proces za informativna sigurnost (glava 2 od Cirkularot);
- Kreirawe, implementacija, unapreduvawe i razvoj na Planot za kontinuitet vo raboteweto i Planot za sanacija na katastrofa (glava 5 od Cirkularot);
- Da predlaga do Upravniot odbor politiki, strategii, proceduri i upatstva so koi se postignuva sigurnosta na informativniot sistem;
- Koordinirawe na site sigurnosni aktivnosti na sistemot na bankata;
- Dava odobrenie za vr{ewe na promeni koi se izveduvaat na informativniot sistem na Bankata;
- Dava odobrenie za privilegiran pristap do sistemot;
- Predlaga programa za revizii vo pogled na sigurnosta na informativniot sistem na bankata;
- Vr{i revizija na incidenti povrzani so naru{uvawa na sigurnosta na informativniot sistem, slabostite i gre{kite na sistemot na bankata, vklu~uvaj}i i sorabotka so MVR/NBRM;
- Sorabotka/koordinacija so ~uvarskata slu`ba;;
- Dava specifikacija na sigurnosnite uslovi koi treba da se vmetnat vo dogovorite so treti lica vo vrska so sigurnosta na informativniot sistem na bankata;
- Raboti na podigawe na svesta za sigurnost na informativniot sistem i organizacija na trenizi i obuka na vrabotenite za sigurnost;
- Pomaga pri izvr{uvaweto na revizii i proverki na sigurnosta na informativniot sistem, vr{i ocenka i upravuva so implementacijata na korektivnata akcija na sistemot na bankata;

- Gi pregleduva site revizorski tragi (audit logs) i kontrolni dnevnici (logs) koi se vodat na nivo na banka za odreden period i da garantira deka tie redovno se odr`uvaat;
- Ja izvr{uva svojata rabota vo soglasnost so regulativata i me|unarodnite standardi za sigurnost na informativnite sistemi;
- Gi razjasnuva site nejasnotii vo pogled na sigurnosta na informativniot sistem na licata koi rabotat na sistemot na bankata, vr{i obuka i trenizi vo pogled na sigurnosta.

4.1. Procenka na riziko t

OSIS treba da napravi identifikacija na informativniot sistem i negova klasifikacija. OSIS treba da go vospostavi celokupniot proces na informativna sigurnost (naveden vo glava 2 od Cirkularot) i da izraboti analiza i procenka na rizicite koja }e ja vr{i na kontinuirana osnova. Procenkata na rizikot e naj~esto prviot ~ekor vo kreiraweto na efikasna politika na informativna sigurnost. Bez takva procenka, bankata nema da znae {to treba da se za{titi i koe e potrebnoto nivo na za{tita. Na toj na~in, bankata nema da ima adekvatna pretstava za mo`nite finasiski zagubi koi mo`e da gi pretrpi dokolku se pojavi odredena zakana po informativniot sistem.

4.2. Gradewe na politika ta za sigurnos t na informa tivnio t sis tem

OSIS treba da izraboti politiki, proceduri, standardi i upatstava i istite da gi predlo`i za usvojuvawe do Upravniot odbor na bankata. OSIS treba da se gri`i i za razvoj i nadgradba na politikite na informativna sigurnost. Toa zna~i deka politikata za informativna sigurnost treba da se menuva taka {to sigurnosta na informativnite sistemi }e bide na adekvatno nivo so novite zakani i rizici. OSIS e odgovoren da predlaga unapreduvawe na politikite, upatstvata, standardi, proceduri i sl.

4.3. Gradewe na Plano t za kon t inui te t vo rabo tewe to(PKR)

Kako po~etni ~ekori za izrabotka na PKR, OSIS treba da napravi analiza na mo`nite {teti i procenka na rizikot. OSIS treba aktivno da u~estvuva vo implementacijata, razvojot i testiraweto na PKR. (glava 5 od Cirkularot).

4.4. Kvalifikacii i iskus tvo na OSIS

So cel stru~no i uspe{no izvr{uvawe na svoite rabotni zada~i, prepora~livo e OSIS da gi ima slednite kvalifikacii:

- Visoko obrazovanie (Elektrotehni~ki fakultet-otsek za kompjuterska tehnika ili Ekonomski fakultet);
- Iskustvo od bankarsko rabotewe;
- Integritet[2] na li~nosta;
- Sposobnost da vleva doverba i sigurnost;
- Dobri poznavawa za informativnite sistemi, zakani i rizici;
- Sposobnost da planira i da implementira promeni;

[2] Integritetot na li~nosta se ocenuva preku slednite elementi: ~esnost, kompetentnost, lojalnost, sposobnost za rasuduvawe, rabotlivost, neosuduvanost, rabotewe so koe nema da se vlijae vo nasoka na naru{uvawe na finansiska sostojba na bankata, ugled i verba kaj deponentite, responzivnost kon korektivnite merki izre~eni od strana na Narodna banka na Republika Makedonija, Odlukite na Upravniot odbor, preporakite od Slu`bata za vnatre{na revizija i nadvore{nata revizija.

- Sposobnost da objasnuva i da gi dokumentira novite koncepti i proekti;
- Poznavawe na sistemite i procesite koi se slu~uvaat na nivo na cela banka;
- Sposobnost da razmisluva strate{ki;
- Dobri organizaciski sposobnosti;
- Dobra sposobnost da nosi odluki;
- Dobra komunikaciska sposobnost ;
- Sposobnost da organizira i da vodi timska rabota.

Treba da se napomne deka OSIS treba da ima plan za obuka i trening koj mora da e na kontinuirana osnova, za da bide vo trend so novite tehnolo{ki rizici koi se pojavuvaat i na~inite za nivno kontrolirawe.

4.5. Izvestuvawe do Upravniot odbor i rabotovodniot organ na bankata za sigurnosta na informativniot sistem

OSIS treba da podgotvuva i da dostavuva redovni izvestuvawa do rabotovodniot organ i do upravniot odbor na bankata. OSIS treba da go izvestuva upravniot odbor na bankata najmalku dvapati godi{no, za statusot na procesot na informativna sigurnost. Izve{taite {to se dostavuvaat do Upravniot odbor treba da sodr`at: podatoci za identifikuvanite rizici i nivnata kontrola, informacii za dogovorite so obezbeduva~ite na IT servisi, rezultati od izvr{enite testirawa, naru{uvawa vo sigurnosta na informativniot sistem i soodvetnata reakcija od strana na menaxmentot, kako i preporaki i inicijativi za promeni vo politikata za sigurnost na informativniot sistem na bankata, od aspekt na nejzino unapreduvawe i modernizirawe. Vo izve{taite treba da bidat navedeni na~inot i merkite koi se prezemeni za kontrola na informativnata sigurnost, soveti i preporaki za poslednite promeni i promeni vo profilot na rizik vo klu~nite organizaciski delovi. Treba da se pokrijat planiranite aktivnosti sprovedeni vo minatiot period i da identifikuvaat mestata na koi treba da se implementiraat dopolnitelni kontroli ili onamu kade {to postoi zagri`enost. OSIS treba da izvestuva za stepenot na implementiranost na politikata za informativna sigurnost i da dava predlozi za nejzina promena.

Isto taka, OSIS podgotvuva vonredni izve{tai za poedine~ni incidenti ili za otkrieni novi prioritetni rizici za koi e potrebna momentalna reakcija. Ovie izve{tai treba da se podgotvuvaat vo soglasnost so incidentot i zavisat od frekvencijata na pojava na incidentot i potencijalnata {teta od udarot.

4.6. Koordinacija so IT organizacionata edinica vo pogled na informativnata sigurnost

OSIS treba da sorabotuva so IT organizacionata edinica, za da se obezbedi sorabotka i koordinacija na aktivnostite vo pogled na informativnata sigurnost. IT organizacionata edinica ima primarna odgovornost za odr`uvawe na funkcionalnosta na informativniot sistem. Dokolku vo IT organizacionata edinica ima lica koi se zadol`eni za obezbeduvawe na sigurnost na informativniot sistem, OSIS treba da sorabotuva so niv za da se implementiraat tehni~kite kontroli na nivo na celokupniot informativen sistem. Tie ne smeat da vr{at implementacija i instalacija na tehni~ki kontroli, bez prethodna avtorizacija na OSIS. Vo slu~aj na razli~ni gledi{ta pome|u OSIS i rakovoditelot na IT organizacionata edinica, za kone~en stav treba da se zeme stavot na rabotovodniot organ, a za razli~nite gledi{ta i argumentite po toj osnov OSIS go izvestuva Upravniot odbor.

4.7. Sorabotka so Slu`bata za vnatre{na revizija i nadvore{nata revizija

Redovnite revizii na politikite na informativna sigurnost i nasokite treba da obezbedat adekvatno nivo na za{tita na operaciite na bankata.

OSIS, zaedno so odgovorniot vo slu`bata za vnatre{na revizija vo bankata, predlagaat programa za revizii vo pogled na sigurnosta na informativniot sistem i ja dostavuvaat do Upravniot odbor.

OSIS ima bliska sorabotka vo izvr{uvaweto na vnatre{nite i nadvore{nite revizii na informativna sigurnost so cel podobruvawe na sigurnosta na informativniot sistem.

4.8. Asistirawe na korisnicite na informativniot sistem vo pogled na sigurnost

OSIS treba da raboti na zgolemuvawe na op{toto nivo na kultura i kolektivna svest kon zgolemena sigurnost na informativniot sistem na korisnicite.

OSIS gi zapoznava novite vraboteni so procedurite za informativna sigurnost, za da se osiguri deka se zapoznati so zakanite sprema informativnata oprema i ~ekorite koi se prezemaat za da se izbegnat istite rizici. U~eweto na informativnata tehnologija e va`en ~ekor vo kontinuiraniot proces na obuka na vrabotenite na site nivoa. OSIS treba da izraboti i da poseduva potpi{ani izjavi od site vraboteni za prifatlivo koristewe na informativniot sistem, pred da im dade avtorizacija za otvorawe na korisni~ki profil na informativniot sistem na bankata.

4.9. Nabquduvawe na usoglasenosta so politikata za informativna sigurnost

Implementacija na politikata na informativna sigurnost e kontinuiran proces. Treba da se dizajniraat i da se implementiraat pove}e pravila i nasoki koi go poddr`uvaat procesot na obuka na vrabotenite i podigawe na svesta za sigurnost. Nabquduvaweto na sproveduvaweto na politikata treba da se fokusira ne samo na pronao|awe na licata koi gi prekr{uvaat, tuku treba i da obezbedi na~in na sproveduvawe na procedurite od strana na vrabotenite bez nekoja pogolema pote{kotija ili stres.

4.10. Reakcija pri incidenti

Sigurnosen incident vo smisla na ovoj Cirkular pretstavuva ~in na direktno ili indirektno naru{uvawe na politikata za informativna sigurnost na bankata. Pri slu~uvawe na sigurnosen incident, OSIS mo`e da sostavi tim za reakcija pri incidenti koj mo`e da sodr`i pretstavnici od:

- Kadrova slu`ba-za koordinacija na disciplinskite merki;
- IT organizaciona edinica-za objasnuvawe na prirodata na incidentot;
- Fizi~ko obezbeduvawe-dokolku imalo naru{uvawa na fizi~kata bezbednost;
- Pretstavnici od organizacionata edinica kade nastanal incidentot;

Vo zavisnost od te`inata na incidentot mo`e da bidat prisutni i dopolnitelni ~lenovi primer:

- Rabotovodniot organ;
- MVR;
- Nadvore{ni konsultanti ili specijalisti;
- Pretstavnici od Direkcijata za bankarska supervizija.

Incidentite treba da se prijavat vo NBRM so popolnuvawe na obrazecot koj e vo prilog na ovoj Cirkular (Aneks2), najkasno pet dena posle nivnoto slu~uvawe.

5. PLAN ZA KONTINUITET VO RABOTEWETO

CEL

Prekin na delovnite procesi podrazbira sostojba vo koja bankata ne e sposobna da gi ispolni svoite delovni obvrski od pri~ini koi ne mo`e da gi kontrolira ili vo slu~ai koga bankata e fizi~ki ili telekomunikaciski o{tetena, odnosno ne se dostapni nejzinite informativni sistemi. Bidej}i bankite imaat klu~na uloga vo na{ata ekonomija, treba da bidat otporni na vakov tip na naru{uvawa, so cel namaluvawe na stepenot na prekin na servisot i zgolemuvawe na doverbata vo celokupniot finasiski sistem. Efektiven plan za kontinuitet gi postavuva osnovite za vospostavuvawe na delovnite operacii vo slu~aj na niven neo~ekuvan prekin. Planiraweto na uspe{en plan za kontinuitet vo raboteweto podrazbira restavracija na delovnite operacii vo slu~aj bankata da bide soo~ena so nastani kako {to se prirodni katastrofi, gre{ki vo tehnologijata, ~ove~ki gre{ki ili terorizam.

Celta na Planot za kontinuitet vo raboteweto e minimizirawe na finasiskata zaguba na bankata, restavracija i prodol`uvawe na servisnosta kon klientite i namaluvawe na negativnite efekti koi mo`e da vlijaat na ostvaruvawe na strate{kite planovi na bankata (reputacija, operativnost, likvidnost, pazarna pozicija, i dr.).

Bankata e dol`na da razvie i da implementira sopstven plan za kontinuitet vo raboteweto, koj }e se bazira na pove}e scenarija i }e ovozmo`i operativnost i minimizirawe na zagubite vo slu~aj na te`ok prekin na delovnite procesi.

Bankata treba da ovozmo`i identifikacija na kriti~nite operacii, vklu~uvaj}i gi i tie kade {to bankata zavisi od nadvore{ni obezbeduva~i ili treti lica. Bankata treba:

- da identifikuva alternativni mehanizmi za kontinuitet vo delovnite procesi vo slu~aj na prekin na primarnite mehanizmi;
- da ja identifikuva mo`nosta za restavrirawe na podatocite koi se potrebni za prodol`uvawe na delovniot proces;
- podatocite da se za{titeni na **sekundarna lokacija koja }e bide na adekvatna dale~ina od primarnata lokacija, za da se izbegne i da se minimizira rizikot dvete lokacii da bidat istovremeno nedostapni.**

Pri odbiraweto na alternativnata lokacija, treba da se vnimava taa da e na adekvatna oddale~enost od primarnata lokacija, za da ne mo`e dvete lokacii da bidat o{teteni od istata zakana.

Se prepora~uva alternativnata lokacija da bide oddale~ena najmalku 30 kilometri od primarnata lokacija za da se obezbedi maksimalna za{tita vo slu~ai na regionalni nesre}i i katastrofi.

Pri razvoj na Planot za kontinuitet vo raboteweto bankite treba da gi imaat predvid slednite celi:

- **planiraweto za kontinuitet slu`i za odr`uvawe, prodol`uvawe i restavracija na celiot bankarski proces, a ne samo za restavracija na tehnologijata;**

- **planiraweto za kontinuitet treba da bide na nivo na cela banka, a ne samo za informati~kiot del;**
- **temelna analiza na zakanite i procenka na rizicite se osnova za gradeweto na efektiven plan;**
- **efikasnosta na planot mo`e da se verificira samo so testirawe;**
- **planot i rezultatite od testot treba da bidat predmet na nezavisna kontrola i rezultatite treba da bidat razgledani od upravniot odbor;**
- **povremeno treba da se vr{at izmeni vo planot kako reakcija na nastanatite promeni vo bankata (netehni~ki ili tehni~ki).**

Vo razmisluvawata okolu planot za kontinuitet vo rabotewe, bankata treba da gi identifikuva site kriti~ni mesta za uspe{no izveduvawe na svoite operacii. Planot ne treba da se ograni~i samo na restavracija na informativnite sistemi i podatoci koi se vo elektronski format, bidej}i istite akcii ne mo`e sekoga{ da ja vratat bankata vo normalen tek za uspe{no izveduvawe na operaciite.

Otsustvoto na razvien plan za kontinuitet vo raboteweto zna~i deka bankata vo slu~aj na prekin nema da mo`e da gi uslu`i svoite komintenti na zadovolitelno nivo, odnosno deka informativniot sistem na bankata ne go zadovoluva standardot za raspolo`ivost na sistemot i ocenkata za celokupniot informativen sistem e NESIGUREN.

Bankite koi gi procesiraat svoite operacii preku obezbeduva~i na IT servisi treba da se osiguraat deka obezbeduva~ite na IT servisi imaat svoj sopstven plan za kontinuitet. Vo ovoj slu~aj bankata treba da go pravi svojot plan za kontinuitet vo koordinacija so planot na obezbeduva~ot i da vr{i zaedni~ko testirawe na nivnata funkcionalnost.

Upravniot odbor treba da vr{i promeni vo planot za kontinuitet vo raboteweto kako {to se menuva procesot na raboteweto vo bankata.

Planiraweto na kontinuitet vo rabotewe gi opfa}a slednite ~ekori po redosled:

1. Analiza na {tetite;
2. Procenka na rizikot;
3. Upravuvawe so rizikot;
4. Nabquduvawe.

5.1.Analiza na {tetite

Analizata na {tetite pretstavuva prviot ~ekor vo razvoj na PKR. Potrebnoto vreme za izveduvawe na ovoj ~ekor zavisi od goleminata i kompleksnosta na bankata. Analizata na {tetite treba da vklu~i:

- identifikacija na potencijalnata {teta od nekontrolirani nastani na bankarskite operacii;
- zemawe predvid na site bankarski operacii, a ne samo na operaciite koi se izveduvaat so pomo{ na informati~ka oprema;
- opredeluvawe na koeficient na maksimalno dozvoleno vreme na nefunkcionirawe na sistemot (**MTD-Maximum Tolerable Downtime**) i eventualnata finansiskata zaguba na bankata.

Ovaa faza gi identifikuva potencijalnite {teti od nekontrolirani nastani koi mo`e da se pojavat vo bankarskite procesi. Vo ovaa faza treba da se

identifikuvaat kriti~nite sistemi koi se potrebni za opstanok na bankata. Se vr{i procenka koe e maksimalno dozvolenoto vreme na nefunkcionirawe na sistemot vo slu~aj na mo`en te`ok prekin na delovnite procesi. Procenkata na maksimalno dozvolenoto vreme na nefunkcionirawe na sistemot mo`e da se dvi`i vo slednite granici:

vid na operacija		**MTD**
kriti~ni operacii	**=**	**minuti do ~asovi**
itni operacii	**=**	**24 ~asa**
va`ni operacii	**=**	**72 ~asa**
normalni operacii	**=**	**7 dena**
neva`ni operacii	**=**	**30 dena**

Ova rangirawe treba da se izvr{i spored mo`nite zagubi koi{to mo`e da gi pretrpi bankata dokolku se slu~i te`ok prekin na delovnite procesi. Na ovoj na~in, bankata }e sogleda koi se kriti~nite sistemi i operacii bez koi ne mo`e da opstane i kolku dolgo mo`e da go tolerira nivnoto nefunkcionirawe.

Rabotovodniot organ treba da opredeli prioriteti za restavrirawe, vo koi }e se identifikuvaat vitalnite objekti, tehnologii, komunikacii, podatoci i vraboteni koi se potrebni za prodol`uvawe na bankarskite operacii.

Pri odreduvawe na kriti~nosta na operacii vo odredena organizaciona edinica treba da se zeme vo predvid:

- Dali vo va{ata organizaciona edinica ima nekoja specijalizirana oprema i kako se koristi?
- Kako }e raboti va{ata organizaciona edinica, dokolku ne raboti glavniot server na podatoci, ili e vo prekin kompjuterskata mre`a?
- Kako zavisi va{ata organizaciona edinica od rabotata na drugi organizacioni edinici vo bankata ili od nadvore{ni treti lica?
- Dali postojat slabosti vo oddelot i koi se rizicite povrzani so toa?
- Dali za izvr{uvawe na kriti~nite operacii se potrebni obezbeduva~i na uslugi od oblasta na informativnata tehnologija?
- **Koj e minimalniot broj na vraboteni i kolkav prostor }e vi bide potreben na alternativnata lokacija? (organizacionata edinica da prodol`i so rabota na sekundarna lokacija)**
- Kakvi komunikaciski uredi }e bidat obezbedeni na alternativnata lokacija?
- Dali vrabotenite imaat trening i znaewe za izvr{uvawe na drugi zadol`enija vo va{ata organizaciona edinica?

5.2. Procenka na riziko t

Procenkata na rizikot e vtoriot ~ekor vo razvojot na PKR. Treba da vklu~i:

- Analiza na zakanite bazirani vrz mo`nata {tetata kon bankata;
- Davawe na prioriteti na mo`nite te{ki naru{uvawa na delovnite procesi, bazirani na te`inata na zakanata i frekvencijata na pojavuvawe;
- Komparativna analiza na postojnite PKR dokolku gi ima, za da se postigne o~ekuvanoto maksimalno dozvolenoto vreme na nefunkcionirawe na

sistemot, zemaj}i gi predvid testovite i nabquduvawata obraboteni vo poglavje 5.4. Nabquduvawe na rizicite i testirawe.

Bankite treba da razvijat realni scenarija koi mo`e potencijalno da gi prekinat procesite na bankata. Zakanite mo`e da bidat vo pove}e formi, vklu~uvaj}i aktivnosti od motivirani napa|a~i kako i od prirodni i tehni~ki katastrofi. Dokolku e mo`no, scenarijata treba pove}e da se zadr`at na analiza na {tetata, otkolku na prirodata na zakanata. Scenarijata treba da zemat vo predvid verojatnosta i frekvencijata na pojava na zakanata. Zakanite variraat od onie so visoka verojatnost na pojava i mala {teta (na pr.: prekini vo snabduvaweto so elektri~na energija), do onie so niska verojatnost na pojava me|utoa so golema {teta po bankata (na pr.: terorizam, grabe`i). PKR mora da ima fleksibilnost i da se obrabotat razli~nite tipovi na scenarija za da se opfatat site tipovi na scenarija. Pri analizata na ovie scenarija treba da se imaat predvid i geografskata lokacija na bankata i na alternativnata lokacija i zakanite od prirodnite sili (na pr.: poplavi, po`ari), blizinata do kriti~ni infrastrukturi (na pr. aerodrom, magistralni pati{ta, `eleznici).

Najte{koto scenario treba da vklu~i i zaguba na objekti i vraboteni.

Dokolku scenarijata se necelosni, toga{ i samite odgovori uniformirani vo PKR }e bidat neadekvatni.

5.3. Upravuvawe so rizik

Upravuvawe so rizikot podrazbira razvoj na pi{uvan PKR koj e na nivo na cela banka. Bankata treba da obezbedi PKR da e:

- so dovolna {irina za da mo`at da go implementiraat razli~ni grupi na vraboteni; (mo`e razvivawe na oddelni segmenti na planot koi }e im bidat dostapni na odredeni celni grupi na korisnici);
- da se navedat uslovite potrebni za implementacija na PKR;
- da se navedat koi promptni ~ekori treba da se prezemat vo slu~aj na pojava na odredeni prekini;
- fleksibilen za da reagira na nenadejni zakani i scenarija i interni promeni vo uslovite na raboteweto;
- fokusiranost na toa kako da se povratat procesite vo normala koga e vo prekin specifi~en objekt ili del;
- efikasnosta na planot vo minimizirawe na prekinite i namaluvawe na finasiskata zaguba.

Po fazata na analiza na {tetata i procenka na rizicite, rabotovodniot organ treba da go izraboti PKR. **Planot treba da gi dokumentira startegiite i procedurite za odr`uvawe, prodol`uvawe i sanacija na kriti~nite bankarski aktivnosti i procesi. Rabotovodniot organ treba im dade prioriteti na kriti~nite nasproti nekriti~nite servisi i procesi.** Dobriot PKR treba da gi opi{e tipovite na nastani koi mo`e da dovedat do formalna inicijalizacija na PKR (koj treba da objavi inicijalizacija na PKR). Treba da se navedat odgovornostite i procedurite koi treba da se sledat od sekoj tim i da gi sodr`i neophodnite kontakti na potrebnite lica za sproveduvawe na PKR. PKR treba detalno da gi opi{e procedurite koi treba da se

sledat za restavracija na aktivnostite na bankata i treba da bide pi{uvan na ednostaven na~in.

PKR treba da specificira koi ~ekori vo momentot treba da se prezemat za spre~uvawe na opasnosta koja mo`e da predizvika te`ok prekin na operaciite na bankata. PKR, isto taka, treba da gi predvidi aktivnostite koi treba da se prezemat za restavracija na operaciite, dokolku dojde do niven te`ok prekin. Specifi~nite scenarija treba da predvidat kako }e reagira bankata dokolku:

- klu~nite vraboteni ne se dostapni;
- kriti~nite objekti i zgradi ne se dostapni;
- nastane defekt na opremata (hardverska, telekomunikaciska);
- programite ili podatocite ne se dostapni ili se so gre{ka;
- poddr{kata od obezbeduva~ot na IT servisi e nedostapna;
- prekin na elektri~na energija i telekomunikacii;
- kriti~na dokumentacija ili podatoci ne se dostapni.

Bankite treba da predvidat deka nivnite objekti mo`e da bidat nedostapni ili te{ko o{teteni, a klu~nite lu|e (na primer: rabotovodniot organ na bankata) nema da bidat dostapni vedna{, po prekinot na operaciite.

Bankata mo`e da go poddr`i procesot na PKR so razvoj i na ostanati kontroli i planovi:

- obuka na vrabotenite i komunikacija na PKR niz bankata;
- sinhronizacija na podatocite na dvete lokacii i vr{ewe na za{tita podatoci (primarnata i alternativnata);
- sklu~uvawe na polisi za osiguruvawe.

5.4. Nabquduvawe na rizicite i testirawe

Nabquduvaweto na PKR pretstavuva kontinuiran proces. Efikasnosta na PKR treba da se osigura preku:

- testirawe na PKR najmalku edna{ godi{no;
- PKR i rezultatite da bidat razgleduvani od Slu`bata za vnatre{na revizija;
- vnesuvawe na promeni vo PKR bazirani vrz zabele`anite nedostatoci posle izvr{enite testovi ili promeni vo vrabotenite ili promenite vo funkcioniraweto na bankata.

Nabquduvaweto na rizikot e proces na testirawe na planot i vnesuvawe na periodi~ni izmeni i podobruvawa.

Pred zapo~nuvawe na testiraweto rabotovodniot organ treba da gi definira funkciite, sistemi i procesi }e bidat testirani i koi se celite koi saka da gi postigne. Rabotovodniot organ zatoa treba da pripremi **pi{an plan za test na PKR.** Celta na testiraweto e da se obezbedi deka PKR e to~en, relevanten i funkcionalen i pokraj **"te{kite okolnosti"** koi mo`e da predizvikaat te`ok prekin na delovnite procesi.

Vo testiraweto rabotovodniot organ treba da pristapi kon definirawe na celi koi }e gradiraat od poednostavni pa se do pokompleksni. Limitiranite ili individualnite testovi poleka da se pro{iruvaat na nivo na cela banka, a na kraj po`elno e i vklu~uvawe i so zaedni~ko testirawe so obezbeduva~i na IT servisi.

Pi{aniot plan za testirawe na PKR treba da ima predvid:

- Da ne go zagrozi normalnoto rabotewe na bankata;
- Da se zgolemuva sistematski kompleksnosta i brojot na vklu~eni vraboteni, funkcii i servisi;
- Otkrienite neadekvatnosti da bidat promenati i popraveni;

Za da ne se zagrozi normalnoto rabotewe na bankata, planot za test na PKR treba prethodno da bide revidiran pred da se testira.

Testiraweto na PKR bara centralizirana koordinacija od koordinator na PKR (OSIS) ili tim. Timot ili koordinatorot e odgovoren za ispolnuvawe na celite od testiraweto i za sledewe na rezultatite.

Nadzorot od strana na Slu`bata za vnatre{na revizija }e obezbedi validnost na procesot na testirawe i nezavisnost vo izvestuvawata do Upravniot odbor.

Uspe{en test }e bide onoj vo koj rezultatite od testot se analizirani i sporedeni so odnapred definirani celi vo Planot za test na PKR. Rabotovodniot organ treba da go izvesti Upravniot odbor za rezultatite od testot i za na~inot na koj }e gi re{ava nedostatocite.

Analizite od testot treba da vklu~at:

- ocenka dali se postignati celite na testot;
- ocenka na validnosta na validnosta na testiranite podatoci;
- korektivni akcii ili planovi {to }e se prezemat za da se nadminat problemite;
- predlo`eni promeni na PKR;
- preporaki za idni testovi na PKR.

Upravniot odbor treba da go revidira PKR najmalku edna{ godi{no. Bankata treba da go distribuira revidiraniot PKR do vrabotenite (oddelni segmenti na planot koi }e bidat dostapni na odredeni celni grupi na korisnici).

Slu`bata za vnatre{na revizija ili drugi kvalifikuvani nezavisni lica(nadvore{na revizija) treba da ja ocenat adekvatnosta na PKR i procesite za da se osigura deka nasokite i rezultatite koi mu se prezentirani na Upravniot odbor se to~ni. Slu`bata za vnatre{na revizija treba da se vklu~i vo analiza na sekoja faza i direktno da go nabquduva testiraweto na PKR i da dade izvestuvawe do Upravniot odbor za postignatite rezultati. Upravniot odbor treba vnimatelno da gi razgleda naodite od revizijata vo pogled na PKR i efikasnosta na celiot proces na PKR za da gi identifikuva slabostite vo procesot.

6.Upravuvawe so obezbeduva~ite na IT servisi

Bankite treba da vr{at nabquduvawe na kvalitetot na servisot i finansiskata situacija na nadvore{nata kompanija koja im ovozmo`uva izvr{uvawe na kriti~ni IT operacii. Kako Obezbeduva~i na servisi za bankite naj~esto se javuvaat kompanii, me|utoa mo`e da bidat i drugi finasiski ustanovi (primer: NBRM so sistemite za platen promet, KIBS, NPK, i dr.).

Bankite treba da obezbedat tekovna informacija od nivnite Obezbeduva~i na servisi za da mo`at da napravat celosna analiza na bonitetot i finansiskata situacija na svoite obezbeduva~i najmalku edna{ godi{no. Obvrskata za dostavuvawe na finasiskite izve{tai (po`elno e finasiskite izve{tai da se nezavisno revidirani) treba da bide del od obvrskite vo definirani vo dogovorot za sorabotka.

Dokolku obezbeduva~ot na IT servisi ne uspee da obezbedi finansiski izve{tai za svojata sostojba, bankata treba da ja proceni va`nosta na IT servisite {to im gi obezbeduva toj i da donese odluka dali }e go prodol`i dogovorot so istiot Obezbeduva~ na servisi ili }e sklu~i nov dogovor so drug obezbeduva~.

Rabotovodniot organ treba da izgotvi edinstveni principi i pravila za izbor na obezbeduva~i na IT servisi.

6.1. Dogovori so obezbeduva~ot na IT servisi

Bankite treba da napravat pismen dogovor koj treba da sodr`i i podatoci za:

- optimalnite performansi na servisot i negovata sigurnost i doverlivost;
- obvrskata za dostavuvawe na finansiski izve{tai;
- obvrskite koi treba da gi ispolni obezbeduva~ot na IT servisi, so cel bankata da bide usoglasena so propisite, politikite i procedurite za obezbeduvawe na informativnata sigurnost;
- liniite na komunikacija i izvestuvawe pome|u bankata i obezbeduva~ot na IT servisi.

6.2. Upravuvawe so obezbeduva~ot na IT servisi

Nemo`nosta na obezbeduva~ite na IT servisi da obezbedat kontinuiran servis, mo`e da ja izlo`i bankata na visok operativen rizik.

Bankite treba da gi definiraat uslovite za rabota so obezbeduva~ite na IT servisi preku:

- Definirawe na edinstveni principi na izbor na obezbeduva~i i sledewe na finasiskite izve{taii na svoite obezbeduva~i na IT servisi;
- Dogovorite pome|u bankata i obezbeduva~ot na IT servisi da imaat vgradeni za{titni mehanizmi za implementacija na politikata za informativna sigurnost;

- Obezbeduva~ite na IT servisi treba da rabotat vo soglasnost so odredeni standardi za sigurnost na informativniot sistem, za da mo`at bankite so koi rabotat tie da se usoglasat so standardite propi{ani od strana na Narodna Banka na Republika Makedonija. **Bankite treba da baraat od svoite Obezbeduva~i na IT servisi da imaat pravo za pristap do PKR i pristap do sigurnosnite politiki i proceduri koi va`at za organizacionata edinica kade se iznajmuva servisot za bankata.**
- Da se definira obvrska za neotkrivawe na informaciite i ~uvawe na bankarskata tajna i na soodvetnite lica od obezbeduva~ot na IT servisi koi imaat pristap do informativniot sistem na bankata (na pr.: licata koi imaat pristap od strana na obezbeduva~ na IT servisi treba da imaat **potpi{ana izjava za prifatlivo koristewe na informativniot sistem na bankata pred da im se dade pristap do sistemot na bankata**);
- Bankata treba da bara od svojot obezbeduva~ na IT servisi da vr{i nezavisni testirawa na sigurnosta od stru~ni timovi ili slu`bata na vnatre{na revizija da ima pristap do organizacionata edinica na obezbeduva~ot kade {to bankata go iznajmuva IT servisot;
- Bankata treba da reagira pri sigurnosni incidenti vo koordinacija so obezbeduva~ot na IT servisite dokolku bankata bila alarmirana preku sistemite za nabquduvawe deka incidentot doa|a od strana na obezbeduva~ot na IT servisi. Bankata treba da go prijavi incidentot vo NBRM, najdocna pet dena posle negovoto slu~uvawe;

Rabotovodniot organ e odgovoren za obezbeduvawe na sigurnost na informativniot sistem na bankata i soodvetna za{tita na podatocite, iako informacijata e procesirana, ~uvana ili transportirana preku obezbeduva~i na IT servisi.

Rabotovodniot organ treba da gi analizira soodvetnite informacii od svoite obezbeduva~i i da izgotvi dogovori, koi }e ovozmo`at postignuvawe na sigurnosnite standardi propi{ani od NBRM. **Bankite treba da baraat od nivnite obezbeduva~i na IT servisi da implementiraat adekvatni kontroli za da se za{titi doverlivosta, integritetot i raspolo`ivosta na informacijata koja se ~uva ili procesira preku niv. Rabotovodniot organ e odgovoren za kontinuirano sledewe na situacijata na obezbeduva~ot i izlo`enosta na rizicite na koi e izlo`en toj.**

So dogovorite, bankite treba da baraat od obezbeduva~ite na IT servisi da i obezbedat pristap na slu`bata za vnatre{na revizija na bankata do prostoriite na obezbeduva~ot, kako i do politikite i procedurite koi va`at za organizacionata edinica na obezbeduva~ot na IT servisi koj obezbeduva servis za bankata. **Kako alternativa obezbeduva~ot na IT servisi mo`e da izvr{i nezavisna revizija koja mo`e da ja dostavi do site finasiski institucii na koi im gi iznajmuva svoite servisi.**

Bankite treba da baraat od sopstvenite obezbeduva~ite na IT servisi da razvijat sopstveni PKR i koi{to treba da se vo koordinacija so PKR na bankata. Vo dogovorot so obezbeduva~ot treba da se definira i obvrskata za odr`uvawe i

odgovornostite na obezbeduva~ot za razvoj, implementacija i odr`uvawe na sopstven PKR i vzaemna koordinacija na razli~ni nivoa pome|u bankata i obezbeduva~ot. Bankata treba da gi dobiva rezultatite od izvr{enite testovi ili izvr{eni revizii na PKR za da napravi promeni vo sopstveniot PKR i da vospostavi poefektni procesi za testirawe. Dokolku e mo`no, Slu`bata na vnatre{na revizija na bankata treba da u~estvuva kako nabquduva~ vo testiraweto na PKR na obezbeduva~ot na IT servisi na bankata.Planot za PKR na bankata dokolku e zavisen od PKR na obezbeduva~ite na IT servisi treba da vklu~i i kontakti koi bankata }e mo`e da gi ostvari na primarnata i alternativnata lokacija na obezbeduva~ot na IT servisi.

6.3. Dogovori za odr`uvawe na informativniot sistem

Dokolku poddr{kata na sistemot ne mo`e da se obezbedi preku lokalna ekspertiza vo samata banka ili ne mo`e da odgovori na delovnite barawa na odredeni organizacioni edinici (na pr.:minimalno vreme na odziv od momentot na nastanuvawe na problemot), toga{ bankata treba da sklu~i dogovor za odr`uvawe na sistemot so renomirana kompanija so sedi{te vo RM.

Vo dogovorite so obezbeduva~ite treba da se definira koi se sigurnosnite barawa na bankata (proizleguvaat od politikata na informativna sigurnost) i koi se barawata na bankata vo pogled na efikasno izveduvawe na nejzinite operacii.

Bankata mo`e da sklu~i dogovor za odr`uvawe so renomirana me|unarodna kompanija koja e nadvor od RM, me|utoa treba da obezbedi siguren elektronski na~in[3] na povrzuvawe i teledijagnostika na problemite i efekten na~in na nivno re{avawe. **Dokolku poddr{kata na sistemot ne mo`e da se realizira efikasno i sigurno preku elektronska vrska so bankata, obezbeduva~ot koj se izbira za IT odr`uvawe na sistemot koi se od redot na renomirani firmi, MORA da ima sedi{te ili pretstavni{tvo vo RM.**

Renomirana kompanija vo pogled na odr`uvawe na sistemot mora da poseduva i go zadovoluva standardot za kvalitet i kontrola na kvalitetot, a intervenciite da bidat izvr{uvani od soodvetno {koluvani i sertificirani lica koi se vraboteni vo kompanijata.

7. Utvrduvawe na dinamika na implementacija

Bankite treba da imaat sistematski pristap vo gradeweto i implementacijata na programot za sigurnost na informativniot sistem. Sistematskiot pristap bara odewe po odnapred dogovoreni ~ekori i dvi`ewe vo odredeni vremenski rokovi. Gradeweto i implementacijata na ovaa materija, koja vo na{ite banki e novitet, }e pretstavuva predizvik za vospostavuvawe moderna banka podgotvena da se soo~i so upravuvawe na operativniot rizik soglasno so bazelskite supervizorski standardi.

---

[3] Bankata sama treba da go definira sigurniot elektronski na~in na povrzuvawe, soglasno sopstvenata politika za informativna sigurnost i napravenata analiza na rizici po informativniot sistem. Primer: Kako poseben del od politikata za informativna sigurnost mo`e da bide Politika za dale~inski pristap do informativniot sistem na bankata. Taa politika treba da bide poddr`ana od sigurnosni standardi koi }e se upotrebuvaat za dale~insko povrzuvawe, proceduri i upatstva za uspe{no povrzuvawe so bankata

Po~etnata obvrska na site banki e da nazna~at OSIS. OSIS treba da bidat lica so poznavawe na tehnologijata na bankata, poznavawe na site proceduri i upatstva koi va`at vo bankata i soodvetnata zakonskata regulativa. **Bankite treba{e da nazna~at OSIS zaklu~no so dekemvri 2004 godina soglasno so to~ka 22 od_Odlukata za definirawe na standardite za izgotvuvawe i sproveduvawe na sigurnosta na informativniot sistem.**

Vo narednata faza treba da se napravi po~etniot ~ekor vo implementacija na politikata, a toa e op{ta i celosna **ANALIZA i OCENKA na RIZICITE na informativniot sistem na bankata**. Ovaa materija treba da gi opfati site mo`ni scenarija po sredstvata na informativniot sistem na bankata. (**avgust/septemvri 2005**).

Vrz baza na ovaa sprovedena analiza na rizicite, bankata treba da vospostavi adekvatni politiki, standardi, upatstva i soodvetni proceduri za da se kompletira programata za sigurnost na informativniot sistem (noemvri 2005).

Celokupniot materijal na sprovedenata analiza i ocenka na rizicite, formalnata politikata za sigurnost na informativniot sistem i adekvatnite ostanati politiki, standardi, upatstva i proceduri da se dostavat za soglasnost vo NBRM zaklu~no so noemvri 2005 godina.

Bankata treba da izvr{i **dopolnuvawe na me|usebnite dogovori** so obezbeduva~ite na IT servisi (outsourcing kompanii) zaklu~no so **noemvri 2005 godina**, a soglasno so sopstvenata politika za sigurnost na informativniot sistem.

Za da vospostavi dobar Plan za kontinuitet vo raboteweto, bankata treba da izvr{i analiza i procenka koi operacii se potrebni za opstanok na bankata i koi }e bidat potrebni pri nastanuvawe na te`ok prekin na delovnite procesi na primarnata lokacija.

Bankata treba da ima sekundarna lokacija koja treba da bide adekvatno oddale~ena. Adekvatnata oddale~enost na sekundarnata lokacija na bankata treba da se dobie od izvr{enata analiza na rizici i pritoa da se zeme predvid istata zakana da ne predizvika nefunkcionalnost i prekin na dvete lokacii. Vo prviot ~ekor se podrazbira sproveduvawe na analiza na rizici i dodeluvawe prioritet od strana na rabotovodniot organ, kako i planirawe na maksimalno dozvoleno vreme odredeni organizaciski delovi na bankata da bidat nefunkcionalni. Ovaa analiza da bide zavr{ena do **avgust/septemvri 2005 godina**.

Nareden ~ekor e re{avawe na infrastrukturnoto pra{awe vo odnos na sekundarnata lokacija na bankata.

Prepor~livo e ovaa oddale~enost da bide najmalku 30 km od primarnata lokacija. Ovaa lokacija treba da bide na adekvatna dale~ina i potrebno e taa da poseduva dobra fizi~ka za{tita.

Sekundarnata lokacija na bankata ne mora da bide vo posed na bankata, tuku ovie uslugi mo`e i da se iznajmuvaat od adekvaten obezbeduva~ na IT servisi (outsourcing kompanii). Za bankata e va`no da ima **mo`nosti nepre~eno da vr{i testirawe** na PKR, kako i pri slu~aj na te`ok prekin na delovnite procesi da mo`e da se prefrli vo izbranata lokacija i da gi restavrira vo najkus mo`en rok svoite operacii. Planot za kontinuitet vo raboteweto soglasno so infrastrukturnite re{enija na bankata, soodvetnite timovi i politiki, proceduri, upatstva vo pogled na ova pra{awe treba da bidat zavr{eni do **noemvri 2005 godina** i da se dostavat zaedno so materijalot za politikata za informativna sigurnost za dobivawe na soglasnost vo NBRM.

Bankite se dol`ni da gi testiraat na implementiranite kontroli vrz osnova na obezbeduvawe na sigurnost na informativniot sistem. Testiraweto na kontrolite zna~i **REVIZIJA**. Bankite treba da vr{at redovno testirawe na funkcionalnosta na implementiranite kontroli za sigurnost na informativniot sistem, testirawe i revizija na svoite obezbeduva~i na IT servisi i testirawe i revizija na Planot za kontinuitet vo raboteweto najmalku edna{ godi{no.

DIREKCIJA ZA SUPERVIZIJA

Direktor

Igor Davkov

Aneks 1: Primer za adekvaten najvisok akt na piramidata (slika2) na procesot na informativna sigurnost

POLITIKA ZA SIGURNOST NA INFORMATIVNITE SISTEMI

Cel

Celta na sigurnosta na informativnata sigurnost e obezbeduvawe kontinuitet vo raboteweto i minimizirawe na {tetite predizvikani od mo`ni sigurnosni incidenti.

Sodr`ina

- Celta na ovaa politika e za{tita na informativnite sredstva na bankata od site vidovi na zakani bilo da se namerni ili nenamerni, ili od nadvore{na priroda ili vnatre{na.
- Menaxmentot na bankata ja odobri ovaa politika.
- Ovaa politika treba da obezbedi:
  - za{tita na informacijata od neavtoriziran pristap;
  - obezbeduvawe na doverlivosta na informacijata;
  - odr`uvawe na integritetot na podatocite;
  - odr`uvawe na raspolo`ivosta na informaciite;
  - usoglasenost so regulatornite organi;
  - odr`uvawe na planovite za kontinuitet vo raboteweto i sanacija od katastrofa;
  - obukata za odr`uvawe siguren informativen sistem }e bide dostapna im bide dostapna na site vraboteni
  - site naru{uvawa na sigurnosta na informativniot sistem }e bidat prijaveni i analizirani od strana na OSIS

- Postojat detalni proceduri, standardi i upatstva koi ja poddr`uvaat navedenata politika za sigurnost na informativniot sistem i se nejzin sostaven del. (Navedete gi koi se tie!)
- OSIS ima direktna odgovornost za odr`uvawe na politikata za sigurnost na informativniot sistem i davawe na nasoki vo nejzinata implementacija.
- Site direktori se odgovorni vo ramkite na nivnite direkcii za implementacija na politikata i pridr`uvawe na nivnite vraboteni kon nea
- Sekoj vraboten vo bankata e odgoveren sprema ovaa politika za obezbeduvawe siguren informativen sistem.

...itn

Aneks 2: Prijava za sigurnosniot incident (da se isprati vo NBRM)

PRIJAVA NA NARU[UVAWA NA SIGURNOSTA NA INFORMATIVNIOT SISTEM VO BANKA	
IME NA BANKATA	**DIREKCIJA VO BANKATA**

datum na nastanot	vreme na nastanot
datum na otkrivawe na nastanot	vreme na otkrivawe na nastanot
kratok opis na nastanot	

Naru{ena sigurnost na informativniot sistem preku naru{uvawe na:	
DOVERLIVOSTA na informativniot sistem	☐
INTEGRITETOT na informativniot sistem	☐
RASPOLO@IVOSTA na informativniot sistem	☐

Tip na sigurnosen incident:		**Koristen medium za predizvikuvawe na sigurnosniot incident**	
NEAVTORIZIRAN PRISTAP DO INFORMATIVNIOT SISTEM	☐	KOMPJUTER	☐
KRA@BA NA SREDSTVO NA INFORMATIVNIOT SISTEM	☐	ELEKTRONSKA PO[TA	☐
NARU[ENA FIZI^KA SIGURNOST	☐	INTERNET	☐
GRE[KA VO APLIKACII (SOFTVER)	☐	TEL./FAKS	☐
SISTEMSKI GRE[KI (SERVERI)	☐	**Sigurnosniot incident e predizvikan od:**	
GRE[KI VO TO^NOSTA NA PODATOCITE ILI GRE[KI VO OBRABOTKATA NA TRANSAKCIITE	☐	TRETI LICA (Vo RM ili nadvor od RM)	☐
PREKINI VO TELEKOMUNIKACII	☐	VRABOTENI	☐
PREKINI NA SERVISOT NA DOBAVUVA^OT NA IT SERVISI	☐	KOMINTENTI	☐
PREKINI NA EL. ENERGIJA	☐	DOBAVUVA^I NA IT SERVISI	☐
NARU[ENI AVTORSKI PRAVA	☐	DRUGO:	
DRUGO:			

Rabotovoden organ na BANKATA:	**DATUM:**