

Departman za postdiplomske studije

SAVREMENE INFORMACIONE TEHNOLOGIJE

MASTER STUDIJE

– Master rad –

**Standardi za upravljanje informacionim sistemima finansijskih
institucija**

Mentor
Prof. dr Milan Milosavljević

Kandidat
Darko Šehović 410578/2012

Sažetak

U današnje vreme finansijske institucije su među vodećim igračima na polju informacionih tehnologija. Veliki obrt novca omogućio im je pristup sofisticiranim sistemima, a uska povezanost, ako ne i totalna zavisnost od tehnologije za obavljanje primarne delatnosti ovih institucija, učinila je da budu izložene najrazličitijim rizicima. Trend konstantnog i eksponencijalnog rasta količine podataka i broja operacija koje ovakvi sistemi izvršavaju rešava se nabavkama novih sve bržih i složenijih tehnologija. Ovim se problem trenutno rešava, ali se s druge strane otvaraju nova pitanja i izazovi.

Da li je sistem spreman da upravlja na adekvatan način novim tehnologijama, da li je period upoznavanja sa njima adekvatan, da li su sagledani novi sigurnosni rizici koji se neminovno pojavljuju usložnjavanjem ovih sistema? Da li potreba za progresom i brzina širenja sistema nadjačava i narušava osnovna pravila i postulate stabilnosti i bezbednosti informacionih sistema?

Ovaj rad daje pregled i analizu odluke Narodne banke Srbije *O minimalnim standardima upravljanja informacionim sistemom finansijske institucije* koja pokušava da ovaj problem reši smernicama i uputima u ovom dokumentu.

Abstract

At present time financial institutions are among leaders in information technology field. Huge amount of money allow them access to sophisticated technology and tight connection of even addiction to technology exposes them to great risks. Big data trend and complexity of operations usually is solved with new hardware but that only solve problem in first place and open other questions and challenges.

Is system ready to use new technology are we familiar with them enough, is new risk detected and is appropriate countermeasures in use. Is progress and expansion of financial systems avoid postulate and basics of information system security.

This paper will try to analyse document „Minimal standards of information systems in financial institutions“ that National bank of Serbia is bring to public as a set of recommendations and instructions with intention to help standardize this important segment.

Sadržaj

1. Metodologija istraživačkog rada	1
1.1 Uvodne napomene	1
1.2 Predmet istraživanja	1
1.3 Hipotetički okvir	1
1.4 Ciljevi istraživanja	1
1.5 Metode istraživanja i tok istraživačkog procesa	2
2. Uvod	3
3. Dokument o minimalnim standardima	5
3.1 Nastanak dokumenta	5
3.2 Okvir za upravljanje informacionim sisitemima	5
3.3 Upravljanje rizikom informacionog sistema	5
3.4 Unutrašnja revizija informacionog sistema	6
3.5 Bezbednost informacionog sistema.....	6
3.6 Upravljanje kontinuitetom poslovanja i oporavak aktivnosti u slučaju katastrofa	7
3.7 Razvoj i održavanje informacionog sistema	9
3.8 Poveravanje aktivnosti u vezi sa informacionim sistemom trećim licima	10
3.9 Elektronsko bankarstvo	12
4. Analiza odluke.....	13
4.1 Okvir za upravljanjem IS	13
4.2 Upravljenje rizikom informacionog sistema	15
4.3 Unutrašnja revizija informacionog sistema	16
4.4. bezbednost informacionog sistema	17
4.5 Upravljanje kontinuitetom poslovanja i oporavak aktivnosti u slučaju katastrofa	21
4.6. Razvoj i održavanje informacionog sistema	23
4.7 Poveravanje aktivnosti u vezi sa informacionim sistemom trećim licima	25
4.8 Elektronsko bankarstvo	27
5. Međunarodni standardi i iskustva.....	28
5.1 O standardima.....	28
5.2 CobiT.....	29

5.3	ISO 38500.....	30
5.4	ITIL	30
5.5	ISO 20000 standard	31
5.6	ISO 2700x standardi	32
5.7	ISO 22301 standard	33
5.8	ISO 27013 standard	33
5.9	Bazel 2	34
5.10	Bazel 3	35
5.11	Međunarodna iskustva	35
6.	Zaključak	36
7.	Literatura.....	38
Prilog 1. Tabela akcija potrebnih za usklađivanje sa Odlukom NBS.....		40

1. Metodologija istraživačkog rada

1.1 Uvodne napomene

Istraživanje sprovedeno tokom pisanja ovog rada pokazalo je da je inicijalnim dokumentom Narodne banke Srbije obuhvaćen veliki broj oblasti koje u sebi sadrže savete i uputstva za upravljanje, održavanje i osiguravanje informacionih sistema. Kako su ova dokumenta pisana generički i većinom za što širu ciljnu grupu, sami korisnici ovih uputa moraju da urade detaljne analize svojih informacionih sistema i izvrše prilagođavanja sa pomenutim standardima.

Rad se može koristiti kao prvi nivo dekompozicije dokumenta koji donosi NBS i koji im može poslužiti za bolje sagledavanje pred njih stavljenih zahteva.

1.2 Predmet istraživanja

Predmet istraživanja su analize svetskih standarda i uputstava, kao i dobre prakse, a u cilju usklađivanja sa zahtevima iz dokumenta NBS.

1.3 Hipotetički okvir

Generalna ili opšta hipoteza: Definisanje standarda za upravljanje informacionim sistemima trebalo bi da omogući svim finansijskim institucijama kvalitetno, efikasno i bezbedno upravljanje informacionim sistemima.

Posebna ili radna hipoteza: U većini sistema prirodno se teži uređivanju istih i stavljanju pod neki vid kontrole, ali se do toga često stiže vremenom, iskustvom i iteracijom pokušaja. Uz pomoć dobro definisanih standarda ovakav posao može se značajno olakšati i učiniti što definisanijim.

Pojedinačna hipoteza: Dobro definisani standardi sadrže uputstva koja omogućavaju postizanje konkretnih rezultata vršenjem konkretnih akcija u delovima sistema koji se uređuju.

1.4 Ciljevi istraživanja

Naučni cilj ovog istraživanja je analiza i razumevanje dokumenta NBS kojim se pokušava definisati minimalni standard za upravljanje informacionim sistemima finansijskih institucija.

Konkretni cilj ovog istraživanja je definisanje konkretnih standarda i uputstava, kao i oblasti u kojima se oni moraju primeniti kako bi se postigli što bolji rezultati pri upravljanju samim sistemima.

1.5 Metode istraživanja i tok istraživačkog procesa

Osnovne metode: Za potrebe istraživanja izvršene su analize svetskih standarda koji se bave konkretnom problematikom i pokušano je da se one razlože u detaljnije upute u odnosu na ono što čini dokument NBS.

Statističke metode: Korišćeni su statistički podaci objavljeni na sajtu banaka, Narodne banke, Udruženja banaka Srbije i svi drugi materijali do kojih je autor mogao da dođe.

Eksperiment: U cilju potpunog razumevanja strukture standarda biće navođeni konkretni primeri sa vrednostima koje se zahtevaju u standardima.

Tok istraživačkog procesa: Najpre je sprovedena analiza dokumenta *Odluka o minimalnim standardima upravljanja informacionim sistemima finansijske institucije*. Objašnjena su značenja svih tačaka u ovom dokumentu. Potom je izvršena analiza tržišta postojećih standarda na koje se dokument indirektno poziva i onih koji se bave sličnom problematikom, konsultovani su i drugi vodeći svetski izvori. Nakon te analize date su preporuke, primeri i putokazi u kom pravcu se može krenuti da bi se odgovarajući standardi ispunili.

2. Uvod

Ključna uloga finansijskih institucija u savremenom poslovanju daje ovim sistemima na važnosti u društvu, a njihova zavisnost od informacionih sistema prebacuje ih u sferu koja je sasvim drugačija od sfere finansija i finansijskih poslova. Ubačeni u zonu informacionih tehnologija i neraskidivo povezani s njom, finansijske institucije i njihovo rukovodstvo našlo se pred velikim izazovima. Kako sagledati i obuhvatiti sve rizike koje ovo okruženje sobom nosi, kako adekvatno na njih odgovoriti, kako obezbediti kontinuiran i stabilan rad sistema, a pri tome zadržati adekvatan nivo bezbednosti? Brzina kojom se promene na polju tehnologija odigravaju zapanjujuća je i pred banke stalno stavlja nove zahteve za inovacijama. Kompetitivno društvo i tržišna utakmica drastično smanjuju vreme od zahteva do trenutka puštanja nove usluge u promet, što donosi nove izazove pri analizi i upravljanju rizicima. Okruženje u kome posluju ove institucije (internet, međudržavna saradnja...) izuzetno je promenljiva sredina koja zahteva konstantan monitoring i prilagođavanje, težnja sistema jeste stalna dostupnost finansijskih servisa, njihove odgovarajuće performanse i sigurnost informacija koje se u njima nalaze, što je moguće postići samo uz kompleksnu informacionu strukturu koja svojom kompleksnošću nosi i ne mali broj rizika za dati sistem.

Dosadašnja iskustva pokazala su da su informacioni sistemi finansijskih institucija iako vrlo moderni i napredni, takođe skloni uobičajenim rizicima u radu. Posledice problema u radu informacionih sistema povlače različite kategorije rizika kao što su rizik od sankcija regulatornog tela, rizik od finansijskog gubitka, reputacioni rizik i drugo. Vođen osnovnim principima sigurnosti – poverljivošću, integritetom i dostupnošću – ovaj dokument Narodne banke Srbije pokušava da obezbedi ove elementa u okviru informacionih sistema finansijskih institucija i da iste uredi donošenjem minimalnog seta standarda za njihovo upravljanje. Dokument takođe naglašava značaj upravljanja rizikom informacionih sistema finansijskih institucija kao bitnim segmentom za njihov rad.

U ovom dokumentu daju se smernica koje treba da služe kao polazna osnova za uspostavljanje kvalitetnog, bezbednog i pouzdanog informacionog sistema koji je redovno nadziran, kontrolisan i unapređivan kako bi se zadržale i unapredile njegove početne osobine. Donošenje dokumenta o minimalnim standardima Narodna banka je stavila konkretne zadatke pred finansijske institucije i primorala ih da svoja poslovanja u domenu informacionih tehnologija podvrgnu detaljnoj analizi i kao krajnji cilj dovedu u stanje koje im daje veće šanse za kontrolisano i uređeno funkcionisanje. U ovom radu vrši se dekompozicija Odluke i daje njena analiza po svim ključnim tačkama. U poglavlju tri izvršeno je predstavljanje dokumenta o minimalnim standardima u finansijskim NBS u celosti i sa ukazivanjem na konkretne akcije koje proizilaze iz konkretnih zahteva. U poglavlju četiri vrši se analiza zahteva iz Odluke NBS i pokušava da se ukaže na moguće načine usklađivanja sa njima. U petom poglavlju dat je pregled međunarodnih standarda sa

kojima se može konsultovati u cilju usklađivanja sa Odlukom NBS i na koje se dokument NBS indirektno oslanja u svojim zahtevima. U prilogu je data tabela akcija potrebnih za usklađivanja sa odlukom NBS koja ima za cilj da olakša sagledavanje potrebnih zadataka i u kratkim crtama ukaže na potrebne standarde, tehnologije ili proizvode koji mogu da pomognu pri ovom zadatku.

3. Dokument o minimalnim standardima

3.1 Nastanak dokumenta

Nastanku dokumenta *Odluka o minimalnim standardima upravljanja informacionim sistemima finansijske institucije*[1] (u daljem tekstu odluka NBS) prethodio je nacrt ovog dokumenta definisan sredinom 2012. godine da bi se konačno pojavio u finalnoj verziji u Službenom glasniku br. 23/2013.

Dokumentom se utvrđuju minimalni standardi i uslovi stabilnog i sigurnog poslovanja koji se odnose na upravljanje informacionim sistemima u finansijskim institucijama, tj. u bankama, **društvima za osiguranje**, davaocima finansijskog lizinga i **društvima za osiguranje**.

U uvodnim odredbama definiše se 37 pojmova koji se tiču date materije.

3.2 Okvir za upravljanje informacionim sistemima

U ovom delu dokumenta NBS definišu se smernice koje imaju za cilj uspostavljanje funkcionalnog, skalabilnog i sveobuhvatnog informacionog sistema finansijskih institucija. U dokumentu se takođe ukazuje na potrebu uspostavljanja programa upravljanja informacionim sistemom, a radi smanjenja izloženosti rizicima i očuvanja bezbednosti. Ukazuje se i na obavezu definisanja strategije razvoja informacionog sistema.

Organizaciona struktura stavlja se u prvi plan kao neophodan mehanizam za uspostavljanje adekvatnog upravljanja informacionim sistemom.

Kao obrazac za uspostavljanje i održavanje upravljanja informacionim sistemom pred finansijske institucije stavlja se zahtev da se usvoji odgovarajuća metodologija upravljanja projektima.

Takođe se uvodi potreba definisanja načina izveštavanja nadležnih organa o relevantnim činjenicama u vezi sa funkcionalnošću i bezbednošću informacionog sistema.

3.3 Upravljanje rizikom informacionog sistema

Shodno ostalim propisima kojima se uređuje upravljanje rizicima u poslovanju finansijskih institucija, tretiraju se i rizici koji nastaju prilikom upravljanja informacionim sistemom. Finansijskim institucijama se nalaže da uspostave proces upravljanja rizikom informacionog sistema koji obuhvata identifikovanje merenje, procenu, ublažavanje, praćenje i kontrolu rizika.

Upravljanje rizikom ne bi smelo da utiče na upravljanje bezbednošću i upravljanje kontinuitetom poslovanja finansijske institucije.

Upravljanje rizikom informacionog sistema mora da obuhvati celokupan informacioni sistem finansijske institucije.

Posebna pažnja usmerava se na upravljanje rizicima koji nastaju iz ugovornih obaveza sa pravnim i fizičkim licima čije aktivnosti se odnose na informacioni sistem finansijske institucije.

3.4 Unutrašnja revizija informacionog sistema

Obaveza je finansijske institucije, tj. unutrašnje revizije date institucije da obuhvati kriterijume, način i postupke unutrašnje revizije na osnovu rezultata procene rizika, kao i da poštuje propise kojima se uređuje poslovanje finansijskih institucija.

3.5 Bezbednost informacionog sistema

Deo koji se tiče bezbednosti informacionih sistema posebno je detaljno obrađen i donosi devet tačaka u kojima se definiše sledeće:

Potreba da finansijska institucija definiše akt politike bezbednosti informacionog sistema kroz koji će definisati principe, načine i procedure postizanja željenog nivoa bezbednosti, kao i ovlašćenja i odgovornosti.

Dužnost je finansijske institucije da politiku bezbednosti usklađuje sa promenama u okruženju i u samom informacionom sistemu.

Proces upravljanja bezbednošću mora biti kontinuiran proces.

Ogrанизacije su u obavezi da prate potrebe za bezbednošću na osnovu rezultata procene rizika, obaveza koje proizilaze iz propisa, unutrašnjih opštih akata, ugovornih odnosa i slično.

Uspostavljanje odgovarajućih kontrola u cilju održavanja željenog nivoa bezbednosti je neophodno.

Finansijska institucija je dužna da uspostavi klasifikaciju informacionih dobara po stepenu osetljivosti i kritičnosti, kao i da u skladu sa tim stepenom štiti ova dobra.

Finansijska institucija je dužna da imenuje lice, odnosno lica zaposlena u toj instituciji koja će biti odgovorna za upravljanje, zaštitu i klasifikaciju ovih dobara.

Potrebno je uvesti u praksu kontrolu pristupa resursima informacionog sistema; ovim sistemom potrebno je obuhvatiti sledeće procese: evidentiranje korisnika informacionog sistema, autorizaciju, identifikaciju, autentifikaciju i nadzor nad pravima korisničkog pristupa.

Poštovanje principa najmanjih mogućih privilegija za prava pristupa.

Prava pristupa potrebno je revidirati minimum jednom godišnje.

Posebna kategorija prava pristupa koja zahteva izdvojen tretman su udaljeni i privilegovani pristup informacionom sistemu.

Finansijska institucija je dužna da uspostavi sistem nadgledanja sistema i generisanje operativnih i sistemskih zapisa, a na osnovu procene rizika informacionog sistema. Sami

zapisi moraju imati dovoljno informacija za identifikovanje potencijalnih problema, otkrivanje neovlašćenog pristupa i rekonstrukciju događaja. Za ove zapise institucija mora da ustanovi vreme i način čuvanja, kao i opseg i način analiziranja istih.

Finansijska institucija je dužna da zaštiti sistem od neovlašćenog fizičkog pristupa, krađe, uništavanja podataka i drugih oštećenja ili uništenja izazvanih ljudskim ili prirodnim faktorom.

Finansijska institucija je dužna da uvođenjem odogovarajućih mera informacioni sistem zaštiti od malicioznog programskog koda.

3.6 Upravljanje kontinuitetom poslovanja i oporavak aktivnosti u slučaju katastrofa

Posebno bitan deo u celokupnom sistemu zaštite sistema i njegove funkcije predstavlja obezbeđivanje kontinuiteta poslovanja sistema i oporavak u slučaju katastrofa.

Imajući u vidu važnost ovakvih sistema kako za poslovanje kompanija, tako i za njegove korisnike, ovaj segment zaštite posebno je bitan za stabilnost i sigurnost sistema.

Finansijska institucija je dužna da ovakav sistem uspostavi na osnovu analiza i procena rizika. Posebnu pažnju treba obratiti na utvrđivanje resursa potrebnih za obavljanje kritičnih poslovnih procesa, procenu rizika u vezi sa detektovanim procesima, utvrđivanje prihvatljivog nivoa rizika i utvrđivanje prihvatljivog prekida procesa (MAO).

Kada organizacija formira strategiju oporavka, potrebno je da istu usvoji i uvede u redovne procedure kompanije. Sama strategija mora da sadrži sledeće elemente: prioritet oporavka poslovnih procesa, ciljane nivoa aktivnosti (SDO), ciljana vremena oporavka (RTO), ciljane tačke oporavka (RPO).

I plan kontinuiteta i plan oporavka aktivnosti u slučaju katastrofe moraju usvojiti odgovarajuća tela u institucijama (Upravni odbor ili nadležni odbor) kako bi se oni smatrali obavezujućim i kako bi se obezbedili potrebni resursi za njihovo uvođenje i sprovođenje.

Plan kontinuiteta poslovanja naročito sadrži:

1. opis procedura u slučaju prekida poslovanja;
2. ažuran spisak svih resursa neophodnih za ponovno uspostavljanje kontinuiteta poslovanja;
3. podatke o timovima koji će biti odgovorni za ponovno uspostavljanje poslovanja u slučaju nastanka nepredviđenih događaja i o imenovanim članovima tih timova, uključujući i njihove jasno utvrđene dužnosti i odgovornosti, kao i plan unutrašnjih i spoljnjih linija komunikacije;
4. rezervnu lokaciju – u slučaju prekida poslovanja i nemogućnosti ponovnog uspostavljanja poslovnih procesa na primarnoj lokaciji.

Plan oporavka aktivnosti u slučaju katastrofa naročito sadrži:

1. procedure za oporavak informacionog sistema kad nastupe katastrofalni događaji;
2. prioritete oporavka resursa informacionog sistema;
3. podatke o timovima koji će biti odgovorni za oporavak informacionog sistema i o imenovanim članovima tih timova, uključujući i njihove jasno utvrđene dužnosti i odgovornosti;
4. rezervnu lokaciju za oporavak informacionog sistema, odnosno lokaciju rezervnog računskog centra.

Svi zaposleni u instituciji moraju biti upoznati sa planom, tj. sa svojim ulogama u njemu i odgovornostima koje iz njih slede.

Finansijska institucija je dužna da najmanje jednom godišnje i posle značajnih promena testira procedure za oporavak.

Finansijska institucija je dužna da u upravljanju kontinuitetom uzme u obzir i aktivnosti poverene trećim licima i zavisnosti nastale od usluga tih lica.

U slučaju nastanka okolnosti koje zahtevaju promenu plana kontinuiteta poslovanja i plana oporavka aktivnosti **u slučaju katastrofe**, finansijska institucija je dužna da o tome obavesti Narodnu banku Srbije najkasnije narednog dana.

Finansijska institucija je dužna da uspostavi mehanizam upravljanja incidentima kako bi omogućila efikasnu i blagovremenu reakciju na eventualno nastale incidente, takođe o nastalim težim incidentima finansijska institucija je dužna da o tome obavesti Narodnu banku Srbije najkasnije narednog dana.

Finansijska institucija je dužna da obezbedi proces upravljanja rezervnim kopijama podataka (detaljne procedure i definisanje odgovornosti). Upravljanje rezervnim kopijama podrazumeva postupke izrade, čuvanja i testiranja kopija, kao i oporavka podataka i softverskih komponenti a u cilju uspostavljanja poslovnih procesa u okviru definisanog ciljnog vremena oporavka (RTO). Same rezervne kopije podataka moraju biti ažurne, adekvatno zaštićene, a procedure za njihovo korišćenje proverene i redovno testirane.

Minimalno jedna kopija rezervnih podataka mora se nalaziti na udaljenoj lokaciji koja procenom rizika ne podleže uticaju istih rizika kao i primarna lokacija.

Finansijska institucija je dužna da obezbedi adekvatan rezervni računski centar i njegovu odgovarajuću udaljenost na lokaciji koja procenom rizika ne podleže uticaju istih rizika kao i primarna lokacija.

3.7 Razvoj i održavanje informacionog sistema

Finansijska institucija je dužna da uspostavi proces razvoja informacionog sistema sa ciljem adekvatnosti datog sistema. Ovaj proces se sprovodi u skladu sa usvojenom strategijom razvoja informacionog sistema i metodologijom upravljanja projektima, uz poštovanje funkcionalnih zahteva i zahteva za bezbednošću.

Proces razvoja informacionog sistema mora se dokumentovati u smislu analize, projektovanja, programiranja, testiranja i uvođenja u produkciju.

Finansijska institucija je dužna da adekvatno razdvoji razvojno, testno i produkcijsko okruženje.

Finansijska institucija je dužna da uspostavi proces upravljanja hardverskim i softverskim komponentama i to u svim fazama njihovog životnog ciklusa. Upravljanje ovim resursima podrazumeva period od nabavke ili razvoja do povlačenja iz upotrebe. U cilju što efikasnijeg upravljanja finansijska institucija je dužna da obezbedi detaljne i ažurne evidencije ovih komponenti, kao i da imenuje zaposlene odgovorne za upravljanje i zaštitu, utvrđivanje pravilnog rukovanja opremom, kao i njenim bezbednim uklanjanjem iz upotrebe.

Finansijska institucija je dužna da hardverske i softverske komponente adekvatno održava prema preporukama proizvođača i da o tom održavanju čuva urednu dokumentaciju, a da pri tome ne ugrozi bezbednost ili funkcionalnost sistema.

Upravljanje promenama softverskih komponenti posebno je naglašena i naročito obuhvata sledeće postupke:

1. utvrđivanje početnih verzija ovih komponentata;
2. iniciranje, analiza i odobravanje zahteva za promenom;
3. hronološko dokumentovanje svih promena ovih komponentata i arhitekture baza podataka, zajedno s vremenom nastanka promene;
4. informisanje korisnika informacionog sistema o detaljima izvršenih promena.

Finansijska institucija je dužna da obezbedi adekvatno testiranje svih softverskih komponenti pre nego li one budu puštene u produkcijski rad. Takođe je neophodno napraviti plan vraćanja u prethodno stanje u slučaju da to bude potrebno. Potrebno je urediti procese upravljanja hitnim promenama hardverskih i softverskih komponenti.

Posebno je definisana situacija prelaska na novi sistem glavnih poslovnih aplikacija (core bussines application) kada je finansijska institucija dužna da o tome obavesti Narodnu banku Srbije najkasnije 30 dana pre početka testiranja planiranog u vezi sa tom migracijom. Obavezne stavke u vezi sa migracijom core sistema su:

1. detaljne opise sistema između kojih se podaci prenose;
2. plan, dinamiku i opis aktivnosti u vezi sa migracijom podataka, uključujući i metodologiju testiranja;

3. rezultate procene rizika i opis kontrola koje će se primeniti tokom migracije podataka, a u cilju očuvanja poverljivosti, integriteta i raspoloživosti podataka;
4. plan vraćanja na stanje pre migracije podataka.

Finansijska institucija je dužna da obezbedi izradu, čuvanje i redovno održavanje dokumentacije koja se odnosi na informacioni sistem kako bi ta dokumentacija bila u svakom trenutku tačna, potpuna i ažurna. Pristup ovim dokumentima potrebno je da imaju zaposleni u skladu sa potrebama posla.

Finansijska institucija je dužna da obezbedi adekvatno, kontinuirano stručno osposobljavanje i obučavanje zaposlenih za korišćenje informacionog sistema i očuvanje njegove bezbednosti i funkcionalnosti.

3.8 Poveravanje aktivnosti u vezi sa informacionim sistemom trećim licima

Ove aktivnosti se uređuju propisima kojima se uređuje poslovanje finansijskih institucija osim ako ovom odlukom nije drukčije propisano.

Aktivnosti koje se pod ovim podrazumevaju su sve aktivnosti koje obuhvataju obradu, čuvanje, i/ili pristup podacima kojima rasploaže finansijska institucija, a odnose se na njeno poslovanje, kao i aktivnosti razvoja i/ili održavanja glavnih poslovnih aplikacija.

Poveravanje aktivnosti uključuje i poveravanje aktivnosti licima povezanim sa finansijskom institucijom imovinskim i upravljačkim odnosima koja posluju u Republici Srbiji ili u inostranstvu. Poveravanjem aktivnosti ne smatra se korišćenje standardizovanih servisa (SWIFT; Bloomberg, Reuters i dr.) telekomunikacionih usluga, kao ni nabavka softvera koji je kao gotovo rešenje komercijalno dostupan na tržištu i slično.

Poveravanje aktivnosti vrši se na osnovu ugovora zaključenog između finansijske institucije i lica kome se te aktivnosti poveravaju.

Posebno se navode stvari koje je finansijska institucija dužna da uredi:

1. proces odlučivanja o poveravanju aktivnosti i kriterijume za donošenje te odluke;
2. način uključivanja tih aktivnosti u proces upravljanja rizicima i u sistem internog izveštavanja o rizicima;
3. način na koji obezbeđuje kontinuitet obavljanja aktivnosti koje je poverila i mere koje preduzima u slučaju raskida ugovornog odnosa s pružaocima usluga, kao i u slučaju privremenog zastoja ili prestanka pružanja tih usluga;
4. način vršenja nadzora nad obavljanjem aktivnosti koje je poverila, uključujući i nadzor nad usklađenošću tih aktivnosti s propisima, dobrim poslovnim običajima i opšteprihvaćenim standardima iz odgovarajuće oblasti.

Pri donošenju odluke naročito se obraća pažnja na uticaj poveravanja aktivnosti na:

1. kontinuitet poslovanja i reputaciju finansijske institucije;
2. troškove, finansijski rezultat, likvidnost i solventnost finansijske institucije;
3. rizični profil finansijske institucije;
4. kvalitet usluga koje finansijska institucija pruža klijentima.

Pre donošenja odluke o poveravanju aktivnosti, finansijska institucija je dužna da :

1. izvrši detaljnu analizu potencijalnog pružaoca usluga koja se odnosi na njegovu sposobnost pružanja usluga, finansijsko stanje i poslovnu reputaciju;
2. utvrdi da li propisi države ili država u kojima potencijalni pružalac usluga posluje omogućuju Narodnoj banci Srbije nesmetano vršenje neposredne kontrole tog poslovanja u delu koji se odnosi na obavljanje poverenih aktivnosti ili je u vezi sa tim aktivnostima;
3. proceni moguće poteškoće i vreme potrebno za izbor drugog pružaoca usluga, ili mogućnost nastavka obavljanja tih aktivnosti unutar finansijske institucije u slučaju prestanka pružanja ugovorenih usluga, kao i da s tim u vezi donese odgovarajuću izlaznu strategiju

Finansijska institucija je dužna da Narodnoj banci Srbije obezbedi nesmentano vršenje kontrole poverenih aktivnosti, kao i nadzora nad njima. Kontrola, odnosno nadzor obuhvataju i neposrednu kontrolu nad obavljanjem poverenih aktivnosti u prostorijama pružaoca usluga, odnosno na lokaciji na kojoj se poverene aktivnosti obavljaju. Finansijska institucija je dužna da obezbedi da ona, spoljni revizor ili Narodna banka Srbije imaju blagovremen i neograničen pristup dokumentaciji, podacima, prostorijama, odgovornim licima i delu poslovanja u vezi sa poverenim aktivnostima.

Cilj prethodnih delova koji se tiču poveravanja aktivnosti trećim licima jeste da se naglasi dužnost finansijske institucije da ne ugrozi bezbednost ili funkcionalnost informacionog sistema, kao i da podaci finansijske institucije ostanu u njenom posedu.

Finansijska institucija i pružalac usluga dužni su da poštuju zakon o zaštiti podataka o ličnosti, kao i druge propise kojima se uređuje čuvanje tajne nastale u poslovanju finansijskih institucija.

Finansijska institucija koja namerava da određene aktivnosti poveri, ili da promeni pružaoca usluga dužna je da o tome obavesti Narodnu banku Srbije najkasnije 30 dana pre planiranog poveravanja aktivnosti, odnosno planirane promene. Obavezni elementi ovog obaveštenja su:

1. odluka nadležnog organa finansijske institucije o poveravanju aktivnosti, odnosno o promeni pružaoca usluga;
2. opis aktivnosti koje finansijska institucija namerava da poveri, kao i obaveza i uslova koje je pružalac usluga dužan da ispuni;
3. osnovne podatke o pružaocu usluga;

4. rezultate detaljne analize pružaoca usluga;
5. izlaznu strategiju u slučaju prekida saradnje sa pružaocem usluga.

Ukoliko se pružalac usluga nalazi izvan teritorije Republike Srbije ili je ugovoreno da poverene aktivnosti obavlja izvan Republike Srbije, finansijska institucija je dužna da dostavi dokumentaciju o tome da propisi date zamlje Narodnoj banci Srbije omogućavaju nesmetano vršenje neposredne kontrole koja se tiče tog poslovanja.

Pružalac usluga može drugome licu poveriti aktivnosti koje je njemu poverila finansijska institucija ili druge poslove u vezi sa tom aktivnošću samo uz prethodnu saglasnost finansijske institucije. Finansijska institucija dužna je da Narodnu banku Srbije obavesti o poveravanju aktivnosti odmah nakon davanja saglasnosti. Lice kome su poverene aktivnosti može početi da ih obavlja nakon isteka 15 dana od dana davanja saglasnosti. Finansijska institucija odgovara u celosti za aktivnosti koje je poverila pružaocima usluga.

3.9 Elektronsko bankarstvo

Ovaj deo odnosi se samo na banke i definiše njihovu obavezu da se kao sastavni deo upravljanja rizikom uspostavi i proces upravljanja rizicima koji proizilaze iz elektronskog bankarstva.

Banci se stavljaju na dužnost sledeći elementi:

1. obavezna primena sigurnih i efikasnih metoda za proveru i potvrdu identiteta i ovlašćenja lica, procesa i sistema;
2. obezbeđivanje autentifikacije korisnika sa kombinacijom minimum dva elementa pri izvršavanju platnih transakcija u okviru elektronskog bankarstva;
3. obezbeđena potvrda identiteta banke pri komunikaciji preko distributivnog kanala; elektronskog bankarstva u cilju omogućavanja korisnicima provere autentičnosti banke;
4. postojanje odgovarajućih sistemskih i operativnih zapisa u cilju obezbeđivanja neporecivosti i dokazivosti radnji u vezi sa elektronskim bankarstvom.

4. Analiza odluke

4.1 Okvir za upravljanjem IS

Uspostavljanje adekvatnog informacionog sistema koji poseduje sve navedene uslove moguće je pod uslovom da se izvrši potpuna dekompozicija sistema i izvrši sagledavanje tokova podataka, kao i analiziranje trenutnih performansi svih ključnih tačaka u sistemu koji utiču na tok podataka.

Obezbeđivanje tačnih i potpunih informacija uslovljava organizacije da uvedu detaljne kontrole pri unosu podataka, kao i dodatne kontrolne mehanizme za proveru ispravnosti i eventualno uočavanje spornih podataka.

Projektovanje kontrola za validaciju podataka na ulazu, u toku procesa obrade i na izlazu zahteva konsultovanje analize toka podataka i uspostavljanje odgovarajućih validacija na svim kritičnim tačkama.

Zahtev da se svi poslovno značajni sistemi objedine u jedan integralni sistem koji bi uključivao i sistem za izveštavanje ukazuje na potrebu kreiranja jedinstvenog sistema koji bi modularnošću omogućio skalabilnosti i traženu jedinstvenost ili u većini slučajeva hibridne sisteme koji koriste neki vid međusobne povezanosti u okviru integralnog informacionog sistema.

Da bi se obezbedilo da sistem poseduje funkcionalnost, kapacitete i performanse potrebno je izvršiti detaljnu analizu sistema i uspostaviti mehanizam nadgledanja koji će moći da pruži uvid u rad i efikasnost sistema kako bi se blagovremeno uočili eventualni nedostaci. Ovaj segment dodatno omogućuje proaktivnost što svakako ide u prilog zahtevu za adekvatnim informacionim sistemom.

Obezbeđivanje tačnih i potpunih informacija moguće je samo ukoliko postoje mehanizmi za kontrolu i nadgledanje tj. potencijalno uočavanje neispravnih odnosno sumnjivih podataka. Ova korak svakako nije lak za implementaciju samo uz pomoć tehničkih rešenja pošto kvalitet podataka u mnogome zavisi od osobe koja ga je generisala. Ipak postavljanje što većeg broja kontrolnih tačaka i validacija podataka na ulazu u sistem, u toku obrade kao i na izlazu obezbediće veći kvalitet informacija.

Kako bi se izašlo u susret zahtevu za objedinjavanjem svih poslovno značajnih sistema za kompaniju je veoma bitno da oformi spisak svih sistema i izvrši njihovu kategorizaciju, ovim se postiže uočavanje kritičnih sistema i njihova dalja obrada.

Uspostavljanje, nadziranje, revidiranje i unapređenje informacionog sistema radi smanjenja izloženosti rizicima i očuvanja bezbednosti nešto je sa čime se sve organizacije u većoj ili manjoj meri konstantno bave. Odeljenje rizika i služba informacionih tehnologija zaduženi su za uspostavljanje i održavanje ovakvog sistema[2]. Kao polazna osnova može se uzeti i analiza

rizika koja se vrši i pri uspostavljanju kontinuiteta poslovanja ukoliko je taj posao već urađen. Uspostavljanjem sistema za upravljanje bezbednošću sistema pokriće se drugi deo ovoga zahteva.

Utvrdjivanje ovlašćenja i odgovornosti svojih organa upravljanja i nadzora koji se odnosi na poslove upravljanja rizicima i bezbednošću sastavni je deo Cobit i ITIL dokumenata i taj posao je najefikasnije prikazati uz pomoć COBIT RACI matrica (prikaz aktivnosti i osoba povezanih sa njima)[7].

Obaveza da se uspostavi strategija razvoja informacionog sistema je zahtev koji obezbeđuje da se na strateškom planu sagleda informacioni sistem i na vreme obezbede akcije potrebne za njegov razvoj i normalno funkcionisanje u budućnosti. Praćenjem trendova i razvoja poslovanja kompanije su informisane o mogućim pravcima kretanja industrije a monitoringom i analizom postojećeg sistema dobijaju realne informacije koje oslikavaju stanje trenutnog sistema. Kompanije su u obavezi da usklađuju strategiju sa realnim potrebama. Dobro utvrđena strategija razvoja sprečiće eventualne problem koji bi mogli nastati u slučaju reaktivnog pristupa na događaje.

Bitnost definisanja upravljačke strukture ogleda se u zahtevu za formiranjem jasne organizacione strukture sa ciljem podele poslova i odgovornosti među zaposlenima. Uspostavljanjem ovakve strukture sprečavaju se potencijalni sukobi interesa, razgraničava delokrug odgovornosti i definiše jasna podela posla, što za efekat ima efikasniji rad organizacije. Dobrom organizacionom strukturom vrši se raspodela posla i odgovornosti u najboljem odnosu u skladu sa poslom i resursima koji su nam na raspolaganju[3].

Za efikasan rad svih zaposlenih potrebno je definisati mnoštvo akata i procedura za rad, no njihovim nastankom ne rešavaju se potencijalni problemi, te je potrebno izvršiti upoznavanje zaposlenih sa njihovim sadržinama kako bi se naglasila njihova odgovornost, ovlašćenja i potrebe. Upotreba internih veb portala idalan je način za distribuciju i prezentovanje ovakvih podataka. Sami portali su u manjoj ili većoj meri pristupni u većini sistema tako da je potrebno izvršiti manja usklađivanja i organizovati njihovo održavanje. Bitan stavka uz sam portal svako je i informisanje zaposlenik o njegovom postojanju i upućivanje korisnika na njega. Kako bi se korisnicima dodatno približile informacije poželjno je redovno organizovanje javnih skupova (prezentacije, radionice...) na kojima bi se u kratkim crtama oni informisali o novim dokumentima i podsetili na stare.

Zahtevom da se usvoji odogovarajuća metodologija za upravljanje projektima u vezi sa informacionim sistemom otvara se jedna velika oblast koja zahteva prelazak na projektnu organizaciju i kompletno drugačiji način vođenja projekata za one organizacije koje u dosadašnjem radu to nisu praktikovale. Ispunjavanje uslova koje ova tačka zahteva pred kompanije stavlja veliki izazov i ulaganja ali su prednosti koje donosi sa druge strane poprilično velike.

Uvođenje bilo koje metodologije podrazumeva generalno menjanje koncepta na koji se posao do sada obavljao.

Menadžment projekata za cilj ima da disciplinuje organizacije i da omogući kontrolu resursa tako da se svi poslovi završe u predviđenom vremenskom roku, na očekivanom nivou kvaliteta, i sa sredstvima koja su za to namenjena.

Kompanijama na su na raspolaganju Prince2, MPMM, ITIL, MSF, MITP i mnoge druge metodologije koje mogu da iskoriste za ispunjavanje ovog zahteva. Za koju god da se odlučiće biće potrebna dodatna prilagođavanja kako bi se ona u potpunosti preslikala na konkretnu organizaciju.

Naravno sama metodologije nije čaroban štapić pa je sem nje kompanijama potrebno i kvalitetno osoblje koje ume da realizuje zahteve iz metodologija (menadžeri projekata).

Utvrđivanje izveštavanja nadležnog organa o relevantnim činjenicama u vezi sa funkcionalnošću i bezbednošću informacionog sistema zahtev je koji pred organizaciju stavlja jasan zahtev i obavezu izveštavanja. Ključni deo odluke za organizacije jeste koji događaji i informacije će biti prosleđivani ka nadležnom organu (NBS,) kao i koje osobe će u okviru kompanije biti zadužene za ovaj posao.

4.2 Upravljanje rizikom informacionog sistema

Samo upravljanje rizicima organizovano je mahom u svim organizacijama u okviru posebnih odeljenja koja se bave pitanjima rizika. Specifičnost informacionih tehnologija predstavlja izazov ovakvim organizacionim delovima koji moraju dodatno edukovati postojeće kadrove ili zaposliti nove kako bi se što adekvatnije pokrila ova po poslovanje bitna oblast.

Proces upravljanja rizikom podrazumeva inicijalnu analizu koja za cilj ima da identifikuje što veći broj rizika za informacioni sistem u celini. Ovde detektovani rizici zatim se moraju oceniti i tako klasifikovati po sledećim parametrima verovatnoći pojavljivanja, mogućem uticaju (vrši se kvalitativna i kvantitativna analiza). Sa ovim informacijama potrebno je odrediti adekvatan odgovor za sve detektovane rizike. Odgovori mogu biti prihvatanje, izbegavanje, prepuštanje ili umanjenje.

Uvođenjem procesa upravljanja rizicima informacionog sistema povećava se bezbednost čitavog informacionog sistema i on se čini pouzdanijim i efikasnijim, ali da bi se tako stanje održalo u dužem periodu ovaj proces mora biti kontinuiran i podložen redovnim revizijama i monitoringu. Svaka promena u organizaciji, svaka pojava novih rizika ili promene u atributima postojećih rizika moraju se po automatizmu detektovati, analizirati i uvesti u sistem odgovora na rizike. Redovnim skriningom rizika, penetracionim testovima, internim i eksternim revizijama kao i

unutrašnjom kontrolom moguće je pokriti veliki deo promena u ovom domenu i pripremiti blagovremen odgovor na novonastale situacije.

Postojeći propisi kojima se uređuju opšti uslovi i način upravljanja rizicima primenjuju se i na upravljanje rizikom informacionog sistema osim ako ovom odlukom nije drugačije uređeno.

Od organizacija se zahteva da uspostave proces upravljanja rizikom kako bi se pokrile sve faze, a to su identifikovanje i merenje, procena rizika, a na osnovu ovih faza izvršilo bi se i ublažavanje rizika. Sistem takođe mora da obezbedi adekvatno praćenje i kontrolu svih detektovanih rizika.

Za uvođenje i uspostavljanje zahtevanog sistema organizacijama je na raspolaganju ISO 27005 standard koji se bavi ovim pitanjem.

Pomoć u vidu specijalizovanih softvera takođe je nešto što će u mnogome koristiti svakom sistemu a neki od njih su RSA NetWitness, HP OpenView i dr.

Upravljanje rizikom informacionog sistema ne sme da ugrozi upravljanje bezbednošću i kontinuitetom poslovanja organizacije. Očekuje se integrisanje upravljanja rizikom u sve faze razvoja informacionog sistema. Ovim zahtevima je potvrđena ranije izrečena konstatacija da je svaka karika lanaca podjednako bitna za njegovu čvrstinu tj. za njegovu namenu i smisao, tako se i u domenu rizika oni moraju sagledavati u potpunosti i iz svih delova sistema.

Posebno je naglašena dužnost da se vrši adekvatno upravljanje rizicima koji nastaju iz ugovornih odnosa sa pravnim i fizičkim licima čije se aktivnosti odnose na informacioni sistem. Obaveza je organizacije da vrši kontinuiran nadzor kvaliteta uzgovorenenih aktivnosti i time proverava da li se i kako izvršavaju obaveze iz ugovora. Nadziranje podrazumeva detaljnu analizu ugovora sa trećim licima i njihovo podvrgavanje pravnim i tehničkim analizama u cilju eventualne detekcije problematičnih tačaka. Takođe se predmet ugovora kao i aktivnosti u vezi sa njima stavljaju na spisak aktivnosti za redovnu analizu rizika i sve ostale analize koje su inače pristune u sistemu[2].

4.3 Unutrašnja revizija informacionog sistema

Sve finansijske organizacije podložne su raznim vrstama revizije i navikle su na njihovo delovanje. Odlukom se zahteva uvođenje interne revizije koja bi u svojoj metodologiji koristila procenu rizika i na osnovu nje vršila internu reviziju.

Za razliku od eksterne revizije, interna revizija često ima drugačiji pristup analizi sistema s obzirom na intimno poznavanje same organizacije i njenih eventualnih slabosti.

U svom radu interna revizija veliku pomoć nalazi u CAAT (Computer Assisted Audit Tools) softveru a na raspolaganju su im između ostalog (ACL Analytics, IDEA, WizSoft i dr.) naravno ukoliko korisnici ne žele da razviju svoj interni softver za ovu namenu.

Obavljanje interne revizije informacionog sistema uređuje se propisima o poslovanju finansijskih institucija. Oblast interne revizije informacionih sistema zahteva duboko poznavanje materije i intimno poznavanje samog sistema koji se analizira a to je kombinacija do koje nije nimalo lako doći. U svome radu interni revizori mogu da se oslone na standarde, procedure i metodologiju razvijenu od strane institucija koje se bave ovom problematikom npr. Institute of Internal Auditors, ISACA i dr.

4.4. Bezbednost informacionog sistema

Bitan zahtev odluke, a ujedno i vrlo kompleksan posao predstavlja formiranje, uvođenje i korišćenje politike bezbednosti informacionog sistema.

Politika bezbednosti informacionog sistema je unutrašnji opšti akt kojim se uređuju principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema. Ovakvu politiku organizacija razvija najčešće formiranjem odeljenja za bezbednost informacija i njihovom aktivnošću u tom pravcu. Ovo odeljenje je dužno da ovakvu politiku usklađuje sa promenama i trendovima u okruženju[11].

ISO standardi 27001 i 27003 pružice neophodnu pomoć pri analizi zahteva za uvođenjem kao i konkretnim akcijama za implementaciju, upravljanja, nadgledanje, održavanje i unapređivanje sistema za upravljanje bezbednošću informacionog sistema.

Ovaj proces mora biti kontinuiran kako bi se održao adekvatan nivo bezbednosti. Dužnost je svake finansijske organizacije da na osnovu procene rizika, obaveza koje proizilaze iz propisa, akata i ugovora identifikuje i prati potrebu za bezbednošću sistema. Adekvatan odgovor na ovakve zahteve organizacije mogu dati kroz osnivanje nameskih službi koje će se baviti pitanjem bezbednosti u okviru kompanije. Ova služba zadužena je za uspostavljanje, održavanje i unapređivanje politike bezbednosti informacionog sistema kroz uspostavljanje skupa polisa i procedura koje se naslanjaju na glavni dokument polisu bezbednosti informacionog sistema. Pored generisanje ovakvih dokumenata ova služba ima zadatak da prati i uvodi i predlaže promene u skladu sa aktuelnim dešavanjima na tržištu i u okviru zakona.

Ova služba se u organizacionom dijagramu u novije vreme ne nalazi ispod IT službe već se vezuje direktno za izvršne funkcije i njima polaže račune. Ovim se postiže eliminisanje potencijalnih konflikata na relaciji sa IT službom.

Organizacija je dužna da uspostavi odgovarajuće kontrole, a radi postizanja i održavanja adekvatnog nivoa bezbednosti. Nakon izvršenih analiza rizika potrebno je za sve detektovane rizike odgovoriti uvođenjem odgovarajućih kontrola. Za izvršenje ovih direktiva može se osloniti na sledeće vrste kontrola:

1. Interne – namena da obezbede efikasno i efektivno upravljanje internim resursima organizacije, obezbede usklađivanje sa raznim regulativama, obezbede različite izveštaje u pravo vreme i na pravu adresu
2. Administrativne – namena da se jasno definišu prava i obaveze interno zaposlenih
3. Računovodstvene – namena da se osiguraju podaci i resursi finansijske prirode
4. Preventivne – namena da se spreči pojava neželjenih aktivnosti
5. Detektivne – namena da se nadgleda i uoči pojava neželjenih aktivnosti koje su nastale a nisu uočene od strane preventivnih kontrola
6. Korektivne – namena da se nakon određenih događaja uspostavi pređašnje stanje i otklone nedostaci koji su doveli do pojave događaja
7. Odbijajuće – namena da obeshrabre pojavu neželjenih događaja ukazujući na zakonske ili druge posledice
8. Kompenzujuće – namena da se ublaže posledice akcija koje nije moguće izbeći

Jedan od bitnih faktora u lancu bezbednosti informacija predstavlja i klasifikacija informacionih dobara. Nju su organizacije dužne da izvrše prema stepenu kritičnosti i osetljivosti, a s obzirom na moguće posledice narušavanja njihove poverljivosti, integriteta i raspoloživosti. Nakon izvršene klasifikacije, organizacije su u obavezi da izvrše adekvatno osiguravanje detektovanih dobara.

Za potrebe obavljanja poslova upravljanja informacionim dobrima njihovu klasifikaciju, te zaštitu, organizacija je dužna da imenuje određene osobe (najčešće spomenut sektor za bezbednost informacija).

Sama klasifikacija obezbeđuje jasnu podelu dokumenata po sigurnosnim i drugim prioritetim i kompaniju primorava na detaljnu analizu dokumenata koji se generišu i koji cirkulišu u okviru njihovog informacionog sistema. Identifikovanjem bezbedonosno osetljivih dokumenata i njihovom klasifikacijom ona se posebno tretiraju i time se eliminišu razne sigurnosne pretnje a ovakva dokumenta ističu kao bitna za poslovanje. Standardni nivo za klasifikaciju su javni, interni, poverljiv i strogo poverljiv mada organizacije mogu definisati i druge bezbednosne nivoe za klasifikaciju.

Klasifikacija obuhvata kako štampana tako i elektronska dokumenta u koja spada naravno i elektronska pošta, kao posebno osetljiv kanala komunikacije koji često ostaje nepokriven pri klasifikaciji dokumenata a može biti izvor kompromitovanja podataka.

Primer softvera za klasifikaciju jeste softver Titus istoimene kompanije.

Organizacija je dužna da sprovede odgovarajuću kontrolu pristupa resursima informacionog sistema. Ovde se kao najveća prepreka nalaze mnogobrojna hibridna i raznorodna okruženja koja

se nalaze u informacionim sistemima većine organizacija, te njihova harmonizacija ili uvođenje i održavanje višestrukih sistema za kontrolu pristupa.

Takođe je u okviru organizacije potrebno uspostaviti sistem upravljanja korisničkim pravima, naročito pri evidentiranju korisnika, autorizaciji, identifikaciji i autentifikaciji.

Potrebno je i uvođenje posebnog sistema za nadzor nad korisničkim pravima pristupa, a u cilju prevencije i ranog otkrivanja potencijalnih nepravilnosti u sistemu.

Od organizacija se zahteva poštovanje i uvođenje principa najmanjih privilegija pri autorizaciji korisnika informacionog sistema, koja ima za cilj dodeli najmanjih potrebnih prava za pristup odgovarajućim resursima, a samim tim sprečavanje dodeljivanja prevelikih privilegija. U ovom procesu je potrebno obratiti pažnju da se dodeljivanjem nedovoljnih ovlašćenja ne uskrati mogućnost korisnicima da obavljaju svoje redovne aktivnosti. Dodeljivanje prava moguće je vršiti na nivou korisnika ili grupe stim da se dodela ovašćenja grupi smatra višestruko efikasnijim pristupom u velikim sistemima.

Reviziju korisničkih prava pristupa potrebno je vršiti minimum jednom godišnje.

Udaljen i povlašćen (administratorski) pristup potrebno je urediti posebnim dokumentom, a zbog povećanog sigurnosnog rizika koji proizilazi iz ovih operacija.

Skoro svi popularni sistem na tržištu imaju servis za obavljanje ove funkcije koji korisnicima omogućava granularno dodeljivanje ovlašćenja, neki od ovih sistema su LDAP, Active directory i dr. Ukoliko se želi specijalizovan softver koji bi obuhvatio ove poslove potrebno je pogledati paletu IDM (Identity Management System) sistema npr. IBM Tivoli Identity Manager, Oracle Identity Manager i dr.

Poseban deo posvećen je generisanju i čuvanju zapisa o događajima u sistemu kao ključnom segmentu u analizi, monitoringu i rekonstrukciji dešavanja u sistemu.

Na osnovu procene rizika vrši se uspostavljanje sistema za nadgledanje i generisanje operativnih i sistemskih zapisa. Kako ovi zapisi predstavljaju bitnu kariku u bezbednosti, potrebno je posvetiti posebnu pažnju pri njihovom čuvanju i arhiviranju kako bi se obezbedila neporecivost datih događaja. Još je bitno utvrditi vreme, učestalost, obim i način praćenja tih zapisa.

Ključno je da kada se definiše način sakupljanja i skladištenja zapisa, da oni u sebi sadrže dovoljno informacija zarad otkrivanja eventualnih neovlašćenih pristupa i/ili aktivnostima na resursima informacionog sistema, kao i informacija potrebnih za utvrđivanje odgovornosti s tim u vezi[5].

Posebnu pažnju treba usmeriti na događaje koje udaljeni korisnici (najčešće administratori i eksterni partneri) vrše na sistemu a koje je jako teško ili nemoguće rekonstruisati uz pomoć sistemskih logova. Ovakve akcije najefikasnije se kontrolišu softverima koji vrše snimanje

čitavih sesija (ssh, rdp i dr.) i koji omogućavaju njihovo trajno skladištenje, jednostavnu pretragu i reprodukciju u cilju analize.

Kako bi čitav lanac sigurnosti informacionog sistema bio jedna neraskidiva celina, moraju se uključiti i mere klasične fizičke sigurnosti. Organizacija je dužna da primeni odgovarajuće metode fizičke zaštite kako bi osigurala sistem od neovlašćenog fizičkog pristupa, krađe ili fizičkog oštećenja. Fizička zaštita podrazumeva sprečavanje fizičkog pristupa opremi koja na sebi ima osetljive podatke ili je kritična za rad i funkcionisanje sistema. Ključni predmet osiguranja svakako predstavlja server sala koja sadrži većinu podataka i opreme na jednom mestu i metode njene zaštite su opšte poznate i manje više su ispoštovane u većini finansijskih institucija. Neke od klasičnih metoda zaštite server sale jesu protiv požarna zaštita, kontrola ulaska u salu, kontrola kritičnih parametara (temperatura, vlažnost, dim, voda...), redundantno napajanje, redundantni uređaji za klimatizaciju i dr.

Pored same server sale naravno u samoj organizaciji postoji mnoštvo tačaka koje je potrebno obezbediti i uključiti u plan fizičke bezbednosti kao na primer udaljene kancelarije sa opremom i dokumentima, papirna dokumenta osetljive prirode, mrežna oprema dislocirana iz server sale itd.

Posebnu pažnju potrebno je posvetiti mobilnim uređajima (laptopovi, tableti, pametni mobilni telefoni i dr.) pošto se na njima standardno nalazi velika količina osetljivih podataka a podložni su gubitku, krađi i drugim sigurnosnim pretnjama.

Resurse informacionog sistema potrebno je zaštititi i od potencijalnog ugrožavanja od malicioznog programskog koda. Pod ovom tačkom se podrazumeva uvođenje antimalware softvera, što je inače uobičajana praksa u svim organizacijama. Pored samog uvođenja softvera, potrebno je obezbediti centralni monitoring, delegirati osobu zaduženu za kontrolu i kreirati prateće sigurnosne polise koje se odnose na korišćenje informacionih resursa, a u vezi sa potencijalnim kontaktom sa malicioznim softverom (internet, email, usb, programi i drugo). Različite pretnje zahtevaju i specijalizovan softver kao konkretan odgovor npr. maliciozni softver koji se širi putem elektronske pošte zahteva specijalizovan softver koji se instalira na serverima elektronske pošte i vrši centralnu kontrolu poruka na prvom koraku ulaska u sistem.

Nikako ne treba izostaviti mobilne uređaje (što je čest slučaj danas) jer se njihovim korišćenjem značajno povećava rizik od malicioznog softvera. Njihova javna primena i neadekvatna kontrola predstavlja poseban rizik po njih.

Redovnim i preventivnim kontrolama sve podatke kompanije potrebno je podvrgavati analizama na maliciozni kod po mogućstvu sa više različitih softverskih paketa zbog efikasnijeg učinka.

4.5 Upravljanje kontinuitetom poslovanja i oporavak aktivnosti u slučaju katastrofa

Dinamika kojoj je izloženo funkcionisanje informacionih sistema finansijskih organizacija uslovljava njegovu stalnu dostupnost i potrebu za razvijanjem plana kontinuiteta poslovanja. Ovo je uvidela većina organizacija u ovom sektoru i u nekom obliku su pokušale da uvedu ovaj proces u organizaciju, a zahtevi koji se stavljaju pred njih u ovoj sekciji dokumenta NBS detaljnije definišu delove ovog procesa.

Upravljanje poslovnim kontinuitetom (Business Continuity Management) je sveobuhvatni upravljački proces, koji identifikuje potencijalne udare na poslovanje institucije koji mogu dovesti do gubitka sredstava kojima se obavlja poslovanje, i koji pruža okvir za izgradnju otpornosti i sposobnosti za efikasno reagovanje, uz primenu specifičnih mera, uglavnom organizacionih, infrastrukturnih i tehnoloških koje treba da obezbede nesmetano i kontinuirano funkcionisanje svih kritično važnih procesa i sistema.

Sistemske procesi koji se obavljaju u Sektoru IT su definisani kao kritični jer se većina ostalih procesa oslanja na iste. U tom smislu, funkcionisanje IT servisa ima ključni uticaj na nastavak poslovanja banke u vanrednim situacijama. Osnovni preduslov funkcionisanja IT servisa je postojanje tehničkih preduslova i ljudski resursi.

Plan IT rešenja za DR kao deo poslovnog kontinuiteta ima za cilj i obezbeđuje:

- Brz i adekvatan odgovor na krizne situacije
- Zaštitu života i sigurnost zaposlenih
- Smanjenje štetnih uticaja na poslovanje institucije
- Održanje kritičnih poslovnih funkcija
- Rad sa spoljnim saradnicima za vreme oporavka
- Smanjenje konfuzije za vreme krize
- Obezbeđenje održivosti poslovnih procesa
- Osposobljavanje za nastavak poslovanja u što kraćem roku
- Poštovanje zakonske regulative

Finansijske organizacije su u obavezi da uspostave proces upravljanja kontinuitetom poslovanja. Pod procesom upravljanja kontinuitetom smatraju se sve aktivnosti potrebne da se napravi plan sa ciljem da se održi i uspostavi neometan tok kritičnih poslovnih aktivnosti u slučaju katastrofa. Dobro definisan plan obezbeđuje brz i efikasan odgovor koji omogućava oporavak i ponovno uspostavljanje kritično važnih funkcija.

Proces upravljanja kontinuitetom poslovanja mora biti zasnovan na analizi uticaja na poslovanje i na proceni rizika. Detaljnije su navedene tačke koje se moraju obuhvatiti u analizi:

1. utvrđivanje resursa i sistema potrebnih za odvijanje pojedinačnih poslovnih procesa, kao i njihove međuzavisnosti i povezanosti;

2. procenu rizika u vezi sa pojedinačnim poslovnim procesima, uključujući i verovatnoću nastanak neželjenih događaja i njihov potencijalni uticaj na kontinuitet poslovanja, finansijsko stanje i reputaciju finansijske institucije;
3. utvrđivanje prihvatljivog nivoa rizika i tehnika za ublažavanje identifikovanih rizika;
4. utvrđivanje najdužeg prihvatljivog prekida (MAO) pojedinačnih poslovnih procesa;
5. utvrđivanje kritičnih/ključnih poslovnih procesa i aktivnosti.

Pored samih kritičnih funkcija potrebno je identifikovati i procese unutar tih funkcijam i utvrditi njihove prioritete. Ovakve pretpostavke potrebno je uredno dokumentovati i redovno revidirati.

Na osnovu sakupljenih podataka iz analiza organizacije su dužne da usvoje strategiju oporavka koju će primeniti u slučaju prekida poslovanja. Strategija obavezno mora da sadrži:

1. prioritete oporavka poslovnih procesa, kao i resursa i sistema potrebnih za njihovo odvijanje
2. ciljne nivoe aktivnosti (SDO)
3. ciljna vremena oporavka (RTO)
4. ciljne tačke oporavka (RPO)

Upravni odbori finansijskih institucija u obavezi su da usvoje dva dokumenta, a to su Plan kontinuiteta poslovanja (Business Continuity Plan) i Plan oporavka aktivnosti (Disaster Recovery Plan).

Plan kontinuiteta poslovanja je dokument koji obavezno sadrži[16]:

- opis procedura u slučaju prekida poslovanja
- ažuran spisak svih resursa neophodnih za ponovno uspostavljanje kontinuiteta poslovanja
- podatke o timovima koji će biti odgovorni za ponovno uspostavljanje poslovanja u slučaju nastanka nepredviđenih događaja i o imenovanim članovima tih timova, uključujući i njihove jasno utvrđene dužnosti i odgovornosti, kao i plan unutrašnjih i spoljašnjih linija komunikacije
- rezervnu lokaciju u slučaju prekida poslovanja i nemogućnosti ponovnog uspostavljanja poslovnih procesa na primarnoj lokaciji

Plan oporavka aktivnosti u slučaju katastrofa je dokument koji obavezno sadrži[17]:

- procedure za oporavak informacionog sistema kad nastupe katastrofalni događaji
- prioritete oporavka resursa informacionog sistema
- podatke o timovima koji će biti odgovorni za oporavak informacionog sistema i o imenovanim članovima tih timova uključujući i njihove jasno utvrđene dužnosti i odgovornosti

- rezervnu lokaciju za oporavak informacionog sistema odnosno lokaciju rezervnog računarskog centra

Svi zaposleni moraju biti upoznati sa svojim ulogama i odgovornostima u slučaju nastupanja vanrednih situacija kako bi njihove reakcije u datoj situaciji bile usklađene sa koracima iz plana. Organizacije su u obavezi da prate i usklađuju planove i procedure za oporavak u skladu sa promenama u okruženju, kao i sa poslovnom politikom i strategijom poslovanja.

Ovaj plan organizacija je dužna da testira najmanje jednom godišnje, kao i posle značajnih promena, te da izveštaj o tome dostavi nadležnom organu finansijske institucije.

Finansijska institucija je dužna da u sklopu upravljanja kontinuitetom poslovanja u obzir uzme i aktivnosti poverene trećim licima i zavisnost od usluga tih lica.

Organizacije su u obavezi da u slučaju aktiviranja plana usled nastanka neke od katastrofa o tome obaveste Narodnu banku Srbije i to najkasnije narednog dana od dana nastanka tih okolnosti, kao i da po potrebi dostava dodatnu dokumentaciju u vezi sa relevantnim činjenicama.

Organizacije su dužne da uspostave proces upravljanja incidentima kako bi bile u stanju da daju blagovremen i efikasan odgovor u slučaju narušavanja bezbednosti ili funkcionalnosti resursa informacionog sistema. U slučaju težeg incidenta, organizacije su dužne da o tome obaveste Narodnu banku Srbije najkasnije narednog dana od nastanka tog incidenta.

Upravljanje rezervnim podacima mora biti uspostavljeno kao dokumentovan proces sa jasno podeljenim ulogama i odgovornostima. Ovaj proces obavezno obuhvata postupak izrade, čuvanja i testiranja ovih kopija, kao i oporavak podataka i softverskih komponenti u cilju ponovnog uspostavljanja poslovnih procesa u skladu sa ciljanim vremenom oporavka (RTO).

Rezervne kopije moraju biti ažurne i adekvatno zaštićene, a postupci oporavka uspešno testirani.

Najmanje jedna ažurna i kompletna rezervna kopija mora biti skladištena na odgovarajućoj udaljenosti od primarne lokacije. Udaljenost se određuje na osnovu procene rizika informacionog sistema uz uzimanje u obzir potrebe za izbegavanjem uticaja istih rizika na obe lokacije.

U sklopu upravljanja kontinuitetom poslovanja organizacije su dužne da uspostave adekvatno opremljen rezervni računski centar. Ovaj rezervni centar mora biti adekvatno funkcionalan i bezbedan, kao i na odgovarajućoj udaljenosti od primarnog centra kako bi se izbegao uticaj istih rizika na obe lokacije[16].

4.6. Razvoj i održavanje informacionog sistema

Finansijske organizacije su dužne da uspostave proces razvoja informacionog sistema u skladu s relevantnim promenama unutar institucije, a u cilju kontinuirane adekvatnosti tog sistema.

Proces razvoja informacionog sistema sprovodi se u skladu sa usvojenom strategijom razvoja informacionog sistema i metodologijom upravljanja projektima uz uzimanje u obzir funkcionalnih zahteva i potreba za bezbednošću.

Proces razvoja mora biti dokumentovan u svim svojim delovima, a obavezno za analizu i projektovanje, programiranje, testiranje i uvođenje u produkciju.

Organizacije su dužne da na odgovarajući način razdvoje testno i produkcijsko okruženje.

Obaveza je uspostavljanje procesa upravljanja hardverskim i softverskim komponentama u svim fazama njihovog životnog ciklusa (od nabavke ili razvoja do povlačenja iz upotrebe). Ovaj proces obuhvata i održavanje detaljne i ažurne evidencije ovih komponenta, imenovanje lica odgovornih za upravljanje i zaštitu tih komponentata, kao i utvrđivanje pravila njihovog prihvatljivog korišćenja i bezbednog odlaganja pri povlačenju iz upotrebe.

Organizacije održavanje hardverskih i softverskih komponentata vrše prema preporukama proizvođača i zapise o tome čuvaju. Bitno je ne ugroziti funkcionalnost i bezbednost ovog sistema.

Organizacije su dužne da uspostave proces upravljanja promenama hardverskih i softverskih komponenti informacionog sistema kako bi izbegle da one eventualno dovedu do neočekivanog ponašanja sistema i da time naruše njegovu funkcionalnost i bezbednost.

Upravljanje promenama softverskih komponentata obuhvata obavezno sledeće komponente:

- utvrđivanje početnih verzija ovih komponentata
- iniciranje, analizu i odobravanje zahteva za promenom
- hronološko dokumentovanje svih promena ovih komponentata i arhitekture baza podataka, zajedno sa vremenom nastanka promene
- informisanje korisnika informacionog sistema o detaljima izvršenih promena

Sve promene hardverskih i softverskih komponentata moraju biti testirane i odobrene pre puštanja u produkcijski rad. Takođe, mora postojati plan vraćanja na prethodno stanje.

Hitne promene moraju biti uređene internim opštim aktom.

Organizacije koje planiraju migraciju podataka na novi sistem glavnih poslovnih aplikacija (core business application) o tome moraju obavestiti Narodnu banku Srbije najkasnije 30 dana pre početka testiranja planiranog u vezi sa tom migracijom.

Ovo obaveštenje naročito sadrži:

1. detaljne opise sistema između kojih se podaci prenose
2. plan, dinamiku i opis aktivnosti u vezi sa migracijom podataka, uključujući metodologiju testiranja

3. rezultate procene rizika i opis kontrola koje će se primeniti tokom migracije podataka s ciljem očuvanja poverljivosti, integriteta i raspoloživosti podataka
4. plan vraćanja na stanje pre migracije podataka

Svu dokumentaciju koja se odnosi na informacioni sistem organizacije su dužne da izrade, čuvaju i redovno održavaju tako da ona bude u svakom trenutku tačna, potpuna i ažurna. Pristup ovim dokumentima mora biti obezbeđen svim zaposlenima u skladu sa potrebama posla.

Organizacije su dužne da obezbede adekvatno stručno osposobljavanje i obučavanje zaposlenih za korišćenje informacionog sistema i očuvanje njegove bezbednosti i funkcionalnosti.

4.7 Poveravanje aktivnosti u vezi sa informacionim sistemom trećim licima

Sve aktivnosti koje obuhvataju obradu, čuvanje i/ili pristup podacima kojima raspolaže finansijska institucija, a odnose se na njeno poslovanje, kao i aktivnosti razvoja i/ili održavanja glavnih poslovnih aplikacija, a poverene su trećim licima moraju se posebno tretirati i na njih se odnose sledeće tačke dokumenta NBS[1].

Organizacija koja namerava da neke aktivnosti poveri dužna je da uredi:

- proces odlučivanja o poveravanju aktivnosti i kriterijume za donošenje te odluke
- način uključivanja tih aktivnosti u proces upravljanja rizicima i u sistem internog izveštavanja o rizicima
- način na koji obezbeđuje kontinuitet obavljanja aktivnosti koje je poverila i mere koje preduzima u slučaju raskida ugovornog odnosa s pružaocem usluga, kao i u slučaju privremenog zastoja ili prestanka pružanja tih usluga
- način vršenja nadzora nad obavljanjem aktivnosti koje je poverila i mere koje preduzima u slučaju usklađenosti tih aktivnosti s propisima, dobrim poslovnim običajima i opšteprihvaćenim standardima iz odgovarajuće oblasti.

Posebno su bitne sledeće oblasti uticaja pri poveravanju aktivnosti:

- kontinuitet poslovanja i reputacija finansijske institucije
- troškovi, finansijski rezultat, likvidnost i solventnost finansijske institucije
- rizičan profil finansijske institucije
- kvalitet usluga koje finansijska institucija pruža klijentima

Organizacije su u obavezi da pre sklapanja ugovora o poveravanju aktivnosti provođaju sledeće provere:

- detaljna analiza potencijalnog pružaoca usluga koja se odnosi na njegovu sposobnost pružanja usluga, finansijsko stanje i poslovnu reputaciju

- utvrdi da li propisi države ili država u kojima potencijalni pružalac usluga posluje omogućuju Narodnoj banci Srbije nesmetano vršenje kontrole tog poslovanja u delu koji se odnosi na obavljanje poverljivih aktivnosti ili je u vezi sa tim aktivnostima
- proceni moguće poteškoće i vreme potrebno za izbor drugog pružaoca usluga, ili mogućnost nastavka obavljanja tih aktivnosti unutar finansijske organizacije u slučaju prestanka pružanja ugovorenih usluga, kao i da s tim u vezi donese odgovarajuću izlaznu strategiju.

Finansijska institucija dužna je da Narodnoj banci Srbije omogući nesmetano vršenje kontrole poverljivih aktivnosti, odnosno nadzora nad njima. Ovo podrazumeva i neposrednu kontrolu obavljanja poverljivih aktivnosti u prostorijama pružaoca usluga, odnosno na lokaciji na kojoj se poverene aktivnosti obavljaju. Organizacija je dužna da obezbedi da pružalac usluga njoj, Narodnoj banci Srbije, ili spoljnom revizoru obezbedi blagovremen i neograničen pristup dokumentaciji, podacima, prostorijama odgovornim licima i delu poslovanja u vezi sa poverenim aktivnostima.

Organizacija je dužna da obezbedi da se poveravanjem aktivnosti ne ugrozi bezbednost ili funkcionalnost informacionog sistema, kao i da podaci finansijske institucije ostanu u njenom posedu. Svi učesnici u ovom poslu dužni su da postupaju u skladu sa zakonom o zaštiti podataka o ličnosti, kao i sa drugim propisima kojima se uređuje čuvanje tajne nastale u poslovanju finansijskih institucija.

U slučaju namere da promeni pružaoca usluga, organizacija je dužna da o tome obavesti Narodnu banku Srbije najkasnije 30 dana pre planiranog poveravanja aktivnosti, odnosno planirane promene. Ovo se naročito odnosi na:

1. odluku nadležnog organa finansijske institucije o poveravanju aktivnosti, odnosno o promeni pružaoca usluga
2. opis aktivnosti koje finansijska institucija namerava da poveri, kao i obaveza i uslova koje je pružalac usluga dužan da ispuni
3. osnovne podatke o pružaocu usluga
4. rezultat detaljne analize pružaoca usluga
5. izlaznu strategiju u slučaju prekida ugovora sa pružaocem usluga

Za pružaoce usluga koji imaju sedište izvan Republike Srbije ili se poverena aktivnost obavlja van granica naše zemlje Narodnoj banci Srbije potrebno je dostaviti dokaz o tome da propisi države, odnosno država o kojima se radi omogućavaju Narodnoj banci Srbije nesmetano vršenje neposredne kontrole tog poslovanja u delu koji se odnosi na obavljanje poverljivih aktivnosti ili je u vezi sa njima.

Ukoliko pružalac usluga poverava njemu poverenu aktivnost drugim licima, on to može uraditi samo uz prethodnu saglasnost finansijske institucije u svakom pojedinačnom slučaju. O ovakvoj promeni organizacija obaveštava Narodnu banku Srbije odmah po davanju saglasnosti.

Delegirane poslove lice kome su oni povereni može početi da obavlja tek nakon 15 dana od dana davanja saglasnosti.

Finansijska institucija odgovara u celini za poslove koje je poverila pružaocima usluga.

Ukoliko u kontroli Narodna banka Srbije otkrije neke nepravilnosti u radu pružaoca usluga, ona može naložiti organizaciji da raskine ugovor o poveravanju aktivnosti.

4.8 Elektronsko bankarstvo

Ovaj deo odluke odnosi se isključivo na banke koje i jedine u opisu svog posla imaju ovakvu delatnost. Banke su dužne da kao deo upravljanja rizikom informacionog sistema uspostave i uključe i proces upravljanja rizicima koji proizilaze iz elektronskog bankarstva. Dobre smernice bankari mogu naći u dokumentim bazelskog komiteta poput dokumenta “Risk Management Principles for Electronic Banking” [20].

Banka je dužna da u poslovima elektronskog bankarstva primeni sigurne i efikasne metode za proveru i potvrdu identiteta i ovlašćenja lica, procesa i sistema.

Autentifikacija korisnika u okviru elektronskog bankarstva mora biti minimalno dvofaktorska, tj. da uključuje minimum dva elementa za potvrđivanje korisničkog identiteta (npr. lozinka i sertifikat). Takođe, banka je dužna da obezbedi obostranu autentifikaciju kako bi i korisnici mogli da provere autentičnost banke.

Banka je dužna da obezbedi postojanje odgovarajućih i operativnih zapisa kako bi se obezbedila neporecivost i dokazivost radnji u vezi sa elektronskim bankarstvom.

Kako je ovaj deo bankarskog poslovanja vrlo osetljiv po pitanju sigurnosti dobru praksu i odgovornost ka klijentima banke mogu demonstrirati i usklađivanjem sa međunarodnim standardom PCI-DSS koji se bavi bezbednim upravljanjem osetljivim podacima na platnim i kreditnim karticama[19].

5. Međunarodni standardi i iskustva

5.1 O standardima

Sami standardi organizacijama daju putokaz u kom smeru treba ići i nijedan od standarda ne nudi kompletno rešenje svih problema, zato se od organizacija očekuje da izvrše analize ponuđenih standarda i na osnovu njih za svoju organizaciju usvoje one savete koji su im najprikladniji.

Često je mišljenje da je uvođenje standarda skupo i neefikasno, što može biti slučaj ukoliko se ono tretira samo kao tehničko uputstvo bez da je stvarno ušlo u sam rad organizacije.

Ukoliko se pak standardi uvode pažljivo i ciljano tamo gde će dati najbolje efekte, onda su i rezultati bolji, a samim tim i mišljenje o standardima se menja na bolje.

Najbolja praksa koja je sadržana u ovakvim standardima organizaciji bi trebalo da pruži sledeće prednosti:

- Bolje upravljanje IT
- Efikasniji povraćaj IT investicija
- Lakše usklađivanje sa raznim regulativama
- Definisanje kompleksnih rizika na različitim nivoima IT
- Efiksano upravljanje polisama i procedurama
- Viši nivo pouzdanosti i sigurnosti sistema
- Povećan ugled i poverenje partnera i drugih interesnih strana

Od ključnog značaja za uspeh implementacije standarda jeste upoznavanje viših menadžment struktura sa njima.

Od mnoštva standarda koji se nude na tržištu sama odluka Narodne banke Srbije direktno ne referencira nijedan od njih, ali se paralele mogu naći u kombinaciji sledećih standarda i frejmorka:

1. CobiT, otvoren standard i skup najboljih saveta za upravljanjem IT organizacijama datih u formi šta treba da urade kako bi postigli željeni efekat;
2. ISO/IEC 38500 okvir za korporativno upravljanje i menadžment IT-a;
3. ITIL, skup najboljih saveta za IT podršku i upravljanje servisima organizacije dat u formi kako se šta radi da bi se postigli željeni ciljevi;
4. ISO/IEC 20000 standard za upravljanje IT servisima;
5. ISO 2700x serija standarda koji se bave bezbednošću informacionih sistema i dr.
6. ISO 22301 standard koji se bavi upravljanjem kontinuitetom poslovanja
7. ISO 27013 standard koji se bavi smernicama o integrisanoj primeni ISO 27001 i ISO 20000 standarda

5.2 CobiT

CobiT je globalno prihvaćen IT frejmork za upravljanje IT sistemom sastavljen na temeljima industrijskih standarda i najbolje prakse. CobiT omogućava izvršnim članovima da imaju bolji uvid u rad i upravljanje IT na visokom nivou. CobiT obezbeđuje uvid u IT aktivnosti i olakšava upravljanje investicijama u toku čitavog životnog ciklusa[7].

Kako je CobiT skup internacionalno prihvaćenih alata i tehnika, njegova implementacija ukazuje na dobro uređenu organizaciju. IT menadžmentu olakšava prezentaciju njihovog poslovanja višem menadžmentu.

Prihvatanje CobiTa donosi sledeće predosti:

- IT osoblje i rukovodioci imaju bolji uvid u spregu biznisa i IT
- Cena koštanja IT postaje transparentnija i predvidiva
- Nivo isporučenih usluga IT je viši
- Kvalitet IT servisa i projekata je viši
- Sigurnost i privatnost su vidljiviji i lakše upravljivi
- IT rizicima se lakše upravlja
- Monitoring je efikasniji
- IT komplajans postaje uobičajena praksa

Sam CobiT u verziji 4.0 uključuje sledeće:

- Frejmork – set od 34 kontrolna objekta po jedan za svaki IT proces, grupisani u četiri domena: Planiraj i Organizuj, Pribavi i Implementiraj, Isporuči i Podrži, i Nadgledaj i Evaluiraj.
- Opis procesa – deklarisanje biznis i IT odgovornosti za svaki od 34 navedena IT procesa
- Kontrolni ciljevi – generički najbolji saveti za upravljanje IT procesima
- Saveti za upravljanje – alati za delegiranje odgovornosti i merenje performansi
- Modeli zrelosti – omogućuje određivanje nivoa zrelosti IT odeljenja

COBIT – upravljački okvir:

- Strateško uskladjivanje (Strategic alignment)– osigurati povezanost korporativnih i IT planova, definisanje i kontrola vrednosti investicija.
- Ostvarivanje vrednosti (Value delivery) – kroz IT strategiju i pracenje izvršavanja projekata, obezbeđuje stvaranje poslovnih vrednosti, koncentrišući se na optimizaciju troškova i povećanje efikasnosti.
- Upravljanje resursima (Resource management) – odnosi se na optimalno ulaganje, pravilno upravljanje kritičnim IT elementima: aplikacije, informacije, infrastruktura i ljudi.
- Upravljanje rizicima (Risk management) – upravljanje najvažnijim

rizicima od strane zaposlenih i menadžmenta, indentifikacija najopasnijih rizika po poslovanje i kreiranje akcionog plana za slučaj njegovog ostvarivanja.

- Merenje performansi (Performance measurements) – merenje nivoa usklađenosti rezultata sa strategijom, uspešnosti projekata, korišćenja resursa, procesa rada i pružanja usluga.

5.3 ISO 38500

ISO 38500 je međunarodni standarda za korporativno upravljanje informacionim tehnologijama. Cilj mu je efikasno upravljanje informacionim sistemima, kao i uspostavljanje jačih veza sa rukovodstvom kroz približavanje i upoznavanje rukovodstva sa radom informacionih sistema i njihovim obavezama i odgovornostima prema njemu[8].

5.4 ITIL

Uslovljenost informacionim tehnologijama kompanije navodi na potrebu za što efikasnijim i kvalitetnijim IT servisima. Biznis od IT-ja zahteva sledeće:

- da u potpunosti odgovori na biznis i korisničke zahteve
- da je u saglasnosti sa pravnim i drugim regulativama
- da je efikasno isporučen
- da je konstantno nadgledan i poboljšavan

ITIL IT menadžmentu obezbeđuje skup saveta i najbolje prakse iz koje je proizašla metodologija sa sledećim zadacima[9]:

- Skup procesa za isporučivanje i podržavanje IT usluga, opisanih u biblioteci IT infrastrukture.
- ITIL - *de facto* standard najbolje prakse u isporuci IT usluga, koji promoviše poslovnu efektivnost i efikasnost.
- Vođenje IT kao biznisa koji je sposoban da upravlja troškovima, kvalitetom i rizikom IT usluga
- Povezivanje IT usluga, radne snage, tehnologije i menadžmenta IT procesima u sistem
- Planiranje organizacionog preuređenja
- Identifikacija područja primene tehnologija koje omogućavaju procesni pristup
- Identifikacija sopstvenih slabosti i prednosti, benchmarking
- Odluka o “outsourcing”-u
- Upravljanje životnim ciklusom IT usluga

Procesi i funkcije koje ITIL uređuje su:

- Service Portfolio Management (upravljanje portfeljom usluga)
- Service Level Management (upravljanje nivoom usluga),
- Incident Management (upravljanje incidentima),
- Change Management (upravljanje promenama),
- Demand Management (upravljanje potražnjom),
- Business Relationship Management (upravljanje poslovnim odnosima)
- Financial Management (finansijsko upravljanje),
- Service Catalogue Management (upravljanje katalogom usluga),
- Availability Management (upravljanje raspoloživošću),
- Capacity Management (upravljanje kapacitetima),
- Supplier Management (upravljanje radom dobavljača),
- Information Security Management (upravljanje bezbednošću informacija),
- IT Service Continuity Management (upravljanje kontinuitetom rada usluga),
- Service Asset and Configuration Management (upravljanje osnovnim sredstvima usluge i konfiguracijom),
- Release and Deployment Management (upravljanje izdanjima i primenom),
- Event Management (upravljanje događajima),
- Problem Management (upravljanje problemima),
- Request Fulfilment (ispunjavanje zahteva),
- Access Management (upravljanje dostupnošću),
- The “7 step” improvement process (proces poboljšanja u „7 koraka”)

5.5 ISO 20000 standard

ISO 20000 standard, razvijen 2005. godine, koristi se kao pomoć organizacijama da steknu uvid u kvalitet usluga koje isporučuju, definišu sve procese i stvore sliku o tome šta bi trebalo unaprediti radi povećanja kvaliteta usluga. Standard je nastao iz standarda BS 15000.

Standard ISO/IEC 20000 sastoji se od nekoliko dokumenata koji govore o različitim aspektima upravljanja IT uslugama[10]:

- **ISO/IEC 20000-1:2011** (*Part 1: Service management system requirements*) bliže opisuje sistem upravljanja uslugama. Njime su obuhvaćeni svi zahtevi koje bi organizacija trebalo da ispuni u cilju planiranja, uspostavljanja, primene, sprovođenja, nadgledanja, revidiranja, održavanja i poboljšavanja Service Management sistema. Standard sadrži ukupno 256 zahteva, podeljenih u šest grupa, a koji se odnose na dizajn, promenu, isporuku u poboljšanje usluga.
- **ISO/IEC 20000-2:2012** (*Part 2: Guidance on the application of service management systems*) sadrži uputstvo za primenu SMS-a, na osnovu zahteva opisanih u ISO 20000-1.

Sadrži primere i predloge primene sistema i omogućava organizacijama da na što verodostojniji način interpretiraju i primene ISO 20000-1.

- **ISO/IEC TR 20000-3:2009** (*Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1*): Odnosi se na definisanje obima i primenljivosti ISO/IEC 20000-1 standarda u određenoj organizaciji. Dopunjuje dokument ISO 20000:2, koji sadrži opšta iskustva i može pomoći, kako organizacijama koje posluju prema navedenom standardu, tako i organizacijama koje su zainteresovane da uvedu standard ISO 20000-1 u svoje poslovanje.
- **ISO/IEC TR 20000-4:2010** (*Part 4: Process reference model*) bliže opisuje i olakšava primenu modela procene procesa, opisanog standardom ISO/IEC 15504. Model opisan ovim standardom je logičan prikaz elemenata procesa u okviru upravljanja uslugama koji se mogu sprovoditi na osnovnom nivou. On opisuje sve procese na apstraktnom nivou, uključujući i procese SMS-a opisanih ISO 20000-1 standardom, u vidu osnovne svrhe i izlaznih elemenata.
- **ISO/IEC TR 20000-5:2010** (*Part 5: Exemplar implementation plan for ISO/IEC 20000-1*) predstavlja primer plana implementacije, koji daje bliža uputstva kako primeniti SMS u cilju ispunjavanja zahteva opisanih ISO 20000-1 standardom. Obuhvata savete u vezi sa time kojim redom bi trebalo planirati i primeniti poboljšanja. Takođe, opisuje pristup koji se sastoji od tri faze i koji se koristi prilikom primene SM sistema.

5.6 ISO 2700x standardi

ISO serija standarda 2700x bavi se pitanjima sigurnosti informacionih sistema i to u domenima poverljivosti, dostupnosti i integriteta informacija kroz definisanje i uvođenje mehanizama zaštite. Cilj serije standarda ISO 2700x je identifikacija rizika po bezbednost informacija i uspostavljanje mehanizama za njihovo eliminisanje ili svođenje na prihvatljiv nivo[11].

Prednosti koje donosi uvođenje ISO standarda serije 2700x je:

- Konkurentska prednost
- Smanjenje rizika od uništenja, oštećenje i gubitka informacija
- Usaglašenost sa važećim zakonskim propisima
- Veće poverenje klijenata, zaposlenih, saradnika i dr.
- Postojanje odgovornosti za bezbednos informacija od strane svih na svim nivoima u organizaciji

Serijski standardi podrazumeva sledeće standarde:

- ISO 27000 – Rečnik termina koji se koriste u ISO 27000 seriji standarda;
- ISO 27001:2005 – Sistem upravljanja informacionom sigurnošću;

- ISO 27002:2007 – Kodeks postupaka za upravljanje informacionom sigurnošću;
- ISO 27003 – Vodič za implementaciju sistema za upravljanje informacionom sigurnošću;
- ISO 27004 – Merenje i metrike efikasnosti sistema informacione sigurnosti;
- ISO 27005 – Upravljanje rizicima informacione sigurnosti;
- ISO 27006:2007– Zahtevi za postupkom analize i sertifikovanja standarda;
- ISO/IEC 27007 – Smernice za reviziju upravljanja bezbednošću informacionih sistema;
- ISO/IEC 27011 — Smernice za upravljanje Informacionom bezbednošću telekomunikacionih organizacija;
- ISO/IEC 27033-1 – Pregled i koncepti sigurnosti u mrežama;
- ISO 27799 – Upravljanje sigurnošću u zdravstvu.

5.7 ISO 22301 standard

Ovaj standard pomaže organizacijama da uspostave sistem upravljanja kontinuitetom poslovanja (BCM) tako da su u mogućnosti da na najefikasniji način reaguju na potencijalne prekinde u radu. Uspostavljanje sistema za upravljanje kontinuitetom poslovanja podrazumeva kreiranje analize uticaja na poslovanje (BIA) u kojoj se identifikuju svi kritični procesi, aktivnosti i resursi potrebni za normalno funkcionisanje sistema. Kvalitetno uspostavljen sistem omogućuje uvid u to kakav uticaj imaju kvarovi u detektovanim kritičnim oblastima i olakšava planiranje raznih sa tim povezanih scenarija[12].

Zahtevi u ovom standardu su generički i namenjeni različitim tipovima organizacija.

5.8 ISO 27013 standard

Ovaj standard obezbeđuje savete za korišćenje standarda za informatičku bezbednost i upravljanje pružanjem usluga. Standard podrazumeva usvajanje dva standarda, ISO 27001 i ISO 20000-1[13].

Prednosti integrisanog usvajanja ovih standarda su:

- Ostavljanje utiska na saradnike u domenu pouzdanosti i sigurnosti servisa
- Smanjenje cene integrisanjem projekata
- Skraćivanje vremena potrebnog za implementaciju kroz integraciju zajedničkih procesa standarda
- Eliminisanje nepotrebnih dupliciranja

- Ojačavanje razumevanja između osoblja zaduženog za menadžment servisa i osoblja zaduženih za sigurnost

5.9 Bazel 2

Slučajevi poput Britanske Barings banke iz 1995. u kom je jedna jedina osoba uspela da prevarnim radnjama ošteti banku za čitavih milijardu dolara uzburkao je javnost i po nekim ekspertima ukazao na očigledan nedostatak kontrole i upravljanja rizicima u banci.

Činjenica da se u danas u bankarskim sistemima širom sveta odvijaju milionske transakcije svakog sata, većina njih oslanjajući se na polu ili u potpunosti automatske sisteme (klirinške kuće, ATM mreže...) svakako ukazuje na potrebu da ovakvi sistemi budu u potpunosti sigurni i funkcionalni.

Internacionalna saradnja olakšavajući poslovanje na scenu donosi i problem dostupnosti podacima mnogo većoj publici, a samim tim uvećavajući nivo izloženosti potencijalnim rizicima.

Bazel 2 standardi predloženi 1999. godine, usvojeni 2004, a obavezujući standardi u zemljama Evropske unije od 2007. godine u mnogome pomažu u procesu upravljanja rizicima[14].

U okviru Bazel komiteta postoji i deo zadužen za superviziju banaka (Basel Committee on Banking Supervision – BCBS) koji se bavi pitanjima koja se tiču usklađivanja Bazel 2 standarda sa zahtevima supervizije banaka.

Bazel 2 standard pomaže bankama u borbi protiv operativnih i finansijskih rizika tako što definiše set strogih zahteva koji za cilj imaju obezbeđivanje dovoljnih rezervi kapitala..

Bazel 2 standard u osnovi čine tri „stuba“ :

Stub 1 definiše minimalne kapitalne zahteve za kreditni, tržišni i operativni rizik, uz mogućnost korišćenja sofisticiranih modela i tehnika za njihovo izračunavanje

Stub 2 učvršćuje vezu između optimalnih kapitalnih zahteva i vrste i stepena rizika kojima je banka izložena u svom poslovanju, uvodeći proces interne procene adekvatnosti kapitala (ICAAP) i jačajući proces supervizije

Stub 3 upotpunjuje vezu između Stuba I i Stuba II, ističući značaj tržišne discipline uvođenjem minimalnih zahteva za objavljivanje informacija banaka.

U okviru ovih „stubova“ standard je adresirao nekoliko po sigurnost ključnih elemenata:

Interni podaci – Po Bazelu 2 (paragraf 670 i 671), praćenje događaja koji se tiču gubitka podataka je neophodna mera u cilju razvijanja kredibilnog sistema za kontrolu operativnog rizika. Gubici podataka povezanih sa poslovnom aktivnošću banke, moraju biti dokumentovani...

Objavljivanja – (paragraf 810) sugerise da se formiranjem frejmorka o objavljivanju bančinih rizika postiže bolja vidljivost.

Privatne i poverljive informacije – (paragraf 819) Privatne i poverljive informacije (informacije o proizvodima, sistemima, klijentima), tj. njihovo objavljivanje moraju se definisati posebnim aktom koji je odobrio top menadžment.

Bazel 2 od banaka zahteva razvoj frejmorka za upravljanje rizicima i to posebno u oblastima:

- Integriteta podataka
- Prevencije neautorizovanih promena na softveru
- Obezbeđivanja pravljenja sistemskih rezervnih kopija
- Implementacije konntinutranog poslovanja (plan oporavka)

5.10 Bazel 3

Bazel 3 donosi proširenja u domenu solvency and liquidity koji ima za cilj da obezbedi bankama dovoljan kapital za povraćaj depozita u slučaju krize i (are able to survive a protracted liquidity freeze, and are less dependent on the vagaries of short-term credit markets).

Promene koje očekuju IT sisteme usled usklađivanja sa Bazelom 3 očekuje se da budu srednjeg intenziteta bez potrebe za tektonskim poromenama u postojećim sistemima, pogotovo onim koji su već izvršili usklađivanje sa standardom Bazel 2.

5.11 Međunarodna iskustva

Iskustva zemalja iz okruženja obilato su korišćenja u pisanju Odluke NBS pa se analizama rada njihovih odeljanja za superviziju mogu naslutiti pravci i metodologije obavljanja ovog ni malo jednostavnog posla od strane novoformirane službe NBS[15].

6. Zaključak

Raznolikost samih finansijskih organizacija, kao i kompleksnost pojedinačnih sistema čini izazovnim sve pokušaje da se naprave univerzalna pravila kojima bi se obuhvatili svi saveti i uputstva, a koja bi na jednom mestu autoritativno i univerzalno ispunila očekivanja svih njih.

Smernice date u ovom radu sugerišu određene standarde, tehnologije ili proizvode koji se mogu koristiti prilikom usklađivanja sa konkretnim zahtevima iz Odluke NBS.

Skup saveta i smernica koje ova odluka nudi stavlja pred prosečnu organizaciju velike izazove kako u pogledu operativnih akcija, tako i u finansijskom smislu jer se većina ovih tehnologija kotira kao sofisticirana i svrstava u red skupih tehnologija.

Finansijske institucije iz velikih grupacija će svakako pomoć potražiti u okviru grupe, maksimalno koristeći intelektualnu svojinu, iskustva i hardverske resurse koji su im na raspolaganju. S obzirom na to da se matične kuće većine finansijskih organizacija nalaze u zemljama evro zone, logično je da one poseduju iskustvo i resurse potrebne za u Odluci navedene oblasti poslovanja.

Pred posebnim izazovom naći će se manje organizacije poput lizing kuća, penzionih fondova i osiguravajućih zavoda jer se uglavnom radi o organizacijama sa malim brojem zaposlenih u sektoru informacionih tehnologija. Većina spominjanih standarda pisana je generički, ali implicitno sugeriše na strukture koje broje mnogo više od nekoliko osoba u odeljenjima informacionih tehnologija. Cena samih tehnologija takođe će predstavljati problem za manje organizacije, stoga će one verovatno posegnuti besplatnim i open source rešenjima kao i outsourcingom u svim segmentima u kojim je to moguće.

Trendovi koji su poslednjih godina sve izraženiji takođe idu u prilog outsourcingu servisa i usluga iz oblasti informacionih tehnologija pa je samim tim i ponuda u ovom segmentu veoma kvalitetna. Ulaskom velikih kompanija na ovo tržište podignut je i kvalitet samih usluga pa se one mogu razmatrati čak i u segmentu finansijskih institucija koji je inače tradicionalno zatvoren i veoma nepoverljiv.

Jedna od ključnih poruka koje Odluka NBS ne donosi jeste da se u procese upravljanja informacionim tehnologijama moraju uključiti i gornji upravljački slojevi (top management) kako bi se samim procesima dalo na težini i ozbiljnosti u čitavoj organizaciji. Potencijalni problem je to što se odredbe odluke koje se odnose na top management kompanije ne navode direktno i u meri u kojoj bi to bilo neophodno tako da će se u većini organizacija ovaj dokument ticati isključivo ili ponajviše sektora za informacione tehnologije. Uključivanjem top managementa u proces upravljanja informacionim sistemima finansijskih institucija dobilo bi se na boljoj vidljivosti same službe, kao i na efikasnijem učinku u procesu uključivanja svih zaposlenih u sistem.

Bezbednost nije moguće postići samo uređajima već se ona mora obezbediti kroz slojevit pristup i uvođenjem sigurnosti kao kontinuiranog procesa. U ovom procesu tehnika igra samo sporednu ulogu, dok ključ uspeha leži u ljudima i njihovoj želji, odnosno odluci da se u ovaj proces aktivno uključe. Definisanje procedura i uputstava čini prvi korak, dok je drugi na onima kojima su ta uputstva namenjena.

Bitan faktor u cilju podizanja nivoa svesti i održavanja dobre informisanosti čine i redovni treninzi-predavanja koja je potrebno sprovoditi širom organizacije a koji bi trebalo da obezbede pregled aktuelnih sigurnosnih rizika i načina na koji se oni mogu ublažiti ili zaobići.

Priroda okruženja u kojima posluju finansijske organizacije, kao i aktuelni svetski trendovi, od stručnjaka u informacionim tehnologijama zahtevaju konstantno usavršavanje i prilagođavanje novonastalim situacijama i izazovima stoga su stručni seminari, webinar, specijalistički kursevi i razmena mišljenja među kolegama iz struke neophodan elemenat svakog uspešnog sistema.

Trenutna tumačenja Odluke NBS finansijske institucije obavljaju na osnovu samostalnog tumačenja ili tumačenja spoljnih revizora koji su im pomagali u tom poslu. Od novoformiranog odeljenja za superviziju pri Narodnoj banci Srbije se očekuje da dodatnim pojašnjenjima ili kroz praktične akcije u budućim kontrolama institucijama ukažu na metodologiju svog rada i lična tumačenja sadržine svoje Odluke. Finansijskim institucijama ostaje da ovaj posao usklađivanja privedu kraju, to jest novom početku kontinuiranog usklađivanja i da se u narednom periodu upoznaju sa novoformiranom službom za superviziju informacionih sistema Narodne banke Srbije, koja će im na ovom putu biti nezaobilazni kreativni faktor, a nadamo se ne i prepreka.

7. Literatura

- [1] Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, Službeni glasnik RS br. 23/2013
- [2] National Institute of Standards and Technology, SP 800-30 Risk Management Guide for Information Technology Systems, <http://csrc.nist.gov/publications/>
- [3] National Institute of Standards and Technology, SP 800-100 Information Security Handbook: A Guide for Managers, <http://csrc.nist.gov/publications/>
- [4] National Institute of Standards and Technology, SP 800-61 Rev-1 Computer Security Incident Handling Guide, <http://csrc.nist.gov/publications/>
- [5] National Institute of Standards and Technology, SP 800-92 Guide to Computer Security Log Management, <http://csrc.nist.gov/publications/>
- [6] National Institute of Standards and Technology, SP 800-83 Guide to Malware Incident Prevention and Handling, <http://csrc.nist.gov/publications/>
- [7] Control Objectives for Information and Related Technology (COBIT), <http://www.isaca.org/COBIT/Pages/default.aspx>
- [8] ISO 38500 standard http://www.iso.org/iso/catalogue_detail.htm?csnumber=51639
- [9] The Information Technology Infrastructure Library (ITIL), <http://www.itil-officialsite.com/>
- [10] ISO 20000 standard <http://www.kvalitet.org.rs/standardi/iso-iec-20000>
- [11] ISO 2700x standardi <http://www.27000.org/>
- [12] ISO 22301 standard http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1602
- [13] ISO 27013 standard <http://www.iso27001security.com/html/27013.html>
- [14] Basel Committee on Banking Supervision www.bis.org
- [15] Circular for defining and achieving security standards for the information system of a bank, Nacionalna banka Makedonije <http://www.nbrm.mk/?ItemID=29E450138F24D145B42A0B141F3D2122>
- [16] Business Continuity Institute, The Good Practice Guidelines <http://www.thebci.org/index.php/resources/the-good-practice-guidelines>

[17] National Institute of Standards and Technology, SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, <http://csrc.nist.gov/publications/>

[18] National Institute of Standards and Technology, SP 800-34 Contingency Planning Guide for Information Technology Systems, <http://csrc.nist.gov/publications/>

[19] PCI Security Standards Council, PCI-DSS v3.0, <https://www.pcisecuritystandards.org>

[20] Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking www.bis.org

Prilog 1. Tabela akcija potrebnih za usklađivanje sa Odlukom NBS

Okvir za upravljanje IS		
1. Uspostaviti adekvatan informacijski sistem		
2. Uspostaviti proces upravljanja informacijskim sistemom (radi smanjenja izloženosti rizicima i bezbednosti)	Usklađivanje rada IT sektora sa nekim od međunarodno priznatih frejmorka ili standarda kao što su: ITIL, COBIT, ISO 38500, ISO 20000...	
3. Doneti strategiju razvoja informacijskog sistema u skladu sa strategijom poslovanja	Konsultovati strategiju poslovanja ukoliko postoji ili je definisati i na osnovu nje definisati strategiju razvoj.	
a. dužna da po potrebi menja ovu strategiju	Uvesti monitoring i kontrolu promena.	
4. Obezbediti adekvatnu organizacionu strukturu (jasna podela poslova i dužnosti, utvrđene unutrašnje kontrole kojima se sprečava sukob interesa)	Uskladiti organizacionu šemu u skladu sa potrebama i mogućnostima. Izdvojiti sektor za bezbednost informacijskog sistema od sektora informacijskih tehnologija.	
5. Obezbediti primenu svih unutrašnjih opštih akata i procedura u vezi sa informacijskim sistemom i informisati korisnike sa sadržajem	Interna kontrola upravljanja procesima. Definisano standardom ISO 9001 ukoliko ga kompanija analizira. Korisnicima obezbediti konstantan pristup svom sadržaju koji se tiče njihovog domena rada. Sadržaj je moguće objaviti upotrebom internih portala, deljenih mrežnih foldera ili specijalizovanim aplikacijama.	
6. Usvojiti odgovarajuću metodologiju upravljanja projektima u vezi sa informacijskim sistemom	Koristiti PMBOK Guide dokument američkog Projekta Menadžment instituta PMI koji je međunarodno prihvaćen kao ANSI standard, ili definisati svoju sopstvenu metodologiju na osnovu dosadašnje prakse vođenja projekata. Neki od softvera za upravljanje projektima su HP Project and Portfolio Management Center, Microsoft Office Project, Oracle Primavera Enterprise Project Portfolio Management i dr.	
7. Utvrditi kriterijume, način i postupke izveštavanja svog nadležnog organa o relevantnim činjenicama u vezi sa funkcionalnošću i bezbednošću informacijskog sistema	Analizirati formu i interval izveštavanja NBS preko javnih glasila i sajta NBS.	
Upravljanje rizikom IS		
8. Uspostaviti proces upravljanja rizicima	Uspostaviti kontinuirani proces upravljanja rizikom celokupnog informacijskog sistema i svih IT resursa. • detaljan opis, identifikacija i upravljanje rizicima • analiza i prevazilaženje rizika Od softverskih alata moguće je koristiti platforme za upravljanje, rizike i komplejns (GRC)	

		kao što su: EMC RSA Archer GRC, IBM OpenPages GRC, SAP Risk Management, Wynyard Risk Management.	
	Unutrašnja revizija informacionog sistema		
	9. Obuhvatiti kriterijume, način i postupke unutrašnje revizije zasnovane na rezultatima procene rizika	Organizovati internu reviziju u skladu sa međunarodnim standardima i domaćom regulativom kojom se uređuje ova oblast. Način rada i kriterijume revizije definisati na osnovu procene rizika.	
	10. Unutrašnja revizija obavlja se u skladu sa propisima kojima se uređuje poslovanje FI		
	Bezbednost IS		
	11. Doneti Politiku bezbednosti informacionog sistema	Doneti politika za upravljanje bezbednošću informacija ili Information security management system (ISMS) kao krovni dokument sektora koji se bavi bezbednošću informacionog sistema. Dokument se usklađuje prema standardima: • ISO 27001 • ISO 27002 • ISO 13335-1 • Zakon o zaštiti podataka o ličnosti • Zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine • Zakon o elektronskom potpisu • Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala • Krivični zakon Zakon Na ISMS politiku se nadovezuju bezbedonosne politike i procedure iz oblasti koje su od interesa za zaštitu.	
	12. Upravljanje bezbednošću uspostaviti kao kontinuirani proces	Definisanje organizacionog dela koji je zadužen za bezbednost. Redovnim revidiranjem i usklađivanje sa akuelnim zakonima, propisima i dobrom praksom.	
	13. Izvršiti klasifikaciju informacionih dobara	Utvrditi stepen osetljivosti i kritičnosti informacija u kontekstu njihove poverljivosti, integriteta i raspoloživosti. Na osnovu ovih informacija definisati adekvatan nivo zaštite. Na praviti matricu i identifikovati vlasnike, čuvare i korisnike dokumenata kako bi se kasnije olakšala analiza kretanja informacija i naglasila odgovornost za korisnike informacija.	
	14. Sprovesti odgovarajuću kontrolu pristupa resursima IS	Uspostaviti adekvatne kontrole pristupa: • kroz evidentiranje korisnika • autorizaciju • identifikaciju	

		• autentifikaciju • nadzor nad korisničkim pravima pristupa Softveri koji omogućuju ove funkcije su Microsoft Active Directory, IBM Security Identity and Access Manager, Dell Quest One Identity Suite, CA IdentityMinder i dr.	
	15. Uspostaviti adekvatan sistem nadgledanja sistema i generisanja operativnih i sistemskih zapisa	Automatizovati sakupljanje, analizu i čuvanje zapisa u cilju što identifikacije problema, rekonstrukcije događaja, otkrivanja neovlašćenih aktivnosti i utvrđivanja odgovornosti. Sami zapisi trebalo bi da budu takvi da mogu da posluže kao relevantni dokaz pred nadležnim organima i u slučaju pokretanje eventulanih sudskih sporova. Neki od softvera koji pokrivaju ovaj zahtev su HP ArchSight, IBM QRadar, Symantec Security Information Manager, McAfee Enterprise Security Manager, Tripwire, Splunk i dr.	
	16. Zaštiti resurse IS i dr. sistem koji su podrška funkcionisanju IS od neovlašćenog fizičkog pristupa, krađe i uništenja	Upotrebiti sve adekvatne mere fizičke zaštite u cilju obezbeđivanja resursa informacionog sistema uključujući i zaštitu od štetnih uticaja iz okruženja.	
	17. Zaštiti resurse IS od malicioznog koda	Upotrebiti odgovarajuće uređaje ili softverske aplikacije na adekvatnim mestima na kojima postoji potencijalna opasnost od malicioznog koda. • Mail serveri • Serveri • Radne stanice • Mobilni uređaji • Internet linkovi • Eksterni linkovi Vrši redovne analize ranjivosti sistema. Definirati upravljanje ažuriranjem uređaja i sistema. Uvesti uređaje za detekciju i prevenciju upada (IDS/IPS) kao i Next generation firewall uređaje. Neki od uređaja i vendora su: Cisco(ASA, IronPort, IPS i ISE), HP TippingPoint, CheckPoint, FireEye, Symante, McAfee i dr.	
	Upravljanje kontinuitetom poslovanja i oporavak u slučaju katastrofa		
	18. Uspostaviti proces upravljanja kontinuitetom poslovanja	Izvršiti analizu uticaja na poslovanje i procenu rizika (Business impact analysis BIA) • utvrđivanje resursa i sistema potrebnih za odvijanje pojedinačnih poslovnih procesa, kao i njihove međuzavisnosti i povezanosti; • procenu rizika u vezi sa pojedinačnim	

		poslovnim procesima, uključujući i verovatnoću nastanak neželjenih događaja i njihov potencijalni uticaj na kontinuitet poslovanja, finansijsko stanje i reputaciju finansijske institucije; • utvrđivanje prihvatljivog nivoa rizika i tehnika za ublažavanje identifikovanih rizika; • utvrđivanje najdužeg prihvatljivog prekida (MAO) pojedinačnih poslovnih procesa; • utvrđivanje kritičnih/ključnih poslovnih procesa i aktivnosti.	
	19. Usvojiti strategiju oporavka	Usvojiti sledeće tačke: • prioritete oporavka poslovnih procesa, kao i resursa i sistema potrebnih za njihovo odvijanje • ciljne nivoe aktivnosti (SDO) • ciljna vremena oporavka (RTO) • ciljne tačke oporavka (RPO)	
	20. Doneti plan kontinuiteta (Business Continuity Plan)	Definisati plan koji naročito sadrži: • opis procedura u slučaju prekida poslovanja • ažuran spisak svih resursa neophodnih za ponovno uspostavljanje kontinuiteta poslovanja • podatke o timovima koji će biti odgovorni za ponovno uspostavljanje poslovanja u slučaju nastanka nepredviđenih događaja i o imenovanim članovima tih timova, uključujući i njihove jasno utvrđene dužnosti i odgovornosti, kao i plan unutrašnjih i spoljašnjih linija komunikacije • rezervnu lokaciju u slučaju prekida poslovanja i nemogućnosti ponovnog uspostavljanja poslovnih procesa na primarnoj lokaciji	
	21. Doneti plan oporavka aktivnosti u slučaju katastrofa (Disaster Recovery Plan)	Definisati plan koji naročito sadrži: • procedure za oporavak informacionog sistema kad nastupe katastrofalni događaji • prioritete oporavka resursa informacionog sistema • podatke o timovima koji će biti odgovorni za oporavak informacionog sistema i o imenovanim članovima tih timova uključujući i njihove jasno	

		utvrđene dužnosti i odgovornosti • rezervnu lokaciju za oporavak informacionog sistema odnosno lokaciju rezervnog računarskog centra	
	22. Uspostaviti proces upravljanja incidentima	Definisati korake u slučaju detektovanja incidenta. Uraditi kategorizaciju incidenta (npr. teški, srednji, blaži) i povezati ih sa odgovarajućim sistemima za detekciju kao i sa odgovornima za oblast.	
	23. Uspostaviti proces upravljanja rezervnim kopijama podataka	Definisati procedure i odgovornosti za: • izradu rezervnih kopija • čuvanje rezervnih kopija • testiranje rezervnih kopija (uspešno obavljeno) • oporavak (podataka i softverskih komponenti) • adekvatnu ažurnost podataka	
	24. Obezbediti rezervni računarski centar	Odrediti rezervnu lokaciju i odrediti vrstu rezervnog računskog centra: • vruć-vreme odziva i minutima ili automatski po prestanku rada sajta A. Najsofisticiraniji ali i najskuplji vid rezervnog sajta. • mlak- vreme odziva u satima uz ručnu intervenciju na sajtu B • hladni- vreme odziva u danima Ukoliko kompanija nema sopstvenu rezervnu lokaciju, razmotriti usluge telehousinga i serverhousinga u zemlji. Od ponuđača na tržištu nalaze se Telekom, Telenor, Orion, SBB i dr. Uzeti u obzir nivo i kvalitet usluge koji provajder usluga pruža (Tier 1,2,3 ili 4)	
	Razvoj i održavanje IS		
	25. Uspostaviti proces razvoja IS	Na osnovu donete strategije razvoja informacionog sistema i u skladu sa usvojenim metodologijama upravljanja projektima definisati kontinuirani proces razvoja informacionog sistema. Razvoj sistema treba da omogući adekvatnu podršku poslovnim procesima, i da odgovor na promene u životnom ciklusu sistema pri tome zadržavajući unapred definisanu funkcionalnost i bezbednost.	
	26. Razdvojiti testno od produkcijskog okruženja	Za sve kritične produkcijske sisteme definisati i kreirati adekvatna testna okruženja ukoliko već ne postoje. Testno okruženje fizički i/ili logički odvojiti od produkcijskog okruženja tako da akcije koje se vrše nad testnim ni kakvom slučaju	

		ne mogu da ugroze produkcijsko okruženje. Virtualizacija u mnogome olakšava kreiranje testnih okruženja. Obratiti pažnju na bezbednost testnih okruženja jer takođe mogu da sadrže osetljive informacije.	
	27. Uspostaviti proces upravljanja hardverskim i softverskim komponentama	• Uspostavljanje procedura pravilnog korišćenja hardverskih i softverskih komponenti • Pravljenje ažurnog inventara hardverskih i softverskih komponenti • Definisane vlasništva nad komponentama tj. delegiranje odgovornosti • Definisati procedure za nabavljanje i uklanjanje komponenti	
	28. Uspostaviti proces upravljanja promenama hardverskih i softverskih komponentata IS	• Definisati procedure za testiranje i validiranje novih komponenti pre ulaska u sistem • Definisati procedure za povraćaj starih komponenti u slučaju problema sa novim komponentama • Voditi ažuran dnevnik o promenama u vezi sa hardverskim i softverskim komponentama	
	29. Urediti proces upravljanja hitnim promenama hardverskih i softverskih komponentata	Definisati procedure za hitne promene hardverskih i softverskih komponenti. Obratiti pažnju na minimalni set provera pre puštanja u rad kao i na povraćaj starih komponenti ukoliko je on moguć.	
	30. Obezbediti izradu, čuvanje i redovno održavanje dokumentacije koja se odnose na IS	Dokumentacija mora biti dostupna, potpuna, ažurna i bezbedno uskladištena a korisnici obučeni za korišćenje konkretnog sistema. Moguće korišćenje internog portala, deljenih foldera ili aplikacija rađenih po narudžbini.	
	31. Obezbediti adekvatno, kontinuirano stručno osposobljavanje i obučavanje zaposlenih za korišćenje IS i očuvanje njegove bezbednosti i funkcionalnosti	Redovno organizovati predavanja na temu ispravno i bezbedno korišćenje informacionog sistema. Predavanja kontinuirano sprovoditi i usklađivati sa aktuelnim dešavanjima.	
	Poveravanje aktivnosti u vezi sa IS trećim licima		
	32. Finansijska institucija koje određene aktivnosti namerava da poveri dužna je da to uredi.	Definisati kriterijume za izbor dobavljača uključiti procenu rizika. Posebno obratiti pažnju na sledeće oblasti i moguć uticaj na njih: • kontinuitet poslovanja i reputacija finansijske institucije • troškovi , finansijski rezultat, likvidnost i solventnost finansijske institucije • rizičan profil finansijske institucije • kvalitet usluga koje finansijska institucija pruža klijentima	

33. Organizacije su u obavezi da pre sklapanja ugovora o poveravanju aktivnosti provo izvrše određene provere	• detaljna analiza potencijalnog pružaoca usluga koja se odnosi na njegovu sposobnost pružanja usluga, finansijsko stanje i poslovnu reputaciju • utvrdi da li propisi države ili država u kojima potencijalni pružalac usluga posluje omogućuju Narodnoj banci Srbije nesmetano vršenje kontrole tog poslovanja u delu koji se odnosi na obavljanje poverljivih aktivnosti ili je u vezi sa tim aktivnostima • proceni moguće poteškoće i vreme potrebno za izbor drugog pružaoca usluga, ili mogućnost nastavka obavljanja tih aktivnosti unutar finansijske organizacije u slučaju prestanka pružanja ugovorenih usluga, kao i da s tim u vezi donese odgovarajuću izlaznu strategiju.
34. Finansijska institucija dužna je da Narodnoj banci Srbije omogući nesmetano vršenje kontrole poverljivih aktivnosti, odnosno nadzora nad njima...	Aneksirati ugovore sa izvođačima softvera i uključiti deo koji se tiče mogućnosti provere od strane NBS
35. Organizacija je dužna da obezbedi da se poveravanjem aktivnosti ne ugrozi bezbednost ili funkcionalnost informacionog sistema, kao i da podaci finansijske institucije ostanu u njenom posedu. Svi učesnici u ovom poslu dužni su da postupaju u skladu sa zakonom o zaštiti podataka o ličnosti, kao i sa drugim propisima kojima se uređuje čuvanje tajne nastale u poslovanju finansijskih institucija.	Obezbediti kontrolu nad podacima koji se nalaze u sistemu. Nadgledati aktivnosti koje pružalac usluga obavlja i iste evidentirati (u sklopu centralnog dnevnika događaja ili sl.) Ugovorom obavezati pružaoca usluga da se pridržava zakona o zaštiti podataka o ličnosti, ugovora o poslovnoj tajni i sl.
36. U slučaju namere da promeni pružaoca usluga, organizacija je dužna da o tome obavesti Narodnu banku Srbije najkasnije 30 dana pre planiranog poveravanja aktivnosti	