SMJERNICE ZA UPRAVLJANJE INFORMACIJSKIM SUSTAVOM U CILJU SMANJENJA OPERATIVNOG RIZIKA

OŽUJAK 2006.

HRVATSKA NARODNA BANKA

Sadržaj

1. Uvod

Osnovna načela u poslovanju banaka jesu načelo likvidnosti i načelo solventnosti. Kako bi osigurale poslovanje u skladu sa spomenutim načelima, banke su dužne kontinuirano obavljati mjerenje, procjenu i upravljanje svim rizicima kojima su u svom poslovanju izložene. Rizici kojima su banke izložene u svom poslovanju i za koje minimalno moraju biti propisani postupci mjerenja, procjene i upravljanja uključuju i rizik koji proizlazi iz neadekvatnog upravljanja informacijskim i pridruženim tehnologijama. Hrvatska narodna banka uočila je potrebu da se bankama radi osiguranja sigurnosti i stabilnosti bankarskog poslovanja u Republici Hrvatskoj skrene pozornost na pitanja vezana uz rizik koji proizlazi iz neadekvatnog upravljanja informacijskim i pridruženim tehnologijama.

Banke u svom poslovanju ovise o korištenju informacija. Pravodobne, točne i potpune informacije, s obzirom na njihov utjecaj na poslovanje i odlučivanje, ključne su za ostvarivanje poslovnih ciljeva.

Informacijska tehnologija omogućuje korištenje i upravljanje informacijama odnosno podržava i unapređuje poslovne procese kako bi se što djelotvornije ostvarivali poslovni ciljevi i postigla konkurentska prednost. Međudjelovanje informacijske tehnologije, podataka i postupaka za procesiranje podataka te ljudi koji prikupljaju i koriste navedene podatke čini informacijski sustav. Drugim riječima, informacijski je sustav sveobuhvatnost infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz, distribuciju informacija i raspolaganje njima.

S obzirom na ubrzani razvoj i sveprisutnost informacijske tehnologije u poslovnom okruženju, uporaba informacijskih sustava:

- jest jedan od ključnih čimbenika u poslovanju banke;
- povećava međudjelovanje raznih sustava, jer se informacijski sustavi banke povezuju s klijentima, pružateljima usluga te ostalim subjektima preko javno dostupnih i privatnih telekomunikacijskih mreža;
- postavlja temelj za razvoj novih proizvoda i usluga te utječe na oblikovanje konkurentskih prednosti;
- pokreće reinženjering strateški važnih poslovnih procesa;
- povećava potrebu za novim ulaganjima u resurse informacijskog sustava;
- zahtijeva usvajanje i primjenu novih stručnih znanja.

Iz navedenog proizlazi da je korištenje informacijske tehnologije u svim aspektima bankarskog poslovanja stvorilo veliku ovisnost o informacijskoj tehnologiji pa je prema tome potrebno posvetiti veliku pozornost upravljanju informacijskim sustavom kao sastavnom dijelu upravljanja bankom u cjelini. Nadalje, u sklopu upravljanja informacijskim sustavom posebnu pozornost potrebno je obratiti upravljanju rizikom koji proizlazi iz korištenja informacijskog sustava, kako bi se osiguralo pouzdano, sigurno i kontinuirano poslovanje banke.

Rizici se procjenjuju s aspekta učinka koji bi mogao biti uzrokovan narušavanjem funkcionalnosti i sigurnosti informacijskog sustava, odnosno narušavanjem temeljnih načela informacijskog sustava (objašnjava se u nastavku dokumenta). Upravljanje rizikom informacijskog sustava, za potrebe ovog dokumenta, obuhvaća postupke procjene rizika te poduzimanja radnja za smanjenje rizika na prihvatljivu razinu i održavanje prihvatljive razine

rizika. Povećani rizik informacijskog sustava proizlazi iz neprimjerenog korištenja i upravljanja resursima informacijskog sustava, te može povećati financijski, strateški, operativni, reputacijski i pravni rizik.

1.1. Temeljna načela informacijskog sustava

Funkcionalan i siguran informacijski sustav mora se zasnivati na sljedećim temeljnim načelima:

1. **povjerljivosti:** svojstvu da informacije ne budu dostupne ili otkrivene neovlaštenim subjektima;
2. **integritetu:** svojstvu da informacije i procesi nisu neovlašteno ili nepredviđeno mijenjani;
3. **raspoloživosti:** svojstvu koje omogućuje pristup i upotrebljivost na zahtjev ovlaštenog subjekta;
4. **neporecivosti:** svojstvu koje osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacije;
5. **dokazivosti:** svojstvu koje osigurava da aktivnosti subjekta mogu biti praćene jedinstveno do samog subjekta;
6. **autentičnosti:** svojstvu koje osigurava da je identitet subjekta zaista onaj za koji se tvrdi da jest;
7. **pouzdanosti:** svojstvu dosljednog, očekivanog ponašanja i rezultata.

Neporecivost, dokazivost, autentičnost i pouzdanost mogu se promatrati i kao kombinacija načela povjerljivosti, integriteta i raspoloživosti.

Posljedice narušavanja temeljnih načela informacijskog sustava jesu:

- **Gubitak integriteta.** Integritet sustava i podataka odnosi se na potrebu da informacije budu zaštićene od neovlaštenih ili neispravnih izmjena. Neovlaštene ili neispravne izmjene dovode do gubitka integriteta. Ako integritet sustava ili podataka nije ponovo uspostavljen, nastavak korištenja takvim sustavom ili podacima može dovesti do netočnosti, prijevara ili pogrešnih odluka. Isto tako, povreda integriteta može biti prvi korak u narušavanju raspoloživosti ili povjerljivosti sustava. Zbog tih razloga gubitak integriteta smanjuje povjerenje u informacijski sustav.
- **Gubitak raspoloživosti.** Neraspoloživost informacijskog sustava potrebnog za obavljanje zadatka može negativno utjecati na ciljeve banke i kontinuitet poslovanja te onemogućiti odvijanje vitalnih poslovnih procesa. Gubitak funkcionalnosti sustava i operativne djelotvornosti (učinkovitosti) može, primjerice, dovesti do narušavanja reputacije banke, rezultirati gubitkom produktivnog vremena te onemogućiti krajnjeg korisnika u izvršavanju radnih zadataka.
- **Gubitak povjerljivosti.** Neovlašteno, neočekivano ili nenamjerno otkrivanje ili objavljivanje podataka može rezultirati gubitkom povjerljivosti sustava i podataka. Gubitak povjerljivosti može dovesti do teških povreda važećih propisa te utjecati na gubitak povjerenja javnosti i narušavanje reputacije banke, a može prouzročiti i pokretanje sudskog postupka protiv banke.

Pojam "temeljna načela informacijskog sustava" u nastavku dokumenta, ovisno o kontekstu, podrazumijeva jedno načelo ili kombinaciju načela povjerljivosti, integriteta, raspoloživosti, neporecivosti, dokazivosti, autentičnosti i pouzdanosti.

1.2. Ciljevi, strategije i ostali interni akti

Ciljevi, strategije i ostali interni akti banke trebaju biti definirani tako da budu temelj za djelotvorno upravljanje informacijskim sustavom te da podržavaju poslovne procese i temeljna načela informacijskog sustava. Ciljevi određuju što treba ostvariti, dok strategije određuju kako ostvariti postavljene ciljeve. Ciljevi, strategije i ostali interni akti trebaju se razvijati hijerarhijski od upravljačke prema operativnoj razini te trebaju:

- odražavati potrebe organizacijskih jedinica unutar banke
- uzeti u obzir organizacijska i druga ograničenja
- osigurati dosljednost na svim razinama.

Strategije i ostale interne akte potrebno je održavati i ažurirati u skladu s promjenama poslovnih ciljeva i rezultatima periodičnih provjera (primjerice procjenama rizika, revizijama informacijskog sustava) te u skladu s promjenama u okruženju.

1.3. Sigurnost informacijskog sustava

Banke pri obavljanju svojih poslovnih aktivnosti uvelike ovise o obradi i upotrebi informacija. Narušavanje temeljnih načela informacijskog sustava može imati negativne posljedice za banku. Stoga je potrebno primjereno zaštititi informacije i upravljati sigurnošću informacijskog sustava banke. Potreba za zaštitom informacija i upravljanjem sigurnošću posebice je važna u današnjem okruženju jer su informacijski sustavi banaka povezani s drugim informacijskim sustavima.

Upravljanje sigurnošću informacijskog sustava jest, između ostalog, sveobuhvatan, detaljan i sustavan proces identificiranja potreba (radi ostvarivanja zadovoljavajuće razine sigurnosti) te postizanja i održavanja zadovoljavajuće razine sigurnosti informacijskog sustava.

1.4. Elementi upravljanja rizikom

1.4.1. Resursi informacijskog sustava

Pravilno upravljanje resursima informacijskog sustava ključno je za uspjeh banke i za njega su odgovorne sve upravljačke razine. Resursi, uz ostalo, uključuju:

1. opipljivu imovinu (primjerice hardver, komunikacijsku opremu, građevine)
2. informacije/podatke (primjerice dokumente, podatke u bazama podataka)
3. softver
4. sposobnost proizvodnje nekog proizvoda ili pružanja neke usluge (engl. *know-how*)
5. osobe koje održavaju i koriste informacijski sustav
6. neopipljivu imovinu (primjerice zaštitni znak, reputaciju).

Banka bi trebala identificirati i klasificirati resurse prema njihovoj važnosti i vrijednosti te odrediti i implementirati potreban stupanj zaštite tih resursa.

Proces identificiranja resursa i utvrđivanja njihove važnosti i vrijednosti može biti obavljen na najvišoj razini i ne mora uključivati skupe, detaljne i vremenski zahtjevne analize. Detaljnost analize utvrđuje se na temelju postavljenih funkcionalnih i sigurnosnih ciljeva te bi se morala mjeriti u kontekstu utrošenog vremena i nastalih troškova u odnosu na važnost i vrijednost resursa. Obilježja resursa koja pritom treba uzeti u obzir jesu njihova vrijednost i osjetljivost, te eventualna inherentna zaštita. Funkcionalne i sigurnosne potrebe resursa ovise o njihovoj ranjivosti u prisutnosti određene prijetnje.

1.4.2. Prijetnje

Resursi su izloženi raznim vrstama prijetnja. Prijetnja može prouzročiti neželjenu situaciju čija posljedica može biti nanošenje štete resursima banke. Drugim riječima, šteta može nastati kao posljedica ostvarenja prijetnje (primjerice neovlaštenog uništavanja, razotkrivanja, promjene te unošenja promjena koje uzrokuju pogrešno zapisivanje, nedostupnost ili gubitak informacija). Prijetnja mora iskoristiti postojeću ranjivost resursa da bi se realizirala i rezultirala štetom. Prijetnje mogu biti prirodne ili uzrokovane ljudskim djelovanjem (slučajne ili namjerne). Stoga je potrebno točno utvrditi prijetnje kao i njihovu razinu i vjerojatnost.

Primjeri prijetnja prikazani su u tablici br. 1:

Tablica br. 1 Primjeri prijetnja

Ljudske		**Prirodne**
Namjerne	**Slučajne**	
prisluškivanje	pogreške i propusti	potres
modifikacija informacija	nenamjerno brisanje datoteka, podataka i sl.	udar groma
"hakiranje"	pogrešno preusmjeravanje	poplava
maliciozni kod	nenamjerno fizičko uništenje	požar
krađa		

Dostupni su statistički podaci o mnogim vrstama prijetnja koje bi banka trebala pribaviti i iskoristiti prilikom procesa procjene ranjivosti u svezi s određenom prijetnjom. Prijetnja se može pojaviti unutar banke (primjerice u obliku sabotaže nekog od zaposlenika) ili izvan nje, (primjerice u obliku zlonamjernih "hakera" ili industrijske špijunaže). Šteta koju nanose takvi neželjeni događaji može biti prolazne prirode ili trajna (u slučaju potpunog uništenja resursa).

Opseg štete uzrokovane prijetnjom može se razlikovati prema neželjenom događaju. Virus, kao primjer malicioznog koda, može uzrokovati različitu razinu štete ovisno o svom djelovanju.

Prijetnje je često moguće kvantificirati i/ili kvalificirati kako bi se ocijenila njihova razorna moć (primjerice virus se može opisati kao destruktivan ili nedestruktivan, a jačina potresa može se opisati na temelju Richterove ljestvice).

Neke prijetnje mogu utjecati na više od jednog resursa te mogu imati različit učinak ovisno o kojem se resursu radi (primjerice virus na osobnom računalu može imati ograničene ili lokalne posljedice, dok učinak istog virusa na mrežnom poslužitelju može biti puno širi). Svaka prijetnja ima obilježja koja pružaju korisne informacije o samoj prijetnji. Primjeri takvih korisnih informacija uključuju:

1. izvor (primjerice je li riječ o unutrašnjoj ili vanjskoj prijetnji)
2. motiv (primjerice ostvarivanje financijske dobiti, ostvarivanje konkurentske prednosti)
3. učestalost pojavljivanja
4. razornu moć.

Prijetnje je moguće okarakterizirati prema razini i vjerojatnosti pojedine prijetnje (primjerice kao velike, srednje i male).

1.4.3. Ranjivost

Ranjivost je slabost koju je moguće slučajno aktivirati ili namjerno iskoristiti, a posljedica toga može biti nanošenje štete informacijskom sustavu i poslovnim ciljevima. Ranjivosti koje se povezuju s resursima uključuju, između ostalog, slabosti fizičke sigurnosti, organizacije, internih akata, zaposlenika, upravljačke strukture, hardvera, softvera i informacija.

Ranjivost sama po sebi ne nanosi štetu, nego ranjivost možemo definirati kao stanje ili skup stanja koji može omogućiti nekoj prijetnji da utječe na resurse (primjerice nedostatak mehanizama kontrole pristupa jest ranjivost koja bi mogla omogućiti ostvarenje prijetnje neovlaštenog pristupa, što može dovesti do gubitka ili oštećenja resursa). Budući da se okruženje može brzo promijeniti, potrebno je pratiti sve oblike ranjivosti kako bi se identificirale one koje su postale izložene starim i novim prijetnjama. Analiza ranjivosti je procjena slabosti koje identificirane prijetnje mogu iskoristiti. Ta bi analiza trebala uzeti u obzir okruženje i postojeće zaštitne mjere i kontrole. Ranjivost u odnosu na neku prijetnju pokazatelj je lakoće kojom je moguće naštetiti sustavu ili resursima.

Ranjivost se može okarakterizirati ovisno o ishodu analize ranjivosti (primjerice kao velika, srednja i mala).

1.4.4. Učinak

Učinak je posljedica nekoga neželjenog događaja, izazvanog namjerno ili slučajno, koji utječe na resurse. Posljedice mogu biti uništenje nekog resursa, nanošenje štete informacijskom sustavu te gubitak temeljnih načela informacijskog sustava čega rezultat može biti (što može prouzročiti) financijski gubitak i gubitak tržišnog udjela ili reputacije banke.

Učestalost pojave neželjenog događaja također treba uzeti u obzir, posebice kada je razina štete počinjene svakim događajem niska, ali ukupan učinak većeg broja događaja s vremenom može biti znatan. Analiza učinka važan je element procjene rizika i odabira zaštitnih mjera.

Kvantitativna i kvalitativna mjerenja učinka mogu biti provedena na različite načine, kao što su:

- utvrđivanje troškova
- pridruživanje neke empirijske skale za njegovo mjerenje (npr. od 1 do 10)
- upotreba unaprijed određenog načina stupnjevanja (npr. mali, srednji i veliki).

1.4.5. Rizik

Rizik je funkcija vjerojatnosti da će identificirani izvor prijetnje iskoristiti određenu ranjivost i učinka koji taj neželjeni događaj može imati na banku. Drugim riječima, rizik obilježava kombinacija dvaju faktora, a to su vjerojatnost da će se neželjeni događaj dogoditi te njegov učinak. Svaka promjena resursa, prijetnja, ranjivosti ili zaštitnih mjera može znatno utjecati na rizik. Rano otkrivanje te prepoznavanje promjena koje su nastale u okruženju ili sustavu povećava mogućnost pravodobnog poduzimanja koraka potrebnih za smanjivanje rizika.

1.4.6. Mjere

Mjere uključuju sve postupke, procedure i mehanizme kojima se:

- štite resursi informacijskog sustava od prijetnja;
- smanjuju ranjivosti informacijskog sustava;
- ograničava učinak neželjenih događaja;
- otkrivaju neželjeni događaji;
- pospješuje oporavak.

Budući da mjere smanjuju izloženost banke riziku, možemo ih smatrati i zaštitnim mjerama. Zaštitne se mjere odnose na upravljačku, logičku i fizičku razinu. Djelotvorno upravljanje informacijskim sustavom obično zahtijeva kombiniranje različitih zaštitnih mjera kako bi se osigurala slojevita zaštita resursa informacijskog sustava.

Zaštitne mjere imaju jednu od sljedećih uloga ili više njih:

1. prevencije
2. odvraćanja
3. otkrivanja
4. ograničavanja

5. korigiranja
6. oporavka
7. nadzora
8. osvješćivanja.

Zaštitne se mjere provode uvođenjem novih ili izmjenom postojećih kontrola. Podizanje razine znanja i svijesti zaposlenika vezanih uz sigurnost i funkcionalnost informacijskog sustava važna je zaštitna mjera.

1.4.7. Preostali rizici

U većini slučajeva provedba zaštitnih mjera ne uklanja u potpunosti rizike, što upućuje na postojanje preostalih (rezidualnih) rizika.

Upravljačke strukture trebaju biti svjesne svih preostalih rizika sa stajališta njihova mogućeg učinka i vjerojatnosti pojave negativnog događaja, te donijeti odluku o prihvaćanju preostalih rizika kojima je izložen informacijski sustav.

1.4.8. Ograničenja

Pri odabiru i provedbi mjera potrebno je uzeti u obzir ograničenja kao što su:
1. organizacijska ograničenja
2. financijska ograničenja
3. ograničenja određenog okruženja
4. ograničenja vezana uz ljudske resurse
5. vremenska ograničenja
6. pravna ograničenja
7. tehnička ograničenja
8. kulturološka i društvena ograničenja.

Većinu navedenih ograničenja obično postavljaju upravljačke strukture banke, te na njih utječe okruženje u kojem banka posluje. Isto tako, potrebno je periodično revidirati ograničenja kako bi se identificirala nova ograničenja i uočile promjene već poznatih ograničenja.

2. Upravljanje informacijskim sustavom

Cilj upravljanja informacijskim sustavom jest podržavanje poslovnih ciljeva i strategije banke uz efikasno korištenje resursa informacijskog sustava te primjereno upravljanje rizicima koji proizlaze iz korištenja informacijske tehnologije. Uspješno upravljanje informacijskim sustavom rezultira postizanjem optimalnog učinka informacijske tehnologije, te naposljetku daje dodatnu vrijednost poslovanju. Nadalje, upravljanje informacijskim sustavom odnosi se na sve osobe, sustave i procese koji svojim aktivnostima vezanim uz informacijski sustav pridonose ispunjavaju poslovnih ciljeva i strategije banke, te postizanju i održavanju temeljnih načela informacijskog sustava.

Primjereno upravljanje informacijskim sustavom uključuje, među ostalim, i uspostavu:

- adekvatne organizacijske strukture (primjerice organizacijske jedinice za informacijsku tehnologiju, organizacijske jedinice za upravljanje rizikom)
- odgovarajućih funkcija i odbora (kao što su voditelj organizacijske jedinice za informacijsku tehnologiju, voditelj sigurnosti informacijskog sustava, odbor za upravljanje informacijskim sustavom)
- procesa upravljanja rizikom informacijskog sustava (procjene rizika, poduzimanje radnja za smanjenje rizika na prihvatljivu razinu i održavanje prihvatljive razine rizika) i nadzora nad tim procesom.

Nadalje, upravljanje informacijskim sustavom treba obuhvatiti sljedeća područja:

- sigurnost informacijskog sustava
- planiranje kontinuiteta poslovanja
- razvoj sustava i eksternalizaciju
- održavanje informacijskog sustava.

Banka bi trebala uspostaviti organizacijsku jedinicu za informacijsku tehnologiju koja bi trebala pružati adekvatnu informatičku podršku ostalim organizacijskim jedinicama. Pri određivanju organizacijske strukture i definiranju funkcija organizacijske jedinice za informacijsku tehnologiju potrebno je osigurati adekvatnu podjelu zadataka i ovlasti. Navedeno je potrebno kako bi se osiguralo prikladno raspoređivanje resursa za sve funkcije organizacijske jedinice za informacijsku tehnologiju i adekvatno razdvajanje (segregiranje) dužnosti.

Upravljanje informacijskim sustavom banke trebalo bi biti predmetom nadzora unutarnje revizije kako bi se neovisno i objektivno provjerila adekvatnost upravljanja tim sustavom.

Strategija i planiranje

Banka bi trebala donijeti strategiju informacijskog sustava koja treba biti usklađena s poslovnom strategijom banke. Strategija informacijskog sustava trebala bi obuhvatiti dugoročne i kratkoročne inicijative povezane s informacijskim sustavom, pri čemu valja uzeti u obzir barem sljedeće:

- nove poslovne inicijative
- organizacijske promjene
- tehnološki razvoj

- regulatorne zahtjeve
- potrebe za resursima i nadzorom
- ograničenja.

Nadalje, strategija informacijskog sustava trebala bi biti formalno dokumentirana, odobrena od strane uprave banke te ažurirana i revidirana na godišnjoj razini. Strategiju informacijskog sustava potrebno je razraditi donošenjem strateških i operativnih planova.

Strateško planiranje vezano uz informacijski sustav usredotočeno je na srednji rok te pomaže osigurati dosljednost primjene i usklađenost tehnoloških planova s poslovnim ciljevima banke. Uspješno strateško planiranje treba osigurati informatičku podršku kojom bi se održala ravnoteža troškova i djelotvornosti te istodobno omogućilo poslovnim organizacijskim jedinicama da adekvatno odgovore na zahtjeve tržišta. Isto tako, potrebno je procijeniti potrebna financijska sredstva.

Prilikom planiranja informacijskih sustava potrebno je razmotriti barem sljedeće čimbenike:

- poslovne ciljeve i planove banke
- uvjete na tržištu
- planirani rast banke
- tehnološke standarde
- važeće propise
- kontrolu troškova
- unapređenje procesa i porast djelotvornosti
- kvalitetu usluga pruženih klijentima banke
- usporedbu eksternalizacije procesa i provođenja procesa unutar banke
- optimalnu infrastrukturu
- sposobnost usvajanja i uvođenja novih tehnologija
- ograničenja.

Operativno planiranje proizlazi iz strateškog planiranja, usredotočeno je na kratkoročne aktivnosti te uključuje i donošenje financijskog plana. S obzirom na prije navedeno operativno bi planiranje trebalo biti usredotočeno na neposredna pitanja kao što su postojanje adekvatnih resursa informacijskog sustava, dostatnost financijskih sredstava, adekvatno upravljanje rizikom te učinak mogućih promjena na poslovne procese, kako bi se zadovoljile operativne potrebe.

Strateške i operativne planove potrebno je međusobno prilagođavati, ovisno o promjenama poslovnih ciljeva.

Interni akti

Donošenje i primjena internih akata vezanih uz informacijski sustav osnova su za uspostavljanje i održavanje upravljačkih kontrola koje bi trebale biti slojevite i hijerarhijski uspostavljene od najviše (strateške) razine prema najnižoj (operativnoj) razini. Banka bi trebala donijeti, dokumentirati, provoditi i održavati interne akte kako bi adekvatno upravljala rizicima koji proizlaze iz korištenja informacijske tehnologije te naposljetku kako bi djelotvorno upravljala informacijskim sustavom u cjelini. Internim aktima smatraju se odluke, politike, standardi, smjernice, procedure, upute i ostali dokumenti za čije je donošenje

odgovorna uprava banke. Interne akte potrebno je integrirati u procese informacijskog sustava i svakodnevne aktivnosti zaposlenika. Nadalje, interni bi akti trebali biti usklađeni s propisima, standardima i pravilima struke.

Interni akti na najvišoj konceptualnoj ili hijerarhijskoj razini (primjerice politike) trebali bi obuhvatiti sva područja i aspekte informacijskog sustava banke uključujući osobe, sustave i procese. Banka bi trebala procijeniti i odrediti koja je područja i aspekte informacijskog sustava potrebno razraditi detaljnijim internim aktima niže razine (primjerice smjernicama, uputama i procedurama) te definirati razinu detaljnosti razrade. Razina detaljnosti i obuhvat pojedinog internog akta ovise o njegovoj svrsi, namjeni, vrsti te o kompleksnosti informacijskog sustava.

2.1. Uprava banke

Upravljanje informacijskim sustavom vrlo je važno u procesu donošenja poslovnih odluka. Kako bi banka primjereno upravljala informacijskim sustavom, uprava bi banke, između ostalog, trebala:

- biti upoznata s konceptima i aktivnostima vezanim uz informacijski sustav
- odrediti člana uprave koji će biti nadležan za nadzor i kontrolu procesa upravljanja informacijskim sustavom
- uspostaviti adekvatnu organizacijsku strukturu, pripadajuće funkcije i odbore koji upravljaju informacijskim sustavom banke
- delegirati ovlasti prema uspostavljenoj organizacijskoj i funkcionalnoj strukturi
- definirati kriterije, načine i postupke izvješćivanja uprave
- usvojiti strategiju informacijskog sustava te nadzirati njezino provođenje
- donijeti interne akte kojima se uređuje upravljanje informacijskim sustavom
- uspostaviti proces upravljanja rizikom informacijskog sustava.

2.2. Voditelj organizacijske jedinice za informacijsku tehnologiju

Uprava banke trebala bi imenovati voditelja organizacijske jedinice za informacijsku tehnologiju (engl. *Chief Information Officer*) te definirati njegove ovlasti, odgovornosti kao i djelokrug rada. Voditelj organizacijske jedinice informacijske tehnologije trebao bi prvenstveno biti usmjeren na strateška pitanja vezana uz informacijski sustav, upravljanje, nadzor i koordinaciju rada organizacijske jedinice informacijske tehnologije te na funkcionalnost i djelotvornost informacijskog sustava u cjelini. Nadalje, voditelj organizacijske jedinice informacijske tehnologije trebao bi imati prikladno stručno obrazovanje i znanje te odgovarajuće iskustvo na području informacijske tehnologije i upravljanja njome.

Dobre prakse nalažu da djelokrug rada voditelja organizacijske jedinice za informacijsku tehnologiju obuhvaća sljedeće:

- razvoj i održavanje informacijskog sustava
- pružanje podrške korisnicima informacijskog sustava
- sudjelovanje u izradi strategije i strateškog plana informacijskog sustava
- planiranje, organizaciju, koordinaciju i nadzor aktivnosti organizacijske jedinice za informacijsku tehnologiju
- pokretanje inicijativa (npr. unapređivanje postojećih funkcionalnosti informacijskog sustava, uvođenje novih tehnoloških rješenja, unapređenje sigurnosti informacijskog sustava i slično)
- provedbu svih prihvaćenih inicijativa koje banka poduzima u svezi s informacijskim sustavom
- koordiniranje aktivnosti vezanih uz sigurnost informacijskog sustava s voditeljem sigurnosti informacijskog sustava
- koordiniranje aktivnosti glede informacijskog sustava s ostalim organizacijskim jedinicama i tijelima banke
- planiranje ulaganja u informacijski sustav
- sudjelovanje u procesu odabira i nabave informatičke opreme
- sudjelovanje u planiranju, provedbi i nadzoru eksternalizacije (dijela) informacijskog sustava
- sudjelovanje u izradi internih akata povezanih s informacijskim sustavom (politika, standarda, procedura, smjernica, uputa, planova)
- planiranje izobrazbe
- upravljanje imovinom informacijskog sustava
- upravljanje odnosom s dobavljačima
- izvještavanje uprave banke
- ostalo (ovisno o procjeni i odluci uprave banke).

2.3. Voditelj sigurnosti informacijskog sustava

Banka bi trebala uspostaviti neovisnu funkciju voditelja sigurnosti informacijskog sustava (engl. *Chief Information Systems Security Officer – CISSO*). Voditelj sigurnosti informacijskog sustava ne bi trebao istodobno biti angažiran na drugim funkcijama koje mogu stvoriti sukob interesa (kao što su rukovoditelj ili zaposlenik organizacijske jedinice za informacijsku tehnologiju i unutarnji revizor informacijskog sustava). Voditelj sigurnosti trebao bi biti odgovoran upravi banke te svoja izvješća dostavljati izravno upravi, a ukoliko procijeni da je potrebno, i nadzornom odboru banke. Nadalje, jednom godišnje voditelj sigurnosti informacijskog sustava trebao bi za upravu i nadzorni odbor izraditi izvješće o stanju sigurnosti informacijskog sustava u proteklih godinu dana. Voditelj organizacijske jedinice za informacijsku tehnologiju i unutarnji revizor trebali bi biti upoznati s navedenim izvješćima.

Voditelj sigurnosti informacijskog sustava trebao bi:

- nadzirati i koordinirati aktivnosti vezane uz sigurnost informacijskog sustava
- inicirati primjenu dobrih praksi i prihvaćenih standarda vezanih uz sigurnost informacijskog sustava
- imati savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

Zadaci voditelja sigurnosti trebali bi, između ostalog, uključivati sljedeće:

- određivanje sigurnosnih ciljeva u skladu sa strategijom informacijskog sustava banke
- razvoj politike sigurnosti informacijskog sustava, standarda, smjernica i ostalih internih akata s ciljem postizanja i održavanja zadovoljavajuće razine sigurnosti
- razvoj i primjenu strategije sigurnosti i sigurnosne arhitekture informacijskog sustava
- nadziranje istrage u slučajevima narušavanja sigurnosti informacijskog sustava
- suradnju s vanjskim suradnicima prilikom obavljanja neovisnih revizija i testiranja sigurnosti informacijskog sustava
- analiziranje sigurnosnih potreba te u skladu s njima predlaganje planiranja, implementacije, testiranja i nadziranja aktivnosti za poboljšanje sigurnosti informacijskog sustava
- planiranje i koordiniranje analize isplativosti preporučenih i postojećih sigurnosnih rješenja
- upozoravanje na potrebu za izobrazbom i davanje smjernica za izobrazbu svih osoba koje se koriste informacijskim sustavom banke, a u svezi sa sigurnosti informacijskog sustava
- dostavljanje izvješća upravi i nadzornom odboru banke
- procjenu rizika sigurnosti informacijskog sustava
- kontroliranje provođenja politike sigurnosti informacijskog sustava i ostalih internih akata koji se odnose na sve aspekte sigurnosti informacijskog sustava
- koordiniranje aktivnosti s organizacijskom jedinicom informacijske tehnologije i unutarnjom revizijom
- sudjelovanje u značajnijim fazama u životnom ciklusu informacijskog sustava s aspekta sigurnosti
- sudjelovanje u planiranju kontinuiteta poslovanja.

2.4. Odbor za upravljanje informacijskim sustavom

Uprava banke trebala bi imenovati odbor za upravljanje informacijskim sustavom čija je uloga praćenje i nadziranje informacijskog sustava i njegovih aktivnosti u smislu usklađenosti s poslovnim ciljevima i strateškim planom banke. Isto tako, uloga odbora za upravljanje informacijskim sustavom jest koordinacija inicijativa vezanih uz informacijski sustav na upravljačkoj razini, omogućavanje optimizacije troškova i boljeg upravljanja informacijskim sustavom te smanjivanje rizika informacijskog sustava. Opseg djelovanja, ovlasti i ciljevi odbora za upravljanje informacijskim sustavom moraju biti jasno definirani.

Aktivnosti odbora za upravljanje informacijskim sustavom trebale bi uključiti barem sljedeće:

- koordiniranje i nadzor razvoja i primjenu strategije i strateškog plana informacijskog sustava
- ocjenjivanje i prihvaćanje politike sigurnosti informacijskog sustava kako bi se osiguralo da politika sigurnosti odgovara poslovnim zahtjevima i ne ograničava poslovne aktivnosti
- odobravanje i kontrolu važnijih projekata vezanih uz informacijski sustav, kao i sredstava potrebnih za njihovu realizaciju
- postavljanje prioriteta važnih aktivnosti vezanih uz informacijski sustav
- predlaganje novih te ocjenjivanje postojećih internih akata koji se odnose na informacijski sustav
- nadziranje funkcionalnosti i sigurnosti informacijskog sustava u cjelini
- ovisno o potrebi, predlaganje ulaganja u informacijski sustav koja odstupaju od planiranih troškova
- arbitriranje u slučaju nesuglasica i spornih pitanja povezanih s informacijskim sustavom
- procjenjivanje i odobravanje eksternalizacije (dijela) poslovnih procesa te koordiniranje aktivnosti vezanih uz eksternalizaciju
- koordiniranje, nadzor i potvrđivanje klasifikacije informacija
- podnošenje izvješća upravi banke o svom radu
- davanje mišljenja o imenovanju voditelja sigurnosti informacijskog sustava.

Odbor za upravljanje informacijskim sustavom trebao bi dobivati potrebne informacije od organizacijske jedinice za informacijsku tehnologiju i ostalih organizacijskih jedinica te unutarnje i vanjske revizije kako bi mogli djelotvorno koordinirati i kontrolirati resurse informacijskog sustava. Odbor za upravljanje informacijskim sustavom trebao bi se redovito sastajati te sastavljati zabilješke radi dokumentiranja svojih aktivnosti i odluka.

Dobre prakse nalažu da članovi odbora za upravljanje informacijskim sustavom budu:

- član uprave banke
- rukovoditelj organizacijske jedinice za informacijsku tehnologiju
- voditelj sigurnosti informacijskog sustava
- osoba koja obavlja unutarnju reviziju informacijskog sustava (djelovanje te osobe u odboru ne bi smjelo stvoriti sukob interesa utjecanjem na proces donošenja odluka)
- predstavnici ostalih organizacijskih jedinica banke, odnosno barem onih organizacijskih jedinica koje su izrazito ovisne o informacijskom sustavu.

Sve navedene aktivnosti odbora za upravljanje informacijskim sustavom mogu provoditi i drugi odbori u skladu s potrebama i odlukom uprave banke.

2.5. Upravljanje projektima

Dobre prakse nalažu primjenu projektnog pristupa za postizanje specifičnih ciljeva u okviru upravljanja informacijskim sustavom banke. Upravljanje projektima je primjena znanja, vještina, alata i jasno definiranih te provjerenih tehnika na različite aktivnosti za potrebe projekata. Upravljanje projektima podrazumijeva uspostavu procesa planiranja, organizacije, provedbe i kontrole osoba, sustava i procesa radi postizanja postavljenih ciljeva.

Detaljni projektni planovi, jasno postavljeni zahtjevi i očekivanja, iskustvo voditelja projekata, realan budžet i djelotvorna komunikacija uvelike pridonose uspješnom upravljanju projektima. Neprimjereno vođenje projekata može rezultirati, primjerice, kašnjenjem projekta, prekoračenjem budžeta projekta ili smanjenom kvalitetom proizvoda ili usluge. Smanjena kvaliteta proizvoda ili usluge može se očitovati u problemima s pouzdanošću, djelotvornošću ili sigurnošću, a svaka naknadna promjena koja unapređuje sigurnost, funkcionalnost i sustav kontrola u cjelini može zahtijevati dodatne resurse (primjerice novac, ljude, vrijeme).

Adekvatno upravljanje projektima omogućava banci razvoj novih proizvoda i usluga te širenje poslovanja u skladu sa stvarnim potrebama, pravodobno i u okviru planiranih financijskih i ljudskih resursa. Drugim riječima, primjereno upravljanje projektima povećava sposobnost banke prilagođavanju promjenama u poslovanju i okruženju te omogućuje ostvarivanje postavljenih strateških ciljeva.

Uzimajući u obzir složenost i posebnost projekata i poslovnih procesa, banka bi trebala definirati i formalno propisati proces upravljanja projektima. Metodologija upravljanja projektima (strukturirane tehnike vođenja projekata koje uključuju načela, prakse i procedure) unapređuje kontrolu nad projektima dijeleći složene zadatke u manje cjeline kojima je lakše upravljati.

Metodologija upravljanja projektima trebala bi segmentirati projekte u projektne faze ovisno o odabiru metodologije (primjerice faza inicijacije projekta, planiranja, dizajniranja, razvoja, testiranja, implementacije i održavanja) kao i potrebne aktivnosti unutar projektnih faza. Isto tako, metodologija upravljanja projektima trebala bi se moći prilagoditi karakteristikama pojedinih projekata.

Metodologija upravljanja projektima trebala bi definirati kriterije, načine i postupke upravljanja projektima odnosno osigurati postojanje adekvatnih:

- projektnih planova
- definicija zahtjeva i očekivanja od projekta
- standarda vođenja projekta i procedura
- standarda kontrole kvalitete i upravljanja rizikom projekta
- definicija projektnih uloga i odgovornosti
- financijskih, vremenskih i ljudskih resursa
- kontrolnih točaka
- kanala i načina komunikacije.

Dobre prakse nalažu primjenu projektnog pristupa prilikom:

- nabave, eksternalizacije i razvoja (dijela) informacijskog sustava
- ostalih aktivnosti kao što su migracija sustava i podataka, unapređivanje proizvoda, usluga i infrastrukture.

Radi primjerenog upravljanja projektima vrlo je važno jasno definirati uloge i odgovornosti svih osoba i tijela uključenih u realizaciju projekata kao što su uprava banke, odbor za upravljanje informacijskim sustavom, voditelj projekta, sponzor projekta, organizacijska jedinica za informacijsku tehnologiju, kontrola kvalitete, zaposlenici iz poslovnih sektora, sistemski analitičari i tehnolozi poslovnih procesa, unutarnja revizija te voditelj sigurnosti informacijskog sustava. Ovisno o veličini i složenosti projekta i samih poslovnih procesa uloge se mogu preklapati pri čemu treba uzeti u obzir potrebu za primjerenom segregacijom dužnosti.

U svim projektnim fazama potrebno je obratiti pozornost na sigurnosne aspekte projekta te na zahtjeve koji proizlaze iz potrebe za održavanjem kontinuiteta poslovanja.

3. Upravljanje rizikom informacijskog sustava

Upravljanje rizikom je proces procjene rizika, poduzimanja radnja za smanjenje rizika na prihvatljivu razinu i održavanja prihvatljive razine rizika. Drugim riječima, upravljanje rizikom kontinuirani je proces usporedbe procijenjenih rizika s prednostima i troškovima predloženih mjera te uvođenja odabranih mjera u skladu s poslovnim ciljevima i temeljnim načelima informacijskog sustava.

Upravljanje rizikom treba obuhvatiti cjelokupni informacijski sustav banke. Za nove sustave i sustave koji su u fazi planiranja (uključujući i planiranje značajnih promjena u informacijskom sustavu), upravljanje rizikom treba biti sastavni dio razvojnog procesa, dok se kod postojećih sustava treba uvesti u što kraćem vremenu.

Zaštitne mjere se odabiru ovisno o rizicima odnosno o vjerojatnosti pojave neželjenog događaja i o njegovu učinku na informacijski sustav. Također je važno napomenuti da provođenje zaštitnih mjera može stvoriti nove ranjivosti i tako rezultirati novim rizicima. Stoga je potrebno pomno izabrati odgovarajuće zaštitne mjere, ne samo radi smanjivanja rizika već i zato da bi se izbjeglo izlaganja novim rizicima. Isto tako, potrebno je razmotriti različite vrste zaštitnih mjera i provesti analizu isplativosti te uzeti u obzir prihvatljivu razinu rizika preostalih nakon provođenja odabranih mjera odnosno uvođenja kontrola.

Rizici se procjenjuju s aspekta mogućeg učinka kao posljedice narušavanja funkcionalnosti i sigurnosti informacijskog sustava, odnosno narušavanja temeljnih načela informacijskog sustava. Većina prijetnja i ranjivosti neposredno se odnosi na sigurnost informacijskog sustava stoga je u nastavku ovog dokumenta poseban naglasak stavljen na procjenu i smanjenje rizika s aspekta sigurnosti.

Kako bi se postigla zadovoljavajuća razina sigurnosti, banka bi trebala utvrditi sigurnosni potencijal kojim treba raspolagati informacijski sustav te planirati sredstva za njegovo ostvarenje. Upravljanje rizikom omogućuje uravnoteživanje operativnih troškova i koristi od zaštitnih mjera da bi se adekvatno zaštitio informacijski sustav.

Upravljanje rizikom je kontinuirani proces koji uključuje:

- procjenu rizika
- smanjivanje rizika
- održavanje prihvatljive razine rizika.

Dobre prakse nalažu da se upravljanje rizikom integrira u životni ciklus informacijskog sustava kako bi procijenjeni rizik odgovarao stvarnom stanju sustava te kako bi se podržali poslovni ciljevi banke.

U sljedeća dva poglavlja ukratko su opisane radnje koje bi banka, prema dobrim praksama, trebala poduzimati u sklopu upravljanja rizicima. Spomenute su radnje samo jedan od načina provođenja procjene i smanjenja rizika.

3.1. Procjena rizika

Banka bi trebala pri procjeni rizika utvrditi razinu rizika kojem je izložen informacijski sustav te predložiti zaštitne mjere kako bi se rizik smanjio na prihvatljivu razinu. Rizici se procjenjuju s aspekta mogućeg učinka uzrokovanog narušavanjem funkcionalnosti i/ili sigurnosti informacijskog sustava. Kako bi se utvrdila vjerojatnost pojave nekog štetnog događaja, potrebno je analizirati prijetnje informacijskom sustavu zajedno s ranjivostima te kontrolama koje su primijenjene u informacijskom sustavu. Učinak se odnosi na opseg i veličinu štete koju prijetnja može uzrokovati ako iskoristi određenu ranjivost.

Procjena rizika trebala bi uključivati sljedeće radnje:
1. određivanje obilježja sustava
2. identifikaciju prijetnja
3. identifikaciju ranjivosti
4. analizu sustava kontrola
5. određivanje vjerojatnosti
6. analizu učinka
7. utvrđivanje rizika
8. predlaganje mjera
9. dokumentiranje rezultata u obliku formalnog izvješća.

3.1.1. Određivanje obilježja sustava

Određivanje obilježja informacijskog sustava definira opseg procesa procjene rizika te daje informacije ključne za definiranje rizika. Utvrđivanje rizika kojem je izložen informacijski sustav zahtijeva razumijevanje njegova okruženja. Stoga je potrebno prikupiti informacije o informacijskom sustavu koje uključuju:
- hardver
- softver
- sistemska sučelja (npr. interna i eksterna sposobnost povezivanja)
- poslovne informacije i ostale informacije koje rabi informacijski sustav (informacije je potrebno klasificirati u različite grupe prema stupnju njihove osjetljivosti, što je detaljnije opisano u poglavlju "Klasifikacija informacija")
- osobe koje održavaju i koriste informacijski sustav
- svrhu sustava (npr. procesi koje obavlja informacijski sustav)
- važnost i osjetljivost sustava i podataka (npr. vrijednost sustava ili kolika je njegova važnost za banku)
- ostalo.

Nadalje, potrebno je prikupiti i dodatne informacije povezane s operativnim okruženjem informacijskog sustava koje uključuju sljedeće (ali nisu ograničene na to):
- funkcionalne potrebe
- interne akte koji se odnose na informacijski sustav
- arhitekturu sigurnosti sustava
- topologiju mreže (npr. dijagram mreže)

- tok informacija koje se odnose na informacijski sustav (npr. sistemska sučelja, dijagram toka ulaznih i izlaznih podataka sustava)
- identifikaciju upravljačkih, logičkih i fizičkih kontrola
- fizičku sigurnost (npr. sigurnost prostorija, politike pristupa sistemskoj prostoriji)
- sigurnost okoline u kojoj je informacijski sustav (npr. kontrola vlažnosti, vode, napajanja, onečišćenja, temperature i kontrola prisutnosti kemikalija).

Rezultat: izvješće o obilježjima informacijskog sustava s cjelovitim prikazom okruženja informacijskog sustava

3.1.2. Identifikacija prijetnja

Prijetnja je potencijal određenog izvora prijetnja da uspješno iskoristi određenu ranjivost. Izvor prijetnje ne utječe na rizik ako ne može iskoristiti ranjivost.

Cilj identifikacije prijetnja jest otkriti prijetnje koje se odnose na informacijski sustav koji se procjenjuje, identificirati izvore prijetnja (ako je to moguće) te sastaviti popis identificiranih prijetnja i izvora.

Prijetnja je:
- namjera ili radnja usmjerena k namjernom iskorištavanju ranjivosti sustava ili
- situacija ili radnja koja može slučajno aktivirati ranjivost.

Izvor prijetnje može nanijeti štetu informacijskom sustavu. Uobičajeni izvori prijetnja mogu biti prirodni, ljudski ili iz okruženja. Stoga je potrebno identificirati sve prijetnje i izvore prijetnja koji bi mogli naštetiti informacijskom sustavu banke i njegovu okruženju.

Rezultat: izvješće s popisom prijetnja koje bi mogle iskoristiti ranjivosti informacijskog sustava banke i njihovih izvora

3.1.3. Identifikacija ranjivosti

Ranjivost je slabost koju je moguće slučajno aktivirati ili namjerno iskoristiti. Sa stanovišta sigurnosti informacijskog sustava ranjivost je mana ili slabost u sigurnosnim procedurama sustava, njegovu dizajnu, implementaciji ili unutarnjim kontrolama, koja može biti iskorištena te rezultirati povredom sigurnosti. Cilj identifikacije ranjivosti jest utvrđivanje ranjivosti informacijskog sustava koje bi mogli iskoristiti izvori prijetnja.

Ranjivosti informacijskog sustava mogu biti otkrivene pomoću različitih metoda prikupljanja informacija. Pri analizi ranjivosti potrebno je, između ostalog, uzeti u obzir sljedeće:
- dokumentaciju o prethodnoj procjeni rizika informacijskog sustava
- izvješća unutarnje i vanjske revizije informacijskog sustava
- izvješća o nepravilnostima u sustavu
- izvješća o sigurnosti
- izvješća o testiranju informacijskog sustava

- popise ranjivosti
- stručne publikacije vezane uz informacijske sustave
- preporuke dobavljača i proizvođača
- izvješća o rezultatima testiranja informacijskog sustava pomoću proaktivnih metoda testiranja (primjerice alata za automatsko otkrivanje ranjivosti, testiranje mogućnosti prodora u sustav i slično).

Kao metoda u otkrivanju ranjivosti može poslužiti i izrada kontrolne liste zahtjeva koja sadrži osnovne funkcionalne i sigurnosne kriterije koje je potrebno provjeriti kako bi se utvrdile ranjivosti resursa informacijskog sustava.

Pri otkrivanju ranjivosti mogu se primijeniti kriteriji u sljedećim sigurnosnim segmentima:
- upravljačkom (primjerice dodjela ovlasti i odgovornosti, procjena rizika)
- logičkom (primjerice kontrole pristupa, komunikacija, operativni i sistemski zapisi)
- fizičkom (primjerice kontrola i zaštita okoline, fizički pristup i raspolaganje medijima s podacima).

Rezultat: izvješće s popisom identificiranih ranjivosti informacijskog sustava koje prijetnje mogu iskoristiti

3.1.4. Analiza sustava kontrola

Cilj ove radnje jest analizirati sustav kontrola koje je banka uvela ili planira uvesti radi smanjenja ili otklanjanja vjerojatnosti (ili mogućnosti) da neka prijetnja iskoristi ranjivost informacijskog sustava. Analiza sustava kontrola uključuje ispitivanje djelotvornosti kontrola koje su već primijenjene u informacijskom sustavu. Sastavljanje kontrolne liste zahtjeva i/ili upotreba dostupne kontrolne liste može biti od velike pomoći pri djelotvornom i sistematičnom analiziranju sustava kontrola.

Rezultat: izvješće s popisom kontrola i ocjenom njihove djelotvornosti

3.1.5. Utvrđivanje vjerojatnosti

Kako bi banka mogla utvrditi vjerojatnost da identificirana ranjivost bude iskorištena u okruženju izloženom prijetnji, potrebno je uzeti u obzir barem sljedeće čimbenike:
- motivaciju i sposobnost izvora prijetnje
- značajke određene ranjivosti
- postojanje i djelotvornost postojećih kontrola.

Vjerojatnost da izvor prijetnje iskoristi ranjivost može se iskazati pridruživanjem neke empirijske skale za mjerenje vjerojatnosti (npr. od 0 do 1) ili upotrebom unaprijed određenog načina stupnjevanja kao npr. mala, srednja i velika vjerojatnost.

Rezultat: ocjena vjerojatnosti

3.1.6. Analiza učinka

Analiza učinka je procjenjivanje negativnog učinka koji bi mogao nastati ukoliko prijetnja uspješno iskoristi ranjivost. Osnovne informacije potrebne za analizu učinka uključuju barem sljedeće:

- svrhu sustava (primjerice procesa koje obavlja informacijski sustav)
- važnost sustava i podataka za poslovanje banke
- osjetljivost podataka i sustava.

Navedene informacije moguće je dobiti iz analize utjecaja na poslovanje, klasifikacije informacija te prikupljanjem informacija od zaposlenika i ostalih izvora.

Na temelju dobivenih informacija potrebno je procijeniti negativan učinak nekog neželjenog događaja. Negativan učinak događaja moguće je opisati kao narušavanje funkcionalnosti ili gubitak odnosno kompromitiranje bilo kojeg temeljnog načela informacijskog sustava ili kombinacije tih načela.

Pojedine učinke moguće je mjeriti kvantitativno, u obliku izgubljenog prihoda, troškova popravka sustava ili vremena koje je potrebno uložiti kako bi se riješili problemi nastali izvršenjem prijetnje. Drugi učinci (npr. gubitak povjerenja javnosti, gubitak kredibiliteta, šteta načinjena interesima banke) ne mogu se mjeriti određenim mjernim jedinicama, ali ih je moguće odrediti ili opisati kvalitativno (npr. kao male, srednje i velike učinke).

Rezultat: izvješće o procijenjenoj razini učinka

3.1.7. Utvrđivanje rizika

Svrha ove radnje jest procijeniti razinu rizika kojem je izložen informacijski sustav banke. Utvrđivanje rizika izloženosti određenoj kombinaciji prijetnje i ranjivosti može se izraziti kao funkcija:

- vjerojatnosti da će identificirani izvor prijetnje iskoristiti određenu ranjivost
- jačine (razine) učinka ako izvor prijetnje uspješno iskoristi ranjivost.

Prilikom utvrđivanja razine rizika potrebno je uzeti u obzir i prikladnost planiranih ili postojećih kontrola za smanjivanje ili uklanjanje rizika te učestalost pojave neželjenih događaja.

Jedan od načina mjerenja rizika jest izrada matrice razine rizika i ljestvice rizika.

Matrica razine rizika

Razina rizika utvrđuje se množenjem ocjene koja je dodijeljena vjerojatnosti da izvor prijetnje iskoristi ranjivost s ocjenom učinka neželjenog događaja, pri čemu se uzima u obzir prikladnost planiranih ili postojećih kontrola. Tablica br. 2 daje jednostavan primjer kako se mogu odrediti rizici na temelju podataka o vjerojatnosti da izvor prijetnje iskoristi ranjivost i o učinku.

Primjer u tablici br. 2 jest matrica vjerojatnosti da izvor prijetnje iskoristi ranjivost (velika, srednja i mala) i učinka (velikog, srednjeg i malog), koja prikazuje kako se računa ukupna razina rizika. Na primjer:

- ocjena vjerojatnosti da izvor prijetnje iskoristi ranjivost koja se pripisuje svakoj razini vjerojatnosti prijetnje jest 1,0 za veliku, 0,5 za srednju i 0,1 za malu;
- ocjena učinka koja se dodjeljuje svakoj razini jačine učinka jest 100 za veliku, 50 za srednju i 10 za malu.

Ovisno o potrebama i detaljnosti procjene rizika može se koristiti matrica proizvoljnih dimenzija.

Tablica br. 2 Matrica razine rizika (engl. *Risk-Level Matrix*)

Vjerojatnost da izvor prijetnje iskoristi ranjivost	**Učinak**		
	Mali (10)	Srednji (50)	Veliki (100)
Velika (1,0)	10 x 1,0 = **10**	50 x 1,0 = **50**	
Srednja (0,5)	10 x 0,5 = **5**	50 x 0,5 = **25**	100 x 0,5 = **50**
Mala (0,1)	10 x 0,1 = **1**	50 x 0,1 = **5**	100 x 0,1 = **10**

Ljestvica rizika

Tablica br. 3 opisuje razine rizika prikazane u tablici br. 2. Ljestvica rizika s pripadajućim ocjenama predstavlja stupanj ili razinu rizika kojem su izloženi resursi informacijskog sustava ako je iskorištena određena ranjivost. Stupanj ili razina rizika određuje aktivnosti koje bi se trebale poduzeti.

Tablica br. 3 Primjer ljestvice rizika i aktivnosti koje je potrebno poduzeti

Razina rizika	**Opis rizika i aktivnosti koje je potrebno poduzeti**
Velik rizik (veći od 51)	Ako je rizik procijenjen kao velik, nužno je hitno provođenje mjera za smanjenje rizika. Postojeći sustav može nastaviti raditi, ali nužno je u što kraćem roku sastaviti plan provođenja mjera te odrediti prioritete i rokove.
Srednji rizik (11 do 50)	Ako je rizik procijenjen kao srednji, nužno je provođenje mjera za smanjenje rizika. Potrebno je sastaviti plan provođenja mjera kako bi se one provele u razumnom vremenu.
Malen rizik (1 do 10)	Ako je rizik procijenjen kao malen, potrebno je utvrditi je li nužno provođenje mjera za smanjenje rizika ili se rizik može prihvatiti.

Ako je razina nekih elemenata (vjerojatnosti, učinka ili rizika) tako mala da se može okarakterizirati kao "zanemariva" ili nevažna (primjerice vrijednost je < 1 na ljestvici od 0 do 100), potrebno ju je posebno zabilježiti. Time se osigurava da isti elementi budu uključeni u sljedeću procjenu. Navedeno je posebno važno jer "zanemarivi" rizici mogu s vremenom prerasti u rizike zbog kojih je potrebno poduzeti određene aktivnosti.

Rezultat:

- **matrica razine rizika**
- **ljestvica rizika i aktivnosti koje je potrebno poduzeti**

3.1.8. Predlaganje mjera

Predložene mjere jedan su od rezultata procesa procjene rizika. Cilj predloženih mjera jest smanjiti razinu rizika kojem je izložen informacijski sustav na prihvatljivu razinu. Prilikom predlaganja mjera za smanjenje ili otklanjanje utvrđenih rizika treba uzeti u obzir, između ostalog, sljedeće čimbenike:

- djelotvornost predloženih mjera
- važeće propise
- interne akte banke
- utjecaj na poslovne procese
- utjecaj na temeljna načela informacijskog sustava.

U procesu smanjenja rizika odabiru se najprikladnije predložene mjere te se slijedom toga provode uvođenjem novih ili izmjenom postojećih kontrola.

Rezultat: izvješće o predloženim mjerama za smanjivanje rizika

3.1.9. Izvješće o procjeni rizika

Nakon završetka procjene rizika (određena su obilježja sustava, identificirane prijetnje i ranjivosti, procijenjeni rizici te predložene mjere) potrebno je dokumentirati rezultate u obliku formalnog izvješća. Izvješće o procjeni rizika pomaže upravi banke i drugim odgovornim osobama da donesu odluke o promjenama internih akata i proračuna te odluke o operativnim i upravljačkim promjenama. Izvješće o procjeni rizika trebalo bi biti sastavljeno na sistematičan, analitičan i afirmativan način koji će upravi banke omogućiti prepoznavanje rizika i promovirati potrebu alociranja sredstva kako bi utvrđeni rizici bili smanjeni na prihvatljivu razinu, a potencijalni gubici izbjegnuti.

Rezultat: izvješće o procjeni rizika

3.2. Smanjivanje rizika

Smanjivanje rizika uključuje određivanje prioriteta, procjenu, odabir i provođenje adekvatnih zaštitnih mjera za smanjivanje rizika (predloženih u sklopu procesa procjene rizika) s obzirom na učestalost pojave neželjenih događaja i njihov učinak. Budući da je uklanjanje svih rizika kojima je izložen informacijski sustav gotovo nemoguće, banka bi trebala poduzeti sve potrebne radnje kako bi smanjila rizik informacijskog sustava na prihvatljivu razinu provođenjem adekvatnih zaštitnih mjera. Prilikom provođenja mjera potrebno je posebnu pozornost posvetiti smanjenju najznačajnijih rizika (kombinacija prijetnja i ranjivosti koje mogu potencijalno uzrokovati značajan negativan učinak) na prihvatljivu razinu uz najmanji mogući utjecaj na ostale poslovne procese. Smanjivanje rizika identificiranih u procesu procjene rizika može se postići na sljedeće načine:

- **Izbjegavanjem rizika.** Izbjegavanje rizika uklanjanjem uzroka rizika i/ili posljedica (npr. odričući se određenih funkcija sustava ili prestankom korištenja sustava kad su rizici otkriveni).
- **Ograničavanjem rizika.** Ograničavanje rizika provođenjem mjera (npr. primjenom preventivnih i detekcijskih kontrola) kojima se smanjuju potencijalni negativni učinci na prihvatljivu razinu.
- **Prenošenjem rizika.** Prenošenje rizika pomoću drugih načina naknade pretrpljene štete (npr. ugovaranjem osiguranja).

Pri odabiru bilo koje od ovih mogućnosti smanjenja rizika potrebno je uzeti u obzir poslovne ciljeve i zadatke banke te potrebu za očuvanjem temeljnih načela informacijskog sustava.

Ukoliko banka u procesu procjene rizika utvrdi da je rizik prihvatljiv, odnosno da nije potrebno njegovo daljnje smanjivanje, navedeni je rizik moguće prihvatiti donošenjem odluke o prihvaćanju preostalih rizika.

Smanjivanje rizika trebalo bi obuhvatiti sljedeće radnje:

1. određivanje prioriteta aktivnosti
2. procjenu predloženih mjera za smanjivanje rizika
3. provođenje analize isplativosti
4. odabir mjera za smanjivanje rizika
5. dodjeljivanje odgovornosti
6. izradu plana provođenja odabranih mjera
7. utvrđivanje preostalih rizika.

3.2.1. Određivanje prioriteta aktivnosti

Prioriteti provođenja aktivnosti određuju se na temelju utvrđenih razina rizika sadržanih u ljestvici rizika i u izvješću o procjeni rizika. Višim razinama rizika dodijelit će se viši prioriteti (primjerice aktivnosti povezane s rizikom kojem je dodijeljena ocjena rizika vrlo visok ili visok, imat će najviši prioritet). U skladu s dodijeljenim prioritetima potrebno je provesti mjere kako bi se smanjili rizici kojima je izložen informacijski sustav i zaštitili poslovni ciljevi.

Rezultat: popis aktivnosti ocijenjenih prema prioritetima

3.2.2. Procjena predloženih mjera za smanjivanje rizika

Pri procjenjivanju predloženih mjera potrebno je analizirati njihovu izvedivost (npr. kompatibilnost, prihvaćanje od strane korisnika) i djelotvornost (npr. stupanj zaštite i razinu smanjivanja rizika) zato što neke od predloženih mjera nisu uvijek i najprikladnija ili najisplativija rješenja za banku i informacijski sustav. Cilj je ove radnje odabrati najprikladniju mjeru kako bi se rizik smanjio na prihvatljivu razinu.

Rezultat: popis prikladnih mjera

3.2.3. Provođenje analize isplativosti

Analiza isplativosti prikladnih mjera provodi se kako bi se olakšalo donošenje odluka i utvrdila isplativost provođenja navedenih mjera. Rezultati analize mogu se iskazati kvalitativno ili kvantitativno. Svrha takve analize jest utvrđivanje mjera čiji će troškovi provođenja biti opravdani smanjenjem razine rizika na prihvatljivu razinu.

Rezultat: izvješće o analizi isplativosti koja opisuje troškove i prednosti provođenja mjera ili razloge zbog kojih mjere nisu isplative

3.2.4. Odabir mjera za smanjivanje rizika

Svrha ove radnje jest odabrati najdjelotvornije mjere za smanjivanje rizika. Odabrane mjere trebale bi kombinirati upravljačke, logičke i fizičke elemente.

Rezultat: popis odabranih mjera za smanjivanje rizika

3.2.5. Dodjeljivanje odgovornosti

Svrha ove radnje jest odabir osoba (zaposlenika banke ili vanjskih suradnika) koje raspolažu adekvatnim znanjem i vještinama potrebnim za provođenje odabranih mjera te dodjeljivanje odgovornosti za provođenje mjera.

Rezultat: popis dodijeljenih odgovornosti

3.2.6. Izrada plana provođenja odabranih mjera

Svrha ove radnje jest izrada plana prema kojem će se provoditi odabrane mjere za smanjenje rizika. Provođenje odabranih mjera ostvaruje se uvođenjem novih ili izmjenom postojećih kontrola. Plan provođenja odabranih mjera treba sadržavati barem sljedeće:

- rizike (kombinacije ranjivosti i prijetnja) i pripadajuće razine rizika (rezultate izvješća o procjeni rizika)

- predložene mjere (rezultat izvješća o predloženim mjerama za smanjivanje rizika)
- ocjenu prioriteta (u skladu s razinama rizika)
- odabrane mjere (na temelju popisa odabranih mjera za smanjivanje rizika)
- resurse potrebne za provođenje odabranih zaštitnih mjera
- popise odgovornih osoba
- datume početka i završetka provedbe odabranih zaštitnih mjera.

Rezultat: plan provođenja odabranih mjera

3.2.7. Utvrđivanje preostalih rizika

U većini slučajeva provedene mjere za smanjivanje rizika rezultiraju smanjenjem, ali ne i potpunim otklanjanjem rizika, što upućuje na postojanje preostalih (rezidualnih) rizika. Nakon provođenja odabranih mjera potrebno je utvrditi preostale rizike te donijeti odluku o prihvaćanju preostalih rizika ili poduzimanju radnja za daljnje smanjenje rizika.

Rezultat: popis preostalih (rezidualnih) rizika

3.3. Kontrole

Provođenje odabranih mjera za smanjivanje rizika ostvaruje se uvođenjem novih ili izmjenom postojećih kontrola. Kontrole je moguće podijeliti na sljedeće tri kategorije: upravljačke, logičke (tehničke) i fizičke. Budući da je informacijski sustav siguran onoliko koliko je siguran njegov najranjiviji dio, nužan je slojevit pristup u izgradnji sigurnosne infrastrukture, koji uključuje različite kombinacije upravljačkih, logičkih i fizičkih kontrola. Korištenjem navedenih kategorija kontrola značajno se smanjuje rizik od narušavanja temeljnih načela informacijskog sustava.

Pravilnim provođenjem kontrola moguće je spriječiti ili ograničiti štetu koju izvor prijetnje može nanijeti banci, odnosno smanjiti rizik informacijskog sustava.

Kontrole (slično kao i zaštitne mjere) dijele se i prema njihovim ulogama na kontrole:

1. prevencije
2. odvraćanja
3. otkrivanja
4. ograničavanja
5. korigiranja
6. oporavka
7. nadzora
8. osvješćivanja.

3.3.1. Upravljačke kontrole

Upravljačke se kontrole provode donošenjem i primjenom internih akata radi osiguranja funkcionalnosti i sigurnosti te očuvanja temeljnih načela informacijskog sustava banke. Primjeri upravljačkih kontrola jesu:

- dodjeljivanje odgovornosti
- razvijanje i održavanje politike sigurnosti informacijskog sustava te ostalih internih akata vezanih uz informacijski sustav
- uvođenje sigurnosne kontrole zaposlenika (primjerice razdvajanje dužnosti, princip dodjeljivanja prava korištenja informacijskog sustava samo do razine koja je nužno potrebna za izvršavanje radnih zadataka, dodjeljivanje posebnih dozvola, rotacija dužnosti te dodjeljivanje i ukidanje prava pristupa informacijskom sustavu)
- kontrole vezane uz radnje koje je potrebno provoditi prilikom zapošljavanja, prekida radnog odnosa, premještaja u drugu organizacijsku jedinicu i promaknuća
- provođenje izobrazbe te podizanje razine svijesti o rizicima informacijskog sustava kako bi se osiguralo da krajnji korisnici i ostali korisnici sustava budu upoznati s njima te s pravilima ponašanja i odgovornostima
- provođenje periodičnih nadzora i provjera djelotvornosti kontrola
- provođenje periodične revizije informacijskog sustava
- uspostava kontinuiranog procesa upravljanja rizikom radi procjene i smanjenja rizika
- uspostava procesa planiranja kontinuiteta poslovanja
- provođenje testiranja.

3.3.2. Logičke kontrole

Kontrole na softverskim i hardverskim komponentama informacijskog sustava nazivamo logičkim kontrolama. Primjeri logičkih kontrola jesu:

- softverske i hardverske kontrole za utvrđivanje autentičnosti, autorizaciju, provođenje obavezne kontrole pristupa te osiguranje neporecivosti radnja, zaštićenosti komunikacijskih kanala i povjerljivosti transakcija
- kontrole pristupa informacijskom sustavu kao što su: kombinacija korisničko-identifikacijske oznake i zaporke, PKI infrastruktura, biometrijske kontrole, autentifikacija pomoću "pametne kartice" (engl. *smart card*) i slično
- upotreba kriptografskih metoda u svrhu zaštite informacija u postupku njihovog prijenosa kroz telekomunikacijsku mrežu, te za vrijeme pohrane
- upotreba sistemskih i operativnih zapisa kako bi se bilježile aktivnosti koje su učinjene unutar telekomunikacijske mreže, na mrežnom uređaju ili na pojedinom računalu
- upotreba usmjernika, preklopnika, vatrozida i ostalih mrežnih komponenata u svrhu kontrole pristupa mrežnim resursima te izdvajanja i zaštite pojedinih segmenata unutar mreže
- upotreba metoda za otkrivanje neovlaštenog pristupa i radnja na informacijskom sustavu
- upotreba metoda za otkrivanje pogrešaka u podacima i narušavanja njihova integriteta
- metode otkrivanja, sprječavanja širenja i uništavanja malicioznog koda.

3.3.3. Fizičke kontrole

Fizičke kontrole štite i osiguravaju resurse informacijskog sustava od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja. Fizičke kontrole trebaju pružiti potporu upravljačkim i logičkim kontrolama i zajednički djelovati kako bi se rizik informacijskog sustava sveo na prihvatljivu razinu. Primjeri fizičkih kontrola jesu:

- metode fizičke zaštite opipljive imovine (osobnih računala, poslužitelja, mrežnih uređaja, kabela, medija, građevina i slično) od neovlaštenog pristupa
- mehanizmi nadzora okoline (videonadzor prostorija banke, osvjetljivanje okoline, detektori pokreta, senzori, alarmi i slično)
- biometrijske kontrole pristupa informacijskim resursima
- kontrola vlage, temperature, dima i slično
- fizičko odvajanje dijelova telekomunikacijske mreže
- mehanizmi osiguravanja pričuvnog izvora napajanja električnom energijom (npr. sustav za neprekinuto napajanje električnom energijom, generatori).

3.4. Klasifikacija informacija

Banka mora čuvati povjerljive podatke u skladu s važećim propisima. Informacije je potrebno klasificirati u različite grupe prema stupnju njihove osjetljivosti (npr. jako osjetljive, osjetljive i neosjetljive) s obzirom na moguće posljedice narušavanja temeljnih načela informacijskog sustava. Osjetljiva informacija je bilo koja informacija čije razotkrivanje, privremeni ili trajni gubitak, zlouporaba ili neovlaštena modifikacija mogu negativno utjecati na interese banke i klijenata te na usklađenost s važećim propisima.

Banka bi trebala odrediti grupe u koje će se informacije klasificirati, te odrediti smjernice i pravila za svrstavanje u pojedinu grupu. Na temelju toga svaku informaciju potrebno je klasificirati (svrstati u neku od definiranih grupa). Cilj klasifikacije informacija jest postizanje odgovarajućeg stupnja zaštite informacija pri čemu treba uzeti u obzir njihovu osjetljivost. Banka bi trebala donijeti i interne akte kojima bi se definirali kriteriji i postupci te odgovornosti za provođenje klasifikacije informacija. Banka također mora osigurati da informacije pohranjene na različitim medijima budu adekvatno zaštićene te uspostaviti siguran proces odlaganja i uništavanja tih medija.

4. Unutarnja revizija

U skladu s odredbama Zakona o bankama ("Narodne novine", broj 84/2002., u nastavku teksta: ZOB), banka mora organizirati unutarnju reviziju koja će neovisno i objektivno obavljati svoje poslove te koja će svojim savjetima i preporukama pridonositi unapređivanju poslovanja banke. Jedan od zadataka unutarnje revizije jest obavljanje stalnog nadzora nad cjelokupnim poslovanjem banke kako bi se provjerilo upravlja li banka sustavno rizicima koji proizlaze iz poslovnih aktivnosti banke u skladu s načelima stabilnog poslovanja, što uključuje upravljanje resursima informacijske i pridruženih tehnologija.

Unutarnja revizija treba obavljati i poslove revizije informacijskog sustava, iz čega proizlazi da unutarnja revizija treba biti organizirana tako da se osigura sustavno obavljanje revizije informacijskog sustava. Obavljanje revizije informacijskog sustava banke, za potrebe ovog dokumenta, nazivamo unutarnjom revizijom informacijskog sustava.

Kako bi se unutarnja revizija informacijskog sustava banke provela na zadovoljavajući i djelotvoran način, osobe koje obavljaju unutarnju reviziju informacijskog sustava trebale bi:

- posjedovati stručna znanja i vještine, iskustvo te razinu kvalifikacija u skladu s veličinom i složenošću informacijskog sustava banke
- koristiti se metodologijom za provođenje revizije informacijskog sustava temeljenom na procjeni rizika koja bi detaljno definirala kriterije, način i postupke provođenja revizije informacijskog sustava te osigurala dosljednost i sveobuhvatnost revizije informacijskog sustava
- razmotriti dobre prakse upotrebe softverskih alata za provođenje revizije i kontrolu informacijskog sustava
- evidentirati, prikupiti i arhivirati dokumentaciju na temelju koje je sastavljeno izvješće o provedenoj reviziji imajući u vidu potrebu za adekvatnom zaštitom osjetljivih informacija.

Banka bi trebala kontinuirano obavljati unutarnju reviziju informacijskog sustava i definirati razdoblje (ciklus) unutar kojeg će obaviti unutarnju reviziju cjelokupnoga informacijskog sustava.

Prilikom sastavljanja godišnjeg programa rada te određivanja predmeta, obuhvata i učestalosti revizije pojedinih područja informacijskog sustava potrebno je uzeti u obzir i rukovoditi se sljedećim:

- obavljenom procjenom rizika informacijskog sustava banke
- iskustvom te dobrim praksama u reviziji informacijskih sustava
- raspoloživim resursima
- novim saznanjima o informacijskom sustavu.

Na temelju godišnjeg programa rada unutarnje revizije potrebno je donijeti i operativne planove rada za unutarnju reviziju informacijskog sustava. Operativni planovi rada za unutarnju reviziju informacijskog sustava trebali bi sadržavati barem sljedeće:

- ciljeve i opseg revizija
- popis područja koja će biti predmetom revizija
- popis predmeta revizije unutar svakog područja
- vremenski raspored revizija koje će se obaviti u razdoblju obuhvaćenom planom

- trajanje revizija.

Na temelju provedene revizije informacijskog sustava unutarnja revizija informacijskog sustava trebala bi sastaviti pisano izvješće o obavljenoj reviziji informacijskog sustava koje bi trebalo sadržavati barem sljedeće:

- popis revidiranih područja
- popis osoba koje su sudjelovale u reviziji
- cilj i opseg revizije
- ocjenu revidiranih područja
- nedostatke i slabosti revidiranih područja
- nezakonitosti i nepravilnosti, ako su utvrđene tijekom obavljanja revizije informacijskog sustava
- prijedloge, preporuke i rokove za otklanjanje utvrđenih nezakonitosti, nepravilnosti, nedostataka i slabosti.

Unutarnja revizija trebala bi sastaviti izvješća o radu u skladu s rokovima utvrđenima operativnim planom rada. Izvješća o radu trebala bi sadržavati i izvješća o obavljenim revizijama informacijskog sustava.

Dobre prakse nalažu da unutarnja revizija informacijskog sustava bude uključena u revidiranje projekata i/ili njihovih faza (primjerice razvoj aplikacija, nabava, migracija sustava, integracije sustava), kao i ostalih aktivnosti vezanih uz informacijski sustav (primjerice upravljanje informacijskim sustavom, planiranje kontinuiteta poslovanja, eksternalizacija (dijela) informacijskog sustava) koje mogu imati znatan utjecaj na funkcionalnost i sigurnost informacijskog sustava.

5. Sigurnost informacijskog sustava

Sigurnost je odgovornost svih upravljačkih razina banke te je vrlo važna u svim fazama životnog ciklusa informacijskog sustava. Sigurnost informacijskog sustava obuhvaća sve aspekte povezane s definiranjem, ostvarivanjem i održavanjem temeljnih načela informacijskog sustava.

Kako bi se postigla i održala adekvatna razina sigurnosti informacijskog sustava, dobre prakse nalažu rukovođenje sljedećim načelima:

1. načelom zabrane svih radnja koje nisu eksplicitno dopuštene na temelju dodijeljenih ovlasti
2. načelom dodjele najmanjih mogućih ovlasti resursima informacijskog sustava (uključujući osobe, sustave i procese) koje omogućuju djelotvorno poslovanje.

5.1. Politika sigurnosti informacijskog sustava

Politika sigurnosti informacijskog sustava temeljni je okvir za upravljanje sigurnošću informacijskog sustava banke i trebala bi odražavati općeprihvaćena načela sigurnosti. Politika sigurnosti informacijskog sustava trebala bi sadržavati načela i principe upravljanja sigurnošću resursa informacijskog sustava te odgovornosti koje se odnose na sigurnost informacijskog sustava.

Banka bi trebala donijeti politiku sigurnosti informacijskog sustava, upoznati korisnike informacijskog sustava s njom te imenovati osobu odgovornu za praćenje provođenja te politike. Cilj donošenja politike sigurnosti informacijskog sustava jest osiguranje adekvatne razine sigurnosti informacijskog sustava. Politika sigurnosti informacijskog sustava trebala bi obuhvatiti područja upravljačke, logičke i fizičke zaštite resursa informacijskog sustava u skladu s veličinom, obuhvatom i kompleksnosti informacijskog sustava. Na temelju politike sigurnosti informacijskog sustava banka bi trebala propisati i primijeniti detaljne interne akte koji se odnose na sve aspekte sigurnosti informacijskog sustava. Politiku sigurnosti informacijskog sustava potrebno je usklađivati s promjenama u informacijskom sustavu i u njegovoj okolini, u slučajevima narušavanja sigurnosti informacijskog sustava, te ovisno o rezultatima procjene rizika. Politika sigurnosti informacijskog sustava treba sadržavati barem sljedeće:

- cilj i opseg politike sigurnosti informacijskog sustava
- načela upravljanja sigurnošću informacijskih resursa
- opće i posebne odgovornosti koje se odnose na sigurnost informacijskog sustava.

Načela upravljanja sigurnošću resursa informacijskog sustava trebala bi obuhvatiti barem sljedeća područja:

- upravljanje rizikom informacijskog sustava
- klasifikaciju informacija
- upravljanje sigurnošću komunikacijskih i distribucijskih kanala
- osiguravanje kontinuiteta poslovanja banke
- upravljanje incidentima
- oporavak informacijskog sustava
- upravljanje pričuvnom pohranom
- razvoj informacijskih sustava unutar banke
- upravljanje odnosima s pružateljima usluga i dobavljačima opreme
- upravljanje kontrolama pristupa resursima informacijskog sustava
- fizičku sigurnost
- upravljanje operativnim i sistemskim zapisima
- zaštitu od malicioznog koda
- upravljanje imovinom informacijskog sustava
- upravljanje promjenama
- upravljanje konfiguracijama
- upravljanje dokumentacijom
- izobrazbu korisnika informacijskog sustava.

Politika sigurnosti informacijskog sustava treba biti djelotvorna i primjenjiva kako bi se omogućilo ostvarivanje poslovnih ciljeva banke.

5.2. Upravljanje kontrolama pristupa

Kontrole pristupa omogućuju provođenje radnja nad resursima informacijskog sustava (primjerice korištenje, mijenjanje, pregled) u skladu s dodijeljenim ovlastima. Pristup se može definirati kao svojstvo koje omogućuje obavljanje različitih radnja na informacijskom sustavu. Kontrolama pristupa eksplicitno se omogućava, ograničava ili zabranjuje pristup resursima informacijskog sustava, i to korištenjem pojedine kontrole ili kombinacijom upravljačkih, logičkih i fizičkih kontrola. Proces kontrole pristupa obuhvaća uvođenje niza pojedinačnih kontrola pristupa. Cilj uvođenja kontrola pristupa jest sprječavanje neovlaštenog pristupa resursima informacijskog sustava. Pri implementaciji kontrola pristupa potrebno je uzeti u obzir sigurnosne zahtjeve, zahtjeve poslovnih procesa i jednostavnost korištenja za korisnike.

5.2.1. Kriteriji pristupa resursima

Banka bi trebala kontrolirati pristup resursima informacijskog sustava primjenjujući, prema potrebi, neke od sljedećih kriterija:

- **Identitet korisnika.** Identitet korisnika mora biti jedinstven kako bi se mogle utvrditi ovlasti i odgovornosti svakog korisnika.
- **Funkcija.** Pristup informacijama mora biti kontroliran na temelju dodijeljenih poslova i dužnosti u skladu s načelima podjele poslova i segregacije dužnosti. Navedeno uključuje određivanje radnja koje se mogu obavljati nad resursima informacijskog sustava (primjerice pravo čitanja, pisanja, izvršavanja i brisanja).
- **Lokacija.** Identifikacija i autentifikacija mogu ovisiti i o fizičkoj i logičkoj lokaciji osobe, procesa ili sustava koji zahtijevaju pristup (primjerice kada korisnici pristupaju s lokacije koja se nalazi unutar banke, mogu im se dopustiti veće ovlasti nego kada pristupaju putem javno dostupnih telekomunikacijskih mreža).
- **Vrijeme.** Ograničenje kojim se onemogućuje pristup u određenom razdoblju tijekom dana ili određenih dana u tjednu odnosno u mjesecu (primjerice korištenje nekih resursa može biti dopušteno samo tijekom radnog vremena).
- **Transakcija.** Pristup resursima informacijskog sustava može biti ograničen ovisno o tijeku poslovnog procesa (primjerice isplatu s računa nije moguće obaviti dok se provodi neka druga isplata ili uplata na taj račun).

5.2.2. Upravljanje korisničkim pravima

Svakom resursu informacijskog sustava može se pristupati od strane nekog drugog resursa (koji može, ali i ne mora biti dio informacijskog sustava banke), uključujući i osobe. Prava pristupa koja su veća od onih koja su minimalno potrebna za obavljanje poslova, izlažu informacijski sustav banke riziku narušavanja temeljnih načela informacijskog sustava. Prema tome, cilj upravljanja pravima pristupa jest identificirati pristup i ograničiti pristup pojedinom resursu na minimalnu razinu dovoljnu za djelotvorno obavljanje radnih zadataka.

Upravljanje korisničkim pravima (pri tome se misli na osobe, sustave i procese) sastoji se od četiriju procesa:

- **Evidentiranje.** Podrazumijeva dodavanje novih korisnika informacijskog sustava. Ovim procesom utvrđuje se identitet korisnika te određuju informacije i sustavi potrebni za obavljanje radnih zadataka u skladu s opisom radnoga mjesta.
- **Autorizacija.** Podrazumijeva dodjelu prava pristupa korisnika informacijskom sustavu banke. Navedeno obuhvaća dodavanje, brisanje ili modificiranje dodijeljenih prava pristupa operativnim sustavima, aplikacijama i specifičnim vrstama informacija. Postupak dodjele prava pristupa treba biti formaliziran te sva prava trebaju odobriti ovlaštene osobe.
- **Identifikacija i autentifikacija.** Podrazumijeva identifikaciju korisnika i potvrdu njegova identiteta prilikom prijave i tijekom provođenja radnja na informacijskom sustavu.
- **Nadzor.** Obuhvaća praćenje, izmjenu i revidiranje prava pristupa korisnika informacijskog sustava.

Banka bi trebala uspostaviti djelotvoran proces upravljanja korisničkim pravima pristupa. Navedeni proces trebao bi uključiti sljedeće kontrole:

- dodjeljivanje korisnicima prava pristupa koja su strogo ograničena na one kontrole koje su potrebne za obavljanje redovnih poslovnih zadataka
- ažuriranje prava pristupa (primjerice na temelju kadrovskih promjena, promjena na informacijskom sustavu i njegovu okruženju)
- periodično pregledavanje korisničkih prava pristupa (učestalost pregledavanja trebala bi se temeljiti na procjeni rizika).

5.2.3. Identifikacija i autentifikacija

Identifikacija i autentifikacija ključne su komponente u izgradnji sigurnosti informacijskog sustava jer su osnova za mnoge vrste kontrola pristupa i utvrđivanja odgovornosti korisnika (dokazivost). Utvrđivanje odgovornosti korisnika zahtijeva povezivanje aktivnosti na informacijskom sustavu s točno određenim osobama, procesima ili sustavima te je u tu svrhu potrebno da ih informacijski sustav identificira i autentificira.

5.2.3.1. Identifikacija

Identifikacija je proces kojim korisnik predočava informacijskom sustavu zahtijevani identitet. Identifikacija na informacijskim sustavima najčešće se provodi pomoću jedinstvene korisničko-identifikacijske oznake (engl. *User ID*). Pri upotrebi navedene oznake potrebno je obratiti posebnu pozornost na sljedeće:

- **Jedinstvenu identifikaciju.** Potrebno je osigurati jedinstvenu identifikaciju svakom korisniku informacijskog sustava. U određenim slučajevima može se dopustiti upotreba grupnog identiteta, no to je poželjno izbjegavati jer onemogućuje dokazivost.
- **Upravljanje jedinstvenim korisničko-identifikacijskim oznakama.** Ovlasti za rad na sustavu potrebno je pratiti i ažurirati. Kako bi se omogućilo praćenje povijesnih aktivnosti korisnika, potrebno je procijeniti potrebu za čuvanjem korisničko-identifikacijske oznake i nakon ukidanja korisnikovih ovlasti.

- **Neaktivne jedinstvene korisničko-identifikacijske oznake.** Korisnike koji su u određenom razdoblju neaktivni na pojedinom resursu informacijskog sustava, treba analizirati i prema procjeni dezaktivirati njihove oznake i ukinuti ovlasti.
- **Uzajamnu povezanost aktivnosti i korisnika.** Informacijski sustav treba osigurati praćenje identiteta svih korisnika i biti sposoban povezati aktivnosti s točno određenim korisnicima.

5.2.3.2. Autentifikacija

Autentifikacija je proces kojim se potvrđuje korisnički identitet koji zahtijeva pristup informacijskom sustavu. Postoje tri načina utvrđivanja neospornosti korisničkog identiteta koji se mogu primjenjivati samostalno ili u kombinaciji:

- nešto što samo korisnik zna (primjerice zaporka, PIN, kriptografski ključ)
- nešto što samo korisnik posjeduje (primjerice "token", magnetska kartica, "pametna kartica")
- nešto što korisnik jest (primjerice biometrijske metode kao što su otisak prsta, skeniranje rožnice, prepoznavanje glasa i slično).

Banka bi trebala osigurati barem sljedeće:

- **Autentificiranje korisnika.** Banka bi trebala zahtijevati od korisnika da potvrdi svoj identitet na informacijskom sustavu. Isto tako, banka bi u skladu s procjenom rizika trebala razmotriti i mogućnost autentifikacije korisnika pomoću metode samo jedne prijave (engl. *single sign-on*) kojom se pristupa različitim resursima informacijskog sustava.
- **Ograničen pristup autentifikacijskim oznakama.** Autentifikacijske oznake trebaju biti adekvatno zaštićene (primjerice primjenom rigoroznih kontrola pristupa i jednosmjernim kriptiranjem) kako bi se spriječilo da neovlašteni korisnici dođu u posjed navedenih oznaka.
- **Siguran prijenos autentifikacijskih oznaka.** Banka bi trebala adekvatno zaštititi autentifikacijske oznake prilikom njihova prijenosa javno dostupnim ili privatnim telekomunikacijskim mrežama.
- **Ograničiti broj pokušaja pristupa.** Banka bi trebala ograničiti broj neuspjelih pokušaja pristupa, odnosno onemogućiti upotrebu korisničko-identifikacijske oznake nakon određenog broja neuspjelih pokušaja pristupa resursima informacijskog sustava.
- **Zaštita autentifikacijskih oznaka prilikom unošenja.** Banka bi trebala adekvatno zaštititi autentifikacijske oznake od kompromitiranja prilikom unosa u informacijski sustav (primjerice skrivanje zaporka pri unosu).
- **Upravljanje autentifikacijskim oznakama.** Banka bi trebala adekvatno upravljati autentifikacijskim oznakama (primjerice definirati postupke za aktivaciju autentifikacijskih oznaka i dezaktivaciju izgubljenih i ukradenih oznaka).

5.2.4. Upravljanje zaporkama

Zaporke su najčešće upotrebljavan mehanizam autentifikacije korisnika. Međutim, zbog neprimjerenih navika korisnika informacijskog sustava (primjerice dijeljenja zaporka i njihove neadekvatne pohrane te upotrebe neprimjerenih zaporka) one su i jedan od najslabijih mehanizama autentifikacije. Primjereno upravljanje zaporkama (koje uključuje uklanjanje poznatih ranjivosti i prevenciju uobičajenih napada) može uvelike unaprijediti sigurnost informacijskog sustava.

Napadi na zaporke odnosno pokušaji njihova otkrivanja ili zaobilaženja jedna su od najčešćih vrsta napada na informacijske sustave. Neke od najčešćih podvrsta napada na zaporke jesu:

- pokušaj pogađanja zaporka isprobavanjem svih kombinacija dopuštenih simbola (engl. *dictionary attack*)
- pokušaj pogađanja zaporka pomoću specifičnih informacija o osobi koja rabi tu zaporku (primjerice ime supružnika, imena djece, ime kućnog ljubimca i slično)
- pokušaj neautorizirane autentifikacije pomoću standardnih zaporka koje inicijalno definiraju proizvođači hardvera, softvera i telekomunikacijske opreme
- pokušaj neautorizirane autentifikacije pomoću zaporka čija je povjerljivost narušena zbog neadekvatne pohrane.

Ovisno o procjeni rizika, odnosno riziku razotkrivanja zaporka i negativnom učinku koji može nastati kao posljedica tog razotkrivanja, banka bi trebala postići adekvatnu razinu zaštite zaporka pomoću upravljačkih, logičkih i fizičkih kontrola. Zbog mnogobrojnih ranjivosti koje proizlaze iz neadekvatnog korištenja zaporki, te velikog broja prijetnja koje pokušavaju iskoristiti te ranjivosti, banka bi trebala propisati restriktivne postupke upravljanja zaporkama, kako bi se osjetljivost na tu vrstu napada svela na najmanju moguću mjeru.

Pri upravljanju zaporkama banka bi trebala uzeti u obzir barem sljedeće:

- sve zaporke moraju biti povjerljive;
- zaporke ne smiju biti pohranjene ni prikazane u čitljivom (nekriptiranom) obliku izvan adekvatno osigurane okoline (primjerice u sefu);
- zaporke ne smije dijeliti više korisnika kako bi se osigurala dokazivost;
- potrebno je definirati razdoblje nakon kojega se zaporka mora izmijeniti te onemogućiti višekratnu upotrebu iste zaporke;
- zaporke je potrebno izmijeniti ukoliko se pojavi i najmanja sumnja da su njihova povjerljivost ili integritet narušeni;
- potrebno je propisati standarde kreiranja zaporka koji će biti u skladu s dobrim praksama i ograničenjima sustava za autentifikaciju te uključivati propisivanje:
    - najmanje dopuštene duljine zaporka
    - obavezne uporabe što šireg znakovnog skupa
    - nemogućnosti upotrebe tri ili više uzastopnih identičnih simbola u zaporci;
- pri prvoj upotrebi potrebno je izmijeniti prvobitne (inicijalne) i standardne zaporke, kao i ostale zaporke koje su zadali proizvođači i dobavljači informacijske opreme ili pružatelji usluga, a pomoću kojih se pristupa resursima banke;
- mogućnost autentifikacije pomoću određene zaporke potrebno je spriječiti ako korisnik više puta uzastopno pogriješi pri unosu te zaporke.

5.2.5. Mehanizmi kontrole pristupa

Prilikom implementiranja kontrola pristupa banka bi trebala razmotriti upotrebu, primjerice sljedećih mehanizama:

- **Pristupne liste** (engl. *Access Control Lists*)**.** Pristupne liste su evidencije korisnika (uključujući i grupe, sustave i procese) kojima su dane ovlasti za korištenje pojedinih resursa informacijskog sustava i poduzimanje radnja u vezi s njima.
- **Ograničeno korisničko sučelje.** Pristup pojedinim resursima i funkcijama informacijskog sustava ograničen je na radnje za koje je korisnik ovlašten, primjerice upotrebom dinamičkih izbornika, upotrebom prikaza podataka iz tablica baze podataka (engl. *database view*), upotrebom fizičkog ograničenja korisničkog sučelja na bankomatima i slično.
- **Kriptografija.** Kriptografske metode omogućuju primjenu sigurnijih kontrola pristupa. Da bi te metode bile djelotvorne, potrebno je uspostaviti rigorozan sustav upravljanja kriptografskim ključevima.
- **Vatrozidi i ostala sučelja između telekomunikacijskih mreža.** Navedeni uređaji filtriraju promet između povezanih telekomunikacijskih mreža i dopuštaju lokalnim korisnicima povezivanje s vanjskim mrežama, dok u isto vrijeme štite informacijski sustav banke od narušavanja temeljnih načela informacijskog sustava.

5.2.6. Pristup telekomunikacijskim mrežama banke

Mrežna sigurnost zahtijeva djelotvornu primjenu različitih vrsta kontrola kako bi se adekvatno zaštitio pristup resursima informacijskog sustava. Prema složenosti njezine telekomunikacijske mreže banka bi trebala ocijeniti i na odgovarajući način primijeniti upravljačke, logičke i fizičke kontrole. Dobre prakse nalažu uvođenje sljedećeg:

- grupiranje mrežnih poslužitelja, aplikacija, korisnika te ostalih resursa informacijskog sustava u sigurnosne zone, primjerice podjelu u zonu nad kojom banka nema potpunu kontrolu (npr. internet), zonu vanjskih pružatelja usluga i zone različitih grupa internih korisnika
- uspostavu odgovarajućih pravila pristupa unutar pojedine sigurnosne zone ili između više različitih zona
- primjenu odgovarajućih upravljačkih, logičkih i fizičkih kontrola kako bi se dosljedno udovoljilo prethodno navedenim pristupnim zahtjevima.

5.2.7. Pristup sistemskom softveru

Sistemski softver obuhvaća operativne sustave i sistemske uslužne programe. Banka bi trebala primjereno zaštititi pristup sistemskom softveru uzimajući u obzir sljedeće:

- ograničavanje pristupa sistemskim uslužnim programima
- ograničavanje upotrebe i nadzor povlaštenog pristupa
- evidentiranje i nadzor pristupa osjetljivim resursima od strane osoba, procesa ili sustava
- nadograđivanje operativnih sustava sigurnosnim programskim ispravkama (engl. *security patch*)

- zaštitu pristupnih točaka (uključujući i ograničenje broja pristupnih točaka), putem kojih se može pristupiti operativnom sustavu, primjenom logičkih i fizičkih kontrola.

5.2.8. Pristup aplikacijama

U skladu s procjenom rizika u aplikacije je potrebno ugraditi mehanizme kontrole pristupa kojima se ograničava pristup osobama, procesima i sustavima. Za ostvarivanje djelotvorne kontrole pristupa aplikaciji nužna je suradnja osoba zaduženih za sigurnost, zaposlenika koji sudjeluju u razvoju i održavanju aplikacije (uključujući dobavljače aplikacija i pružatelje usluga održavanja) te osoba odgovornih za poslovne procese. Banka bi trebala kontrolirati pristup aplikacijama koristeći, primjerice, sljedeće:

- mehanizme autentifikacije i autorizacije koji odgovaraju procjeni rizika pojedine aplikacije
- nadzor prava pristupa kako bi se osiguralo da su prava korisnika na razini minimalno potrebnih za obavljanje poslovnih zadataka
- pristup aplikaciji samo u određenom razdoblju (primjerice samo u radno vrijeme)
- evidentiranje pristupa i sigurnosnih događaja (primjerice praćenjem sistemskih i operativnih zapisa)
- softver koji omogućava brzu analizu aktivnosti korisnika.

5.2.9. Udaljeni pristup

Banka bi trebala biti svjesna mogućnosti koje pruža udaljeni pristup sustavu i ranjivosti koje iz toga proizlaze, te bi prema tome trebala definirati načine primjene i ograničenja udaljenog pristupa. Svrha je navedenog svođenje na najmanju moguću razinu izloženosti banke šteti koja može proizići iz neovlaštenog korištenja informacijskih resursa banke. Banka bi trebala zaštititi pristup svojim sustavima s udaljene lokacije uzimajući u obzir sljedeće:

- internim je aktima potrebno onemogućiti udaljeni pristup osim ako za to postoje opravdane poslovne potrebe
- potrebno je strogo kontrolirati pristup pomoću formalnog sustava odobrenja i revizije dodijeljenih prava za udaljeni pristup;
- potrebno je uvesti rigorozne kontrole nad konfiguracijama resursa informacijskog sustava koji omogućuju udaljeni pristup kako bi se banka zaštitila od moguće zloupotrebe udaljenog pristupa (primjer takve kontrole je automatski povratni poziv);
- primjenu evidentiranja i nadzora svih radnja provedenih korištenjem udaljenog pristupa (primjerice praćenjem sistemskih i operativnih zapisa); navedeno uključuje podatke kao što su datum, vrijeme, korisnik, lokacija korisnika, trajanje i svrha svih udaljenih pristupa;
- u svrhu zaštite komunikacija potrebno je primijeniti "jaku" autentifikaciju (primjerice kombinaciju dvaju načina utvrđivanja neospornosti korisničkog identiteta) i enkripciju (primjerice VPN).

5.2.10. Povlašteni pristup

Povlašteni pristup omogućuje zaobilaženje sistemskih i aplikativnih kontrola informacijskog sustava. Stoga je posebnu pozornost potrebno posvetiti kontroli osoba, procesa i sustava s pravom povlaštenog pristupa komponentama informacijskoga sustava banke (primjerice korisnika s administratorskim ovlastima na operativnim sustavima, aplikacijama, bazama podataka i mrežnim resursima). Dobre prakse kontrole povlaštenog pristupa uključuju:

- identificiranje svih osoba, procesa i sustava s povlaštenim pravima pristupa
- korištenje povlaštenim pristupom isključivo za radnje koje se ne mogu obaviti pomoću pristupa s manjim pravima
- uspostavu formalnog sustava dodjele prava povlaštenog pristupa
- periodično revidiranje postupka dodjeljivanja te dodijeljenih prava povlaštenog pristupa
- evidentiranje i revidiranje aktivnosti koje se provode putem povlaštenog pristupa (primjerice pregledom sistemskih i operativnih zapisa)
- rigoroznu zaštitu identifikacijskih i autentifikacijskih oznaka koje se rabe za povlašteni pristup na informacijskom sustavu
- definiranje postupaka koji će u izvanrednim situacijama ovlaštenim osobama omogućiti povlašteni pristup informacijskom sustavu (primjerice saznavanje identifikacijskih i autentifikacijskih oznaka korisnika s administratorskim ovlastima pohranjenih u sefu u čitljivom obliku)
- izbjegavanje dijeljenja istih identifikacijskih i autentifikacijskih oznaka s pravima povlaštenog pristupa između više korisnika.

5.3. Kriptografija

Banka bi trebala na osnovi obavljene procjene rizika odrediti adekvatne kriptografske metode čija će primjena smanjiti rizik od narušavanja temeljnih načela informacijskog sustava. Osnovne komponente svake kriptografske metode jesu kriptografski algoritam (opisuje kako se provodi transformacija) te jedan ili više kriptografskih ključeva (podatak pomoću kojeg se obavlja transformacija). Kriptografske metode omogućuju zaštitu podataka i kada oni više nisu pod kontrolom njihova vlasnika. Kriptografske metode rabe se kao vrsta logičkih kontrola, te se njima dodatno osigurava zaštita informacija i smanjuje rizik od narušavanja temeljnih načela informacijskog sustava. Kriptografija se najčešće upotrebljava:

- za enkripciju (enkripcija ili šifriranje je proces u kojem se podaci transformiraju u nečitljivu formu iz koje početne podatke mogu dobiti samo osobe koje posjeduju kriptografski ključ pomoću kojega se obavlja dekripcija; enkripcija osigurava povjerljivost podataka prilikom njihovog prijenosa ili pohrane)
- za elektroničko potpisivanje (elektronički potpis može se dodati bilo kojem podatku pohranjenom u elektroničkom obliku; njime se, pomoću kriptografskih mehanizama, omogućuje potvrđivanje temeljnih načela informacijskog sustava)
- za očuvanje integriteta podataka
- za utvrđivanje autentičnosti korisnika.

Posebnu pozornost potrebno je posvetiti upravljanju kriptografskim ključevima (uključujući, primjerice, postupke njihova generiranja, pohrane, razmjene, upotrebe, uklanjanja iz upotrebe i uništavanja). Izgubljeni ili oštećeni dekripcijski ključevi mogu onemogućiti ovlaštenim osobama pravodobni pristup podacima.

Kriptografske metode mogu se implementirati pomoću softverskih ili hardverskih resursa te njihovom kombinacijom. Dobre prakse nalažu primjenu provjerenih kriptografskih algoritama i implementacija koje su bile predmet detaljnog i opsežnog testiranja.

5.4. Fizička sigurnost

Fizička sigurnost obuhvaća kontrole koje se provode radi zaštite resursa informacijskog sustava od neovlaštenog fizičkog pristupa, krađe, fizičkog oštećenja ili uništenja. Temeljna načela informacijskog sustava mogu biti narušena između ostalog zbog neovlaštenog fizičkog pristupa i oštećenja ili uništenja imovine informacijskog sustava. Rizici povezani s fizičkom sigurnošću mogu se smanjiti uvođenjem sigurnosnih zona. Sigurnosne zone (u nastavku teksta: zone) fizički su prostori s različitim zahtjevima fizičke sigurnosti. Sigurnosni zahtjevi za svaku zonu proizlaze iz vrste i osjetljivosti resursa informacijskog sustava koji su smješteni u zoni, te se trebaju definirati u skladu s procjenom rizika, pri čemu valja uzeti u obzir različite vrste prijetnja (prirodne, uzrokovane ljudskim djelovanjem, slučajne ili namjerne) i ranjivosti te posljedice neželjenih događaja.

Banka bi trebala definirati zone i primijeniti odgovarajuće upravljačke, logičke i fizičke kontrole u svakoj od definiranih zona. Navedene se kontrole, između ostalog, primjenjuju radi zaštite prostorija s resursima informacijskog sustava, samih resursa, kao i sustava koji su podrška funkcioniranju informacijskog sustava (primjerice sustava napajanja električnom energijom, sustava za grijanje i klimatizaciju i slično).

Banka bi trebala uzeti u obzir sljedeće čimbenike koji mogu utjecati na fizičku sigurnost:

- **Kontrole fizičkog pristupa.** Kontrole fizičkog pristupa ograničavaju ulaske i napuštanje prostorija u kojima su smješteni resursi informacijskog sustava banke kao i unošenje te iznošenje opreme i medija. Primjeri su ovakvih prostorija računalni centri, prostorije s poslužiteljima, prostorije s telekomunikacijskom opremom i slično.
- **Zaštita od požara.** Požar ima potencijal da djelomično ili potpuno uništi resurse informacijskog sustava (uključujući i rizik za ljudske živote). Isto tako, dim, nagrizajući plinovi i vlaga, koji se oslobađaju za vrijeme požara, mogu načiniti štetu i na ostalim dijelovima sustava šireći se kroz građevinski objekt.
- **Sustavi za podršku.** Banka bi trebala osigurati ispravan rad sustava za podršku. Zastoji u radu sustava za podršku (primjerice sustava za održavanje stabilnog i neprekinutog napajanja električnom energijom, sustava za grijanje, sustava za klimatizaciju i slično) mogu izazivati prekide u radu informacijskog sustava i njegovo oštećenje. Dobre prakse nalažu provođenje kontrole svojstava zraka (primjerice temperature, vlažnosti, čistoće i koncentracije onečišćenosti zraka) u prostoru s resursima informacijskog sustava kako bi se udovoljilo zahtjevima osoblja i informacijskog sustava.
- **Konstrukcija objekta.** Potrebno je imati u vidu da građevinski objekt može biti podvrgnut većem opterećenju nego što je u stanju izdržati. Konstrukcija objekta može biti oštećena, oslabljena ili uništena zbog potresa, raznih dodatnih opterećenja, eksplozija ili požara. Posljedica uništenja građevinskog objekta može biti fizičko oštećenje ili uništenje (dijela) informacijskog sustava.
- **Zaštita od utjecaja vode.** Prodor vode može biti razoran za informacijski sustav. Potrebno je razmotriti posljedice koje prodor vode može izazvati i posjedovati točne informacije o mreži vodovodnih instalacija te instalacija rashladnih uređaja koje mogu ugroziti resurse informacijskog sustava. Banka bi trebala, u skladu s procjenom rizika, poduzeti adekvatne mjere za smanjenje rizika kao što su ugradnja "dvostrukog poda", premještanje resursa informacijskog sustava te vodovodnih instalacija i slično.

5.5. Upravljanje operativnim i sistemskim zapisima

Operativni i sistemski zapisi omogućuju uvid u aktivnosti resursa informacijskog sustava (primjerice operativnih sustava, vatrozida, usmjernika, sustava za otkrivanje neovlaštenog pristupa i radnja na informacijskom sustavu, aplikacijskih sustava, procesa, osoba). U kombinaciji s odgovarajućim internim aktima, procedurama i alatima, operativni i sistemski zapisi (u nastavku teksta: zapisi) omogućuju postizanje ciljeva povezanih sa sigurnošću i funkcionalnošću, uključujući rekonstrukciju događaja, osobnu odgovornost, otkrivanje neovlaštenog pristupa i radnja te identifikaciju problema. Zapisi se, između ostalog, upotrebljavaju za sljedeće:

- **Rekonstrukciju događaja.** Banka može upotrebljavati zapise za rekonstrukciju izvršenih radnja (primjerice kao pomoć u naknadnoj istrazi kojom se utvrđuje kako, kada i zašto su redovne operacije prekinute te tko je, kako i kada obavio određenu radnju).
- **Osobna odgovornost.** Zapisi služe za poticanje savjesnog korištenja resursa jer korisnici znaju da se njihove radnje mogu naknadno analizirati i jedinstveno pratiti do izvora.
- **Otkrivanje neovlaštenog pristupa i radnja na sustavu.** Zapisi se mogu rabiti kao pomoć u otkrivanju neovlaštenog pristupa i radnja na sustavu ukoliko je sustav za otkrivanje takvih aktivnosti pravilno konfiguriran, odnosno ako bilježi odgovarajuće informacije. Navedene aktivnosti mogu biti otkrivene u realnom vremenu analizom zapisa u trenutku kreiranja ili naknadno.
- **Identifikacija problema.** Zapisi mogu također pomoći u identificiranju ostalih sigurnosnih i funkcionalnih problema na informacijskom sustavu u realnom vremenu.

Zapisi trebaju sadržavati dovoljnu količinu informacija za utvrđivanje pojave događaja i njihova uzroka. Obuhvat i sadržaj zapisa potrebno je pomno definirati, u skladu s procjenom rizika, kako bi se uravnotežila potreba između sigurnosti s jedne strane, te učinkovitosti i troškova s druge strane. Posebnu pozornost treba posvetiti očuvanju integriteta zapisa, da bi se osigurala dokazivost i neporecivost događaja. Isto tako, potrebno je osigurati i povjerljivost zapisa u skladu s klasifikacijom informacija. Općenito, zapis o događaju treba pružiti informaciju:

- o vrsti događaja
- o vremenu kada se događaj dogodio
- o identifikaciji osoba, sustava ili procesa povezanih s događajem
- o programu ili naredbi koja je upotrijebljena za pokretanje događaja.

5.5.1. Sigurnost operativnih i sistemskih zapisa

U svrhu zaštite integriteta, dokazivosti i neporecivosti informacijskog sustava operativni i sistemski zapisi moraju biti adekvatno zaštićeni od neautoriziranog pristupa, izmjena i brisanja, pri čemu treba imati u vidu barem sljedeće:

- povjerljivost i integritet zapisa moraju biti adekvatno zaštićeni;
- potrebno je razdvojiti dužnosti osoba koje administriraju kontrole pristupa i osoba zaduženih za sigurnost od osoba koje administriraju zapise;

- pristup zapisima putem javno dostupnih telekomunikacijskih mreža treba biti strogo kontroliran.

5.5.2. Praćenje operativnih i sistemskih zapisa

Osobe odgovorne za praćenje zapisa trebaju redovito pratiti zapise u skladu sa svojim organizacijskim zaduženjima i ovlastima. Prilikom praćenja zapisa potrebno je obratiti pozornost na sljedeće:

- **Prepoznati uobičajene aktivnosti.** Osobe odgovorne za praćenje zapisa trebaju znati koje su aktivnosti uobičajene kako bi mogle uspješno uočiti neuobičajene aktivnosti.
- **Omogućiti djelotvorno pretraživanje zapisa.** Praćenje zapisa može se olakšati pregledom po parametrima kao što su: korisnička, terminalska i aplikativna identifikacija, datum i vrijeme ili bilo koji drugi grupni parametar.
- **Saznanja o postojećim problemima i ograničenjima.** Administratori na razini sustava ili aplikacija trebali bi pregledavati zapise uzimajući u obzir poznate probleme sustava ili aplikacija, poznata kršenja postojećih zahtjeva od strane korisnika i slično.
- **Razviti smjernice za praćenje zapisa.** Osobe odgovorne za aplikacije, informacije, obradu podataka i sigurnost te administratori informacijskog sustava trebaju na temelju procjene rizika odrediti opseg i učestalost pregleda zapisa.
- **Automatizirani alati.** Banka bi trebala razmotriti primjenu alata koji pomažu u izdvajanju korisnih informacija iz velike količine podataka koje sadrže zapisi (primjerice u prepoznavanju neovlaštenih i neuobičajenih radnja pomoću poznatih uzoraka).

5.6. Zaštita od malicioznog koda

Maliciozni kod je bilo koji oblik programskog koda koji djeluje neočekivano i na potencijalno štetan način. Uobičajene su vrste malicioznog koda virusi, crvi i "trojanski konji", a njihovo djelovanje može imati samostalan učinak ili kombinirani, čime se postiže veća šteta. Maliciozni kod može imati mogućnost repliciranja i širenja na druge resurse informacijskog sustava. Nadalje, maliciozni kod može ugroziti povjerljivost, integritet i raspoloživost resursa informacijskog sustava mijenjajući i brišući podatke, šaljući podatke izvan informacijskog sustava, uklanjajući dokaze koji se mogu iskoristiti za potrebe forenzike ili stvarajući skrivene ranjivosti koje mogu olakšati neovlašteni pristup i radnje na informacijskom sustavu.

Zaštitne mjere i kontrole

Zaštitne mjere i kontrole koje se primjenjuju radi smanjenja rizika od narušavanja ili gubitka temeljnih načela informacijskog sustava zbog utjecaja malicioznog koda, podrazumijevaju slojevito oblikovanje sigurnosne infrastrukture što, između ostalog, uključuje primjenu adekvatne tehnologije, internih akata i edukaciju zaposlenika.

Kontrole koje bi banka trebala primijeniti kako bi smanjila prije navedene rizike, između ostalog, uključuju proizvode i sustave za otkrivanje i uništavanje malicioznog koda kao i ostale sustave za ograničavanje i otkrivanje neuobičajenih ili neovlaštenih radnja te za nadziranje i upravljanje radnjama koje su dopuštene (primjerice vatrozid, IDS).

Budući da se svakodnevno pojavljuju novi primjeri malicioznog koda i neovlaštenih pristupa i radnja, banka bi trebala što češće, a najmanje jednom dnevno, provjeriti ažurnost svojih sustava zaštite od malicioznog koda te neuobičajenih i neovlaštenih radnja. Banka bi u sklopu procjene rizika trebala također uzeti u obzir činjenicu da sustavi za otkrivanje malicioznog koda koji se temelje na prepoznavanju uzorka mogu bitno teže (potrebna je dekripcija) otkriti maliciozni kod u enkriptiranim podacima (primjerice VPN i slično).

Nadalje, banka bi, zbog potencijalno sve složenijih neovlaštenih radnja i zbog toga što se autori malicioznog koda često koriste metodama socijalnog inženjeringa, trebala implementirati ostale kontrole koje, između ostalog, uključuju interne akte o upotrebi resursa informacijskog sustava i edukaciju korisnika informacijskog sustava o mogućim prijetnjama. Banka bi trebala uzeti u obzir sljedeće čimbenike koji mogu utjecati na sigurnost:

- potrebu za redovitim pregledom resursa informacijskog sustava s obzirom na neautorizirani odnosno nedopušteni softver
- sprječavanje neovlaštene instalacije softvera
- edukaciju zaposlenika kako bi ih se upozorilo na opasnosti čitanja poruka nepoznatog podrijetla, pokretanja izvršnih datoteka, socijalni inženjering i slično
- rukovanje medijima za pohranu i prijenos podataka
- načine pristupa javno dostupnim telekomunikacijskim mrežama
- dopuštene aktivnosti tijekom pristupa javno dostupnim telekomunikacijskim mrežama kao i tijekom upotrebe tehnologije za komunikaciju (primjerice elektroničke pošte i slično)
- uklanjanje ranjivosti sustava povezanih s poznatim malicioznim kodovima

- adekvatno upravljanje operativnim i sistemskim zapisima koji se odnose na maliciozni kod.

6. Održavanje informacijskog sustava

6.1. Upravljanje imovinom informacijskog sustava

Upravljanje imovinom informacijskog sustava proces je koji obuhvaća detektiranje, evidentiranje, raspolaganje, praćenje, planiranje, obnavljanje, zaštitu i odlaganje imovine.
Pod imovinom informacijskog sustava (u nastavku teksta: imovina) podrazumijevaju se sve vrste računalnog softvera, hardvera, pripadajućih komponenata te informacija koje se upotrebljavaju za obavljanje poslovnih procesa u banci. Imovina, između ostalog, uključuje sljedeće:

- **informacijsku imovinu:** podatke u bazama podataka i datoteke s podacima, programski kod, sistemsku i aplikacijsku dokumentaciju, korisničke priručnike, materijal za obuku, planove, politike, strategije, standarde i procedure banke, arhivirane informacije i slično
- **softversku imovinu:** aplikacijski softver, sistemski softver, razvojne alate i uslužne programe i slično
- **hardversku imovinu:** računalnu opremu (osobna računala, poslužitelje, monitore, modeme i slično), komunikacijsku opremu (usmjernike, vatrozide, telefonske centrale, telefakse, telefonske sekretarice i slično), medije za pohranu podataka (trake, magnetne diskove, optičke medije i slično) i ostalu tehničku opremu (uređaje za neprekidno napajanje strujom, klimatizacijske uređaje i slično).

Nepostojanje primjerenog procesa praćenja imovine može imati negativan utjecaj na raspodjelu resursa, distribuciju softvera i hardvera i njihovo održavanje, sigurnost informacijskog sustava, na popravke imovine i slično. Isto tako, neprimjereno upravljanje imovinom može otežati ili onemogućiti identifikaciju imovine te osoba odgovornih za imovinu i ostalih korisnika, lociranje imovine u svrhu zamjene i ažuriranja te djelotvorno obavljanje revizije. Nadalje, neadekvatno upravljanje imovinom povećava pravni rizik, primjerice rizik od povrede ugovora o upotrebi licenciranog softvera.

Dobre prakse nalažu da je u sklopu upravljanja imovinom informacijskog sustava potrebno:

- planirati investicije, operativne aktivnosti i pružanje podrške vezane uz imovinu
- alocirati imovinu tako da se osigura djelotvorno pružanje usluga
- uspostaviti sustav izvještavanja o planiranim investicijama i koristima koje takve investicije donose banci
- imenovati osobe odgovorne za imovinu
- dodijeliti pripadajuće odgovornosti za upravljanje i zaštitu imovine.

Banka bi trebala uspostaviti proces upravljanja imovinom informacijskog sustava i donijeti pripadajuće interne akte koji će omogućiti adekvatno upravljanje imovinom tijekom njezina životnog ciklusa. Životni je ciklus imovine razdoblje u kojem se imovina upotrebljava za obavljanje poslovnih procesa te se, primjerice, sastoji od faze nabave, implementacije, korištenja, podrške te povlačenja imovine iz upotrebe.

Isto tako, banka bi u sklopu procesa upravljanja imovinom trebala definirati barem sljedeće:

- postupke upravljanja životnim ciklusom imovine
- prava i obveze korisnika pri rukovanju imovinom
- postupke označavanja postojeće i novonabavljene imovine

- način evidentiranja postojanja i lokacije fizičkih komponenata imovine
- način evidentiranja ugovora o licenciranju, distribucije softvera, odnosno procesa instalacije softverske podrške te nadogradnje
- postupke za izdavanje imovine zaposlenicima, nadzor nad njom i ažuriranje evidencija na godišnjoj osnovi
- postupke premještanja, zamjene, skladištenja, uništavanja i trajnog povlačenja imovine (imajući u vidu, primjerice, brisanje podataka s medija prilikom zamjene, skladištenja imovine, trajnog napuštanja imovine banke i slično).

6.2. Upravljanje promjenama

Brzi napredak informacijske tehnologije, kao i česte izmjene poslovnih zahtjeva uzrokuju potrebu za promjenom softverskih i hardverskih komponenata informacijskog sustava banke. Navedene promjene mogu rezultirati neočekivanim ponašanjem informacijskog sustava (primjerice, nekompatibilnošću i nestabilnošću dijelova sustava, programskim pogreškama – engl. *bug* i slično) i negativno utjecati na njegovu sigurnost. Stoga postupke izmjene informacijskih sustava treba formalno propisati, te se ponašati oprezno i u skladu s dobrim praksama, kako bi se negativni utjecaji sveli na najmanju moguću mjeru. Osnovni je zadatak upravljanja promjenama osigurati da promjene komponenata informacijskog sustava ne naruše (namjerno ili nenamjerno) sigurnost i funkcionalnost informacijskog sustava.

Proces upravljanja promjenama obuhvaća postupak identifikacije početnih inačica softverskih i hardverskih komponenata informacijskog sustava te praćenje svih njihovih promjena. Upravljanje promjenama uključuje i upravljanje novim verzijama softvera i hardverskim komponentama, kao i upravljanje programskim ispravkama ("zakrpa", engl. *patch*). Potrebno je sustavno pratiti objavljivanje programskih ispravaka i izmjena, kao i novih verzija aplikativnih programa i operativnih sustava te ih, ovisno o procjeni prednosti i nedostataka implementirati na informacijskom sustavu. Posebnu pozornost treba posvetiti programskim ispravkama i novim verzijama dijelova informacijskog sustava koji ispravljaju sigurnosne propuste, te ih je na osnovi procjene rizika, a nakon testiranja, potrebno što prije integrirati u informacijski sustav.

Razina detaljnosti i formalnost procesa upravljanja promjenama trebale bi ovisiti o osjetljivosti dijela informacijskog sustava koji se mijenja, odnosno trebale bi biti u skladu s opsegom i karakteristikama samih promjena.

Također je potrebno analizirati potencijalne promjene informacijskog sustava te na temelju definiranih razloga i očekivanja od provođenja promjene odrediti i odobriti daljnje postupke i njihov opseg. Ovisno o rezultatima analize, a u skladu s opsegom i karakteristikama promjene, analiza uvođenja promjene ne mora nužno uključivati i provedbu procjene rizika.

Proces promjene informacijskih sustava trebao bi biti propisan, standardiziran i sadržavati barem sljedeće:

- definiranje zahtjeva kojim se traži promjena
- analizu opravdanosti zahtjeva s izvedenim zaključcima kao i procjenu utjecaja na poslovne procese, pojedine dijelove i komponente informacijskog sustava te sigurnost sustava (primjerice planiranje kontinuiteta poslovanja, politiku sigurnosti informacijskog sustava, funkcionalnost i sigurnost aplikacija i baza podataka)
- planiranje testiranja i definiranje rezultata koji se trebaju ostvariti kako bi se promijenjeni sustav postavio u produkcijsku okolinu; testiranje se mora obaviti u obuhvatu koji ovisi o opsegu i karakteristikama promjene sustava i u kontroliranim uvjetima te u okolini koja je u najvećoj mogućoj mjeri slična produkcijskoj; prilikom testiranja treba voditi računa o povjerljivosti informacija
- kreiranje nove odnosno nadopunu već postojeće dokumentacije
- provedbu potrebne edukacije zaposlenika
- planiranje i uvođenje promjena informacijskog sustava u produkcijsku okolinu; posebnu pozornost potrebno je posvetiti sigurnosti informacijskog sustava odnosno

mogućnosti narušavanja temeljnih načela informacijskog sustava prije, tijekom ili nakon provođenja promjene
- dokumentiranje provedenih promjena
- definiranje osoba ovlaštenih i odgovornih za provođenje svih navedenih postupaka
- arhiviranje dokumentacije nastale u procesu promjene informacijskih sustava.

Banka bi trebala posebnu pozornost posvetiti rizicima koji proizlaze iz neadekvatnog upravljanja promjenama, zato što:
- izostanak pravodobne promjene informacijskog sustava banke može ostaviti neispravljenima uočene sigurnosne propuste
- izostanak analize ili provedba neadekvatne analize može dovesti do uvođenja nepotrebne ili čak štetne promjene informacijskog sustava
- izostanak testiranja promjena informacijskog sustava može dovesti do nekompatibilnosti dijela informacijskog sustava, nestabilnosti sustava ili povećane izloženosti banke vanjskim i unutarnjim prijetnjama;
- promjena informacijskog sustava bez pravodobnog ažuriranja dokumentacije može dovesti do neusklađenosti između stvarnog i dokumentiranog stanja sustava
- promjena informacijskog sustava bez pravodobne edukacije korisnika može dovesti do njihove neadekvatne osposobljenosti za rad na informacijskom sustavu
- suviše formalan i detaljan proces upravljanja promjenama informacijskog sustava može dovesti do nepravodobnog provođenja ili neprovođenja potrebnih promjena, što može rezultirati nestabilnošću sustava ili povećanom izloženošću banke vanjskim i unutarnjim prijetnjama
- neadekvatno praćenje objave novih programskih ispravaka i izmjena, te novih verzija dijelova informacijskog sustava može ugroziti sigurnost i smanjiti funkcionalnost informacijskog sustava.

6.3. Upravljanje konfiguracijama

Većinu hardverskih i softverskih komponenata informacijskog sustava moguće je pomoću niza postavka prilagoditi specifičnim potrebama banke. Navedene postavke moraju biti na zadovoljavajući način konfigurirane, kako bi se funkcionalnost i sigurnost sustava dovele i održale na potrebnoj razini. Postupak upravljanja postavkama sustava nazivamo upravljanjem konfiguracijama sustava. Upravljanje konfiguracijama je proces analize, definiranja, dokumentiranja, testiranja, uvođenja u produkcijski rad, kontrole i praćenja izmjena u postavkama komponenata informacijskog sustava. Upravljanje konfiguracijama treba obuhvatiti sve osjetljive postavke informacijskog sustava. Osjetljivim postavkama smatraju se sve postavke čija izmjena može znatno utjecati na sigurnost ili funkcionalnost informacijskog sustava. Kriteriji, načini i postupci upravljanja konfiguracijama trebaju biti definirani i propisani.

Procjenu rizika potrebno je provesti za nove komponente sustava, kao i prilikom promjena sustava koje imaju utjecaj na funkcionalnost postojećih postavka ili omogućuju nove postavke komponenata informacijskog sustava. Banka bi trebala na temelju obavljene procjene rizika za hardverske i softverske komponente informacijskog sustava analizirati, odrediti, testirati i dokumentirati sigurnosne i funkcionalne postavke komponenata sustava koje moraju biti primijenjene kako bi se osiguralo održavanje temeljnih načela informacijskog sustava.

Izmjene propisanih postavka komponenata informacijskog sustava potrebno je dokumentirati na način koji omogućuje praćenje izmjena tijekom vremena. Sustav upravljanja konfiguracijama mora omogućiti identifikaciju svih osjetljivih postavka informacijskog sustava (koje su značajne za djelotvorno i sigurno funkcioniranje sustava) u određenom trenutku. Isto tako, potrebno je definirati odgovornosti za upravljanje konfiguracijama informacijskog sustava s posebnim naglaskom na zaposlenike koji su ovlašteni mijenjati osjetljive postavke sustava. Pristup postavkama koje mogu utjecati na sigurnost i mogućnost njihove izmjene moraju biti nadzirani i kontrolirani.

Banka bi trebala posebnu pozornost posvetiti rizicima koji proizlaze iz neadekvatnog upravljanja konfiguracijama, zato što:

- nezadovoljavajuće postavljena početna konfiguracija hardverskih i softverskih komponenata može dovesti do nekompatibilnosti dijela informacijskog sustava, do nestabilnosti sustava, te do povećane izloženosti banke vanjskim i unutarnjim prijetnjama;
- izmjene dijelova informacijskog sustava bez adekvatnog praćenja postavka ili nekontrolirane promjene postavki mogu narušiti sigurnost i funkcionalnost sustava;
- suviše restriktivan proces upravljanja konfiguracijama može obeshrabriti, spriječiti ili usporiti provođenje potrebnih izmjena dijelova informacijskih sustava.

6.4. Dokumentacija

Banka bi trebala definirati standarde izrade, pohrane, održavanja i čuvanja dokumentacije koja se odnosi na informacijski sustav banke (u nastavku teksta: dokumentacija). Dokumentacija je korisna samo ako je točna, potpuna i ažurna, te je takvom treba i održavati. Stoga je potrebno definirati osobe odgovorne za dokumentaciju i njihove dužnosti u održavanju točnosti, potpunosti i ažurnosti dokumentacije.

Banka bi trebala zaposlenicima osigurati pristup dokumentaciji koja je povezana s njihovim poslovnim potrebama. Pristup povjerljivoj dokumentaciji mora biti ograničen, kako bi svaki zaposlenik mogao pristupiti samo dokumentima za koje je ovlašten. Važnu dokumentaciju (u skladu s klasifikacijom informacija) trebalo bi pohraniti i na sigurnu udaljenu lokaciju te je periodično ažurirati.

Dobre prakse nalažu organiziranje i vođenje dokumentacije na takav način da se za dokument mogu utvrditi odgovorne osobe, vrijeme nastanka, početak primjene, klasifikacija te inačica. Potrebno je uspostaviti i evidenciju koja će omogućiti sveobuhvatni pregled postojeće dokumentacije.

Primjeri dokumentacije:

- interni akti vezani uz informacijski sustav (odluke, politike, procedure, upute, standardi i slično)
- opisi hardvera i softvera
- programska dokumentacija (programski kod, dijagrami i opisi načina funkcioniranja programa i slično)
- dijagrami i opisi poslovnih procesa
- korisnička dokumentacija
- ugovori s dobavljačima i pružateljima usluga
- izvješća, planovi, zapisnici, dopisi i ostala korespondencija.

6.5. Izobrazba

Izobrazba, odnosno edukacija, kontinuirani je proces koji se mora neprekidno odvijati kako bi se osiguralo da znanja korisnika sustava prate promjene i u informacijskom sustavu i u njegovoj okolini. Spomenute promjene uključuju izmjene postojećih funkcionalnosti i sigurnosnih obilježja informacijskog sustava ili dodavanje novih kao i sve promjene izvan informacijskog sustava banke koje na njega mogu utjecati.

Većina štetnih (neplaniranih i neželjenih) događaja na informacijskim sustavima nastaje kao posljedica ljudskog djelovanja. Od navedenih štetnih događaja zaposlenici poslovnog subjekta uzrokuju kudikamo veći broj nego ostale osobe. Neplanirani i neželjeni događaji najčešće nastaju kao posljedica nenamjernih radnja (pogrešaka ili propusta) ili, rjeđe, kao posljedica namjernih radnja počinjenih s ciljem nanošenja štete informacijskom sustavu banke. Kako bi se navedeni događaji i njihovo štetno djelovanje sveli na prihvatljivu razinu, potrebno je primjereno educirati sve korisnike informacijskog sustava banke.

Posljedica primjerene izobrazbe bit će smanjivanje broja pogrešaka i propusta i ograničavanje njihova dosega te uočavanje i sprječavanje pokušaja narušavanja temeljnih načela informacijskog sustava.

Edukacija bi trebala obuhvatiti sve osobe koje se koriste informacijskim sustavom banke:

- informatičko osoblje banke
- osobe zadužene za sigurnost informacijskog sustava i unutarnju reviziju
- ostale zaposlenike banke koji se koriste informacijskim sustavom, i na operativnim i na upravljačkim razinama
- osobe koje nisu zaposlenici banke, ali se koriste informacijskim sustavom banke (primjerice korisnici e-bankarstva, zaposlenici tvrtki vanjskih suradnika i slično).

Izobrazba korisnika informacijskog sustava trebala bi omogućiti navedenim osobama djelotvorno obavljanje poslovnih zadataka uz istodobno svođenje neželjenih događaja na prihvatljivu razinu. Preciznije, ciljevi edukacije korisnika informacijskog sustava banke jesu:

- razviti i održavati znanja i vještine korisnika na primjerenoj razini, kako bi oni mogli obavljati poslovne zadatke na djelotvoran i siguran način
- upoznati korisnike s internim aktima (primjerice politikama, procedurama i ostalim postupcima kojih se navedeni korisnici moraju pridržavati) kako bi se točno ustanovili zadaci, okviri djelovanja i osobna odgovornost svakog korisnika
- uspostaviti i unapređivati svijest o potrebi zaštite resursa informacijskog sustava
- razviti i održavati znanja potrebna da bi se funkcionalnost i sigurnost informacijskog sustava zadržale na zadovoljavajućoj razini tijekom cijeloga životnog ciklusa informacijskog sustava.

Izobrazba bi trebala biti sastavni dio strategije informacijskog sustava banke te u skladu s planiranim promjenama informacijskog sustava . Izobrazbu je potrebno unaprijed planirati te formalno identificirati i specificirati potrebne aktivnosti, način njihova provođenja te vremenske i financijske okvire unutar kojih će se provoditi. Prilikom planiranja izobrazbe posebnu pozornost valja posvetiti potrebi usvajanja i održavanja visoko specijaliziranih tehničkih znanja čije stjecanje zahtijeva korištenje značajnim financijskim i vremenskim resursima te veliki osobni angažman zaposlenika. Navedena visoko specijalizirana znanja

obično se stječu kontinuiranom izobrazbom i stručnim usavršavanjem stoga ih je potrebno adekvatno planirati i provoditi. Pri tome bi banka trebala posebnu pozornost posvetiti izobrazbi unutarnje revizije, kako bi se revizija informacijskog sustava provodila na zadovoljavajući i djelotvoran način.

Ostvarivanje plana izobrazbe i njegovu provedbu potrebno je dokumentirati i pratiti. Pravilno planirana i provedena izobrazba povećat će produktivnost, iskorištenje postojećih resursa te omogućiti podizanje razine sigurnosti cjelokupnoga informacijskog sustava banke.

Izobrazbu je moguće provoditi na različite načine, od najjednostavnijih poput distribucije pisane dokumentacije do kompleksnih i dugotrajnih usavršavanja. Opseg, detaljnost, trajanje i način provođenja edukacije trebaju biti u skladu s obilježjima ciljane grupe odnosno ciljanih korisnika te s opsežnosti i kompleksnosti tematike. Prilikom određivanja obilježja ciljanih korisnika potrebno je uzeti u obzir poslovne funkcije koje navedeni korisnici obavljaju, njihovo predznanje o predmetu edukacije te općenito poznavanje funkcioniranja informacijskih sustava. Korisnike je potrebno educirati do razine detaljnosti koju zahtijevaju njihovi poslovni zadaci.

7. Planiranje kontinuiteta poslovanja

Planiranje kontinuiteta poslovanja treba u najvećoj mogućoj mjeri osigurati kontinuitet poslovanja te omogućiti banci da pomoću adekvatnih mjera za oporavak u što kraćem vremenu smanji ukupni učinak havarije ili drugih neželjenih i nepredviđenih događaja (čije posljedice mogu prouzročiti prekid poslovnih procesa te u konačnici i poslovanja banke) na prihvatljivu razinu. Osiguravanje kontinuiteta poslovanja postiže se poduzimanjem mjera prevencije neželjenih događaja, ograničavanja njihova učinka i oporavka u slučaju prekida poslovnih procesa. Planiranje kontinuiteta poslovanja treba se temeljiti na analizi utjecaja na poslovanje i na procjeni rizika te omogućiti dosljedno odvijanje poslovnih procesa banke i nastavak pružanja usluga uz značajno smanjenje rizika kojima je banka u svom poslovanju izložena (primjerice reputacijskog, financijskog, operativnog, strateškog i pravnog rizika). Zbog velike ovisnosti banke o informacijskoj tehnologiji te informacijskom sustavu koji omogućuje odvijanje poslovnih procesa, banka bi trebala pri planiranju kontinuiteta poslovanja posebnu pozornost posvetiti osiguranju raspoloživosti resursa informacijskog sustava potrebnih za odvijanje kritičnih i/ili vitalnih poslovnih procesa.

Djelotvornost planiranja kontinuiteta poslovanja ocjenjuje se pomoću testiranja i primjene plana kontinuiteta poslovanja, plana oporavka, plana odgovora na incidente kao i uspostavom adekvatnog procesa upravljanja pričuvnom pohranom.

Banka bi prilikom planiranja kontinuiteta poslovanja trebala obratiti posebnu pozornost:

- na identificiranje kritičnih i/ili vitalnih poslovnih procesa
- na procjenu prihvatljivog vremena neraspoloživosti pojedinih poslovnih procesa
- na identificiranje resursa koji su potrebni za održavanje kritičnih i/ili vitalnih poslovnih procesa
- na procjenjivanje pojave i učinka potencijalnih incidenata, havarija te ostalih neželjenih i nepredviđenih događaja na poslovne procese banke i njezine klijente
- na dodjelu odgovornosti u svezi s izradom, aktiviranjem i provedbom planova
- na revidiranje planova s obzirom na promjene (primjerice osoblja, vanjskog i unutarnjeg okruženja i slično)
- na donošenje ostalih internih akata u svezi s planiranjem kontinuiteta poslovanja
- na testiranje plana kontinuiteta poslovanja, plana oporavka i plana odgovora na incidente te pričuvne pohrane i pričuvnoga računalnog centra
- na procjenu rizika ugovornih odnosa s ključnim pružateljima usluga i dobavljačima;
- na raspoloživost pričuvnoga računalnog centra na udaljenoj lokaciji
- na uspostavu standarda i procedura za komunikaciju sa svim osobama potrebnim za osiguranje kontinuiteta poslovanja
- komunikaciji osoba zaduženih za osiguravanje kontinuiteta poslovanja (primjerice tima za odgovore na incidente) i osoba zaduženih za odnose s javnošću.

Dobre prakse nalažu uspostavu odbora za planiranje kontinuiteta poslovanja koji bi, između ostalog, trebao imati savjetodavnu ulogu prilikom donošenja strateških odluka te nadzirati i koordinirati aktivnosti u svezi s planiranjem kontinuiteta poslovanja. Članovi odbora za planiranje kontinuiteta poslovanja trebali bi biti predstavnici poslovnih organizacijskih jedinica, voditelj sigurnosti informacijskog sustava, unutarnja revizija, predstavnici organizacijske jedinice za informacijsku tehnologiju te član uprave banke.

Neadekvatno planiranje kontinuiteta poslovanja može prouzročiti:

- gubitak raspoloživosti
- gubitak reputacije
- gubitak konkurentskih prednosti
- gubitak podataka
- gubitak produktivnosti
- povećanje operativnih troškova
- povredu ugovornih odnosa
- povredu važećih propisa
- financijski gubitak.

7.1. Analiza utjecaja na poslovanje

Analiza utjecaja na poslovanje (engl. *Business Impact Analysis*) jest proces analiziranja poslovnih procesa i resursa informacijskog sustava potrebnih za odvijanje poslovnih procesa koji obuhvaća barem sljedeće:

1. identifikaciju poslovnih procesa i klasifikaciju s obzirom na njihovu kritičnost i/ili vitalnost
2. identifikaciju resursa informacijskog sustava potrebnih za odvijanje poslovnih procesa, njihovih međuovisnosti te povezanosti s drugim informacijskim sustavima
3. procjenu rizika vezanih uz pojedine poslovne procese
4. određivanje prihvatljive razine pojedinih rizika
5. određivanje prihvatljivog vremena neraspoloživosti pojedinih poslovnih procesa, tj. vremena u kojem je potrebno obnoviti poslovni proces (engl. *Recovery Time Objective – RTO*)
6. određivanje vremena (u odnosu na vrijeme početka havarije ili drugog neželjenog i nepredviđenog događaja) od kojeg će banka biti u stanju obnoviti podatke (engl. *Recovery Point Objective – RPO*)
7. utvrđivanje prioriteta oporavka poslovnih procesa.

Analiza utjecaja na poslovanje temelj je za planiranje kontinuiteta poslovanja i djelotvornog oporavka poslovnih procesa odnosno resursa informacijskog sustava potrebnih za odvijanje poslovnih procesa. Vrijeme i ostali resursi potrebni za provođenje analize utjecaja na poslovanje ovisit će prije svega o veličini banke i kompleksnosti poslovnih procesa i informacijskog sustava.

Analiza utjecaja na poslovanje treba obuhvatiti sve poslovne procese te:

- identificirati potencijalni učinak neželjenog, nepredviđenog (i neuobičajenog) događaja na poslovne procese odnosno resurse informacijskog sustava potrebne za odvijanje tih procesa
- razmotriti utjecaj zahtjeva važećih propisa te potreba za izvješćivanjem Hrvatske narodne banke i ostalih nadležnih institucija na poslovne procese
- procijeniti najduže vrijeme neraspoloživosti pojedinih vitalnih poslovnih procesa, ciljeve i prioritete oporavka te troškove vezane uz zastoje i oporavak
- procijeniti i postaviti prioritete na kritične i/ili vitalne poslovne procese
- razmotriti utjecaj prekida poslovnih procesa na klijente (primjerice obveze banke prema klijentima, očekivanja klijenata) i reputaciju banke.

Učinak neželjenog i nepredviđenog događaja može se promatrati kao gubitak ili narušavanje temeljnih načela informacijskog sustava. Učinak neželjenih i nepredviđenih događaja može se mjeriti:

- kvantitativno (primjerice na osnovi izgubljenih prihoda ili na osnovi troškova ponovne uspostave poslovnih procesa)
- kvalitativno (primjerice događaji s velikim, srednjim ili malim utjecajem na poslovne procese odnosno na resurse informacijskog sustava).

Informacije potrebne u analizi utjecaja na poslovanje mogu se prikupiti na različite načine (primjerice uvidom u dokumentaciju i intervjuiranjem). Proces prikupljanja informacija trebao bi biti ujednačen (primjerice potrebno je provoditi intervjuiranje pomoću upitnika koji će se moći primjenjivati na sve poslovne procese i organizacijske jedinice banke). Na taj će se

način omogućiti postojanost i usporedivost dobivenih informacija čijom analizom bi se trebala odrediti kritičnost i/ili vitalnost poslovnih procesa banke. Prilikom provođenja analize utjecaja na poslovanje posebnu pozornost potrebno je posvetiti:

- identificiranju svih resursa informacijskog sustava koji su potrebni za odvijanje kritičnih i/ili vitalnih poslovnih procesa
- identificiranju osoba odgovornih za odvijanje kritičnih i/ili vitalnih poslovnih procesa
- utjecaju analiziranih poslovnih procesa na cjelokupno poslovanje banke
- određivanju prihvatljivog vremena neraspoloživosti poslovnih procesa i resursa informacijskog sustava potrebnih za odvijanje poslovnih procesa, odnosno vremena unutar kojeg je potrebno obnoviti poslovne procese (engl. *Recovery Time Objective - RTO*)
- određivanju vremena od kojeg će banka biti u stanju obnoviti podatke (engl. *Recovery Point Objective - RPO*)
- međuovisnosti prethodno navedenog
- resursima potrebnim za oporavak.

Analizu utjecaja na poslovanje potrebno je usklađivati s promjenama poslovnih procesa banke, njezina okruženja, informacijskog sustava i drugih okolnosti koje mogu utjecati na poslovanje banke. Budući da je analiza utjecaja na poslovanje temelj za planiranje kontinuiteta poslovanja, nedostatak ili neadekvatno provođenje analize može rezultirati neadekvatnim planiranjem kontinuiteta poslovanja. Navedeno se očituje u nemogućnosti banke da prepozna kritične i/ili vitalne poslovne procese, odredi prihvatljivo vrijeme neraspoloživosti poslovnih procesa kao i moguće troškove. Sve navedeno može dovesti do nemogućnosti uspostave kritičnih i/ili vitalnih poslovnih procesa, gubitka operativne učinkovitosti, neraspoloživosti informacijskog sustava, znatnoga financijskoga gubitka te gubitka reputacije banke.

7.2. Plan kontinuiteta poslovanja

U okviru planiranja kontinuiteta poslovanja banka bi trebala donijeti plan kontinuiteta poslovanja. Planom kontinuiteta poslovanja trebalo bi detaljno opisati postupke koje je potrebno slijediti kako bi se oporavili kritični i/ili vitalni poslovni procesi. Prilikom izrade plana kontinuiteta poslovanja banka bi trebala uzeti u obzir sve vrste događaja koji mogu negativno utjecati na poslovne procese i resurse informacijskog sustava potrebne za odvijanje poslovnih procesa.

Svrha plana kontinuiteta poslovanja jest:

- osigurati ponovnu uspostavu kritičnih i/ili vitalnih poslovnih procesa u zahtijevanom vremenu
- ograničiti i smanjiti gubitke koji mogu nastati kao posljedica prekida poslovnih procesa.

Plan kontinuiteta poslovanja trebao bi:

- biti u pisanom obliku
- temeljiti se na analizi utjecaja na poslovanje i procjeni rizika
- precizno definirati uvjete pod kojima se aktivira te odgovornosti za njegovu aktivaciju i provedbu
- biti specifičan s obzirom na uvjete u kojima se plan treba izvršiti
- biti specifičan s obzirom na hitne postupke u slučaju prekida poslovnih procesa
- uzeti u obzir resurse potrebne za obnavljanje poslovnih procesa
- biti dovoljno prilagodljiv kako bi se mogao primijeniti u nepredviđenim situacijama
- biti usredotočen na održavanje kontinuiteta poslovnih procesa, a ne na istraživanje uzroka incidenta
- biti djelotvoran u smanjivanju štetnog učinka na poslovne procese i financijskog gubitka.

Plan kontinuiteta poslovanja potrebno je usklađivati s promjenama poslovnih procesa banke, njezina okruženja, informacijskog sustava i drugih okolnosti koje mogu utjecati na poslovanje banke. Nadalje, plan kontinuiteta poslovanja potrebno je periodično testirati kako bi bio efikasan i usklađen s navedenim promjenama.

7.3. Plan oporavka

Zastoji i različiti poremećaji u radu informacijskog sustava mogu značajno ugroziti poslovanje banke zbog nemogućnosti odvijanja kritičnih i/ili vitalnih poslovnih procesa. Prilikom planiranja oporavka informacijskog sustava banka bi trebala uzeti u obzir moguće negativne učinke na resurse informacijskog sustava u slučaju različitih havarija te ostalih neželjenih i nepredviđenih događaja. Navedeni negativni učinci mogu nastati kao posljedica ostvarenja prijetnja koje mogu biti prirodne ili uzrokovane ljudskim djelovanjem (slučajno ili namjerno).

U sklopu planiranja oporavka u slučaju havarije te ostalih neželjenih i nepredviđenih događaja banka bi trebala donijeti plan oporavka kojem je cilj osigurati raspoloživost resursa informacijskog sustava potrebnih za odvijanje kritičnih i/ili vitalnih poslovnih procesa u zahtijevanom vremenu. Plan oporavka je skup procedura koje obuhvaćaju postupke hitnog odgovora na neželjeni događaj i oporavka resursa informacijskog sustava.

Banka bi trebala biti svjesna da su vrijeme i ostali resursi potrebni za provođenje analize utjecaja na poslovanje, procjenu rizika, izradu plana oporavka te izradu pričuvnih kopija neusporedivo manji od resursa koji bi bili potrebni kad navedeno ne bi bilo napravljeno, a kad bi došlo do havarije ili nekog drugog neželjenog i nepredviđenog događaja. Gubitak funkcionalnosti glavnog i/ili pričuvnog računalnog centra može usporiti ili u potpunosti onemogućiti odvijanje poslovnih procesa banke te uzrokovati značajan financijski gubitak, ugroziti konkurentski položaj, utjecati na reputaciju banke i prouzročiti znatne povrede važećih propisa.

Plan oporavka, između ostalog, trebao bi:

- imati jasno definirane postupke oporavka ovisno o vrsti događaja i njegovu učinku na resurse informacijskog sustava, uključujući postupke prelaska na pričuvnu lokaciju
- imati definirane prioritete u oporavku resursa informacijskog sustava potrebnih za odvijanje kritičnih i/ili vitalnih poslovnih procesa
- definirati postupke evakuacije
- definirati odgovornosti i ovlasti osoba zaduženih za oporavak
- imati jasno definirane postupke vezane uz ugovorni odnos s pružateljima usluga, a koji se odnose na oporavak.

Nadalje, plan oporavka trebao bi osigurati sljedeće:

- ubrzati potrebno vrijeme reakcije
- skratiti vrijeme oporavka (primjerice definiranjem rutinskih procedura)
- pomoći u donošenju odluka u kriznim situacijama
- jamčiti pouzdanost pričuvnih sustava.

Najveći prioritet pri oporavku u slučaju havarije te ostalih neželjenih i nepredviđenih događaja ima sigurnost ljudi.

Banka bi trebala osigurati da plan oporavka bude cjelovit, provediv, ažuran, testiran, dokumentiran te troškovno opravdan. Budući da je planiranje oporavka u slučaju havarije te ostalih neželjenih i nepredviđenih događaja iznimno složen i zahtjevan proces, dobre prakse nalažu osnivanje odbora za planiranje oporavka.

7.4. Upravljanje incidentima

Incident je neplanirani i neželjeni događaj čija je posljedica povreda (ili koji neposredno prijeti povredom) važećih propisa RH, politike sigurnosti informacijskog sustava, ostalih internih akata banke vezanih uz informacijsku sigurnost kao i narušavanje temeljnih načela informacijskog sustava, prihvaćenih praksi vezanih uz informacijsku sigurnost te funkcionalnosti informacijskog sustava. Upravljanje incidentima je sastavni dio planiranja kontinuiteta poslovanja jer mu je cilj omogućavanje brzog i učinkovitog odgovora u slučaju narušavanja sigurnosti i funkcionalnosti resursa informacijskog sustava koji podržavaju odvijanje poslovnih procesa.

Kako bi banka mogla djelotvorno i pravodobno reagirati u slučajevima narušavanja funkcionalnosti i sigurnosti dijela ili cijeloga informacijskog sustava, potrebno je planirati postupke u slučaju incidenata, što uključuje i izradu plana odgovora na incidente. Cilj planiranja odgovora na incidente jest smanjivanje rizika od narušavanja sigurnosti i funkcionalnosti informacijskog sustava u incidentnim situacijama te pružanje praktičnih smjernica za djelotvorno postupanje kad se dogode incidenti. Adekvatnim planiranjem odgovora na incidente povećava se sposobnost banke da uspješno i brzo odgovori na incidente, da ograniči i ispravi nastale štetne učinke te da smanji štetne posljedice budućih incidenata. Pretpostavka je za uspješno planiranje odgovora na incidente dobro poznavanje okruženja informacijskog sustava i samog sustava, što se odnosi na poznavanje i praćenje potencijalnih prijetnja, s jedne strane, i poznavanja ranjivosti informacijskog sustava s druge strane.

S obzirom na postupke koji se provode prilikom planiranja odgovora na incidente kao i na postupke u kriznim situacijama, upravljanje incidentima može se podijeliti u osnovne faze:

1. **Priprema.** Faza pripreme uključuje:
   - preventivne metode sprječavanja incidenata
   - podršku rukovodstva
   - određivanje osoba zaduženih za odgovor na incidente te definiranje njihovih ovlasti, odgovornosti i djelokruga rada
   - planiranje komunikacije u hitnim slučajevima
   - organizaciju sustava izvješćivanja
   - izobrazbu zaposlenika u vezi s prepoznavanjem incidenata
   - izobrazbu osoba zaduženih za odgovor na incidente
   - donošenje smjernica za suradnju među različitim organizacijskim jedinicama
   - definiranje odgovornosti korisnika informacijskog sustava u svezi s incidentima
   - uspostavljanje odnosa s nadležnim institucijama kao i drugim timovima za odgovor na incidente.

2. **Identifikacija.** Faza identifikacije uključuje identifikaciju incidenta.

3. **Ograničavanje.** Faza ograničavanja uključuje provođenje potrebnih radnja od strane osoba zaduženih za odgovor na incidente (primjerice ispitivanje situacije, izbjegavanje neovlašteno promijenjenog koda, izradu pričuvne pohrane, procjenu rizika od nastavka rada kompromitiranog dijela informacijskog sustava, suradnju s osobama odgovornim za kompromitirani dio informacijskog sustava, promjenu zaporka i slično).

4. **Uklanjanje.** Faza uklanjanja uključuje:
   - određivanje uzroka i značajka incidenta
   - poboljšanje sigurnosnih postavka informacijskog sustava
   - provođenje analize ranjivosti
   - uklanjanje uzroka incidenta
   - lociranje ažurnih pričuvnih kopija koje su napravljene prije nego što je narušena funkcionalnost i sigurnost informacijskog sustava.

5. **Oporavak.** Faza oporavka uključuje ponovnu uspostavu kompromitiranih dijelova informacijskog sustava te procjenu stanja i nadzor poslovnih procesa.

6. **Izvješćivanje.** Faza izvješćivanja uključuje:
   - izvještavanje o svim fazama upravljanja incidentom te izradu izvješća o incidentu
   - izradu preporuka radi bržeg prepoznavanja ili sprečavanja ponavljanja incidenta.

Upravljanje incidentima obuhvaća i određivanje radnja za obranu od specifičnih napada kao što su maliciozni kod, neovlašteno analiziranje mreže, napad uskraćivanjem usluge (engl. *Denial of Service*), neprimjereno korištenje sustavom, špijunaža, prijevare, neautorizirani pristup i slično. Nadalje, dobre prakse upućuju na potrebu praćenja statistika raznih prijetnja (uključujući različite tipove napada) i ranjivosti sustava. Nemogućnost pravodobnog odgovora na incidente izlaže banku značajnom operativnom, pravnom, reputacijskom i financijskom riziku.

Banka bi trebala donijeti plan odgovora na incidente. Plan odgovora na incidente nastaje dokumentiranjem procesa planiranja odgovora na incidente, a temelji se na procjeni rizika informacijskog sustava. Plan odgovora na incidente trebao bi podržati sve faze upravljanja incidentima pri čemu bi posebno valjalo istaknuti:
- definiranje incidenata te njihovo rangiranje
- definiranje procedura za postupanje u slučaju incidenata
- određivanje postupaka izvješćivanja uprave banke, ostalih odgovornih osoba kao i nadležnih institucija ovisno o učincima sigurnosnog incidenta (primjerice izvješćivanje Hrvatske narodne banke, Ministarstva unutarnjih poslova i slično)
- određivanje osoba zaduženih za odgovore na incidente te definiranje njihova djelokruga rada, ovlasti i odgovornosti
- izobrazbu osoba zaduženih za odgovore na incidente.

Budući da velik broj incidenata ima karakteristike sigurnosnih incidenata pa njihovo rješavanje zahtijeva brzi odgovor te primjenu specijalističkih znanja i multidisciplinarni pristup, dobre prakse nalažu osnivanje operativnog ekspertnog tima koji će odgovarati na incidente. Osobe zadužene za odgovor na incidente odnosno tim za odgovor na incidente (engl. *incident response team*) treba biti u svako vrijeme dostupan svim stranama koje sumnjaju u pojavu ili su primijetile incident. Postupci članova tima za odgovor na incidente obuhvaćaju:
- prikupljanje i analizu informacija o incidentu
- određivanje učinka incidenta
- poduzimanje radnja potrebnih za ograničavanje i smanjivanje nastale štete
- poduzimanje radnja za oporavak kompromitiranih poslovnih procesa.

Dobre prakse nalažu usku suradnju tima za odgovor na incidente i pravnika kako bi se riješila pravna pitanja koja se mogu pojaviti kao posljedica incidenta (primjerice odgovornost banke kada je s njezina sustava koji je kompromitiran izvršen napad na sustav neke druge institucije, utvrđivanje odgovornosti za nastalu štetu te odgovornost banke za izvješćivanje nadležnih institucija u slučaju incidenata).

7.5. Upravljanje pričuvnom pohranom

Proces upravljanja pričuvnom pohranom obuhvaća postupke izrade, pohrane, testiranja i restauracije podataka s pričuvnih kopija. Pričuvne kopije moraju sadržavati sve podatke (poslovne podatke, dokumentaciju, aplikativni i sistemski softver i slično) koji su potrebni za ponovno uspostavljanje poslovnih procesa koje podržava informacijski sustav banke. Izrada pričuvnih kopija podataka koji se nalaze u informacijskom sustavu zadatak je s visokim prioritetom u procesu upravljanja informacijskim sustavom.

Upravljanje pričuvnom pohranom potrebno je uspostaviti u skladu s klasifikacijom informacija, analizom utjecaja na poslovanje i procjenom rizika, kako bi se osigurala temeljna načela informacijskog sustava.

Banka bi trebala osigurati postojanje ažurnih pričuvnih kopija kao i provjerenih i testiranih metoda restauriranja podataka, odnosno ponovnog uspostavljanja poslovnih procesa kako bi bio moguć uspješan oporavak u slučaju incidenata, havarija te ostalih neželjenih i nepredviđenih događaja.

Banka bi trebala donijeti interne akte kojima se definiraju kriteriji, načini i postupci upravljanja pričuvnom pohranom kao što su kategorizacija, učestalost izrade, vrsta, rukovanje, pohrana, restauracija i čuvanje pričuvnih kopija. Isto tako, potrebno je definirati i ovlasti i odgovornosti za upravljanje pričuvnom pohranom.

Pričuvne kopije omogućuju oporavak informacijskog sustava u slučajevima gubitka podataka povezanih s događajima kao što su:

- sigurnosni incidenti
- brisanje podataka zbog slučajnih ili namjernih događaja
- neočekivani prekidi u radu informacijskog sustava
- havarije
- ostali neželjeni i nepredviđeni događaji.

Uobičajene dobre prakse pri uspostavljanju sustava upravljanja pričuvnom pohranom uključuju, između ostalog, sljedeće:

- određivanje učestalosti izrade pričuvnih kopija s obzirom na rizik i klasifikaciju informacija te u skladu s time sastavljanje plana izrade pričuvnih kopija
- izradu, održavanje i pregled evidencije o pričuvnim kopijama
- obilježavanje medija na kojima su pohranjeni podaci, što uključuje informacije kao što su sadržaj, datum izrade, vrsta kopije, sistemsko okruženje, razina osjetljivosti te ostale informacije
- izradu pričuvnih kopija sistemskih datoteka (primjerice operativnih sustava, pogonskih programa za hardver i slično)
- adekvatno upravljanje fizičkom sigurnošću pričuvnih kopija
- verificiranje podataka na pričuvnim kopijama kako bi se omogućila uspješna restauracija podataka
- periodično restauriranje podataka na testnu okolinu i/ili provjeru pomoću odgovarajućega softverskog alata kako bi se potvrdilo da su pričuvne kopije pohranjene na ispravan način, da nije narušen integritet podataka te da je podatke moguće restaurirati

- periodično revidiranje procesa izrade i pohrane pričuvnih kopija
- redovito pohranjivanje pričuvnih kopija na udaljenu sigurnu lokaciju
- uporabu kriptografskih metoda
- redovito zamjenjivanje i odlaganje medija na kojima se pohranjuju podaci
- osiguranje raspoloživosti pričuvnoga računalnog centra na udaljenoj lokaciji. Pričuvni računalni centar, ovisno o procjeni rizika, može imati različitu razinu opremljenosti: od redundantnog, koji je opremljen jednako kao i glavni računalni centar, do centra koji ima samo adekvatni prostor i instalacije (energetsku i telekomunikacijsku mrežu te ostale potrebne instalacije). Posebnu pozornost potrebno je posvetiti telekomunikacijskoj povezanosti pričuvnog centra i ugovornim odnosima banke s pružateljima usluga i dobavljačima opreme.

8. Razvoj sustava i eksternalizacija

8.1. Razvoj informacijskih sustava unutar banke

Razvoj informacijskih sustava unutar banke (engl. *in-house development*) složen je proces, koji je potrebno precizno i detaljno definirati te standardizirati kako bi se rizici razvoja sveli na najmanju moguću mjeru. Banka bi trebala donijeti interne akte koji propisuju postupak razvoja informacijskih sustava i koji će se primjenjivati na sve razvojne projekte (u nastavku teksta: projekte), neovisno o karakteristikama samih projekata. Navedeni akti trebali bi obuhvatiti barem sljedeća područja:

- planiranje i formalnu organizaciju projekta razvoja informacijskih sustava
- programski razvoj i isporuku informacijskih sustava
- održavanje informacijskih sustava.

Interni akti o razvoju informacijskih sustava trebali bi za svako od navedenih područja propisati postupke odobravanja, pregleda, provođenja i dokumentiranja važnijih aktivnosti. Pri razvoju informacijskih sustava potrebno je uvijek imati u vidu sigurnost cjelokupnog sustava. Prilikom provedbe opsežnijih projekata razvoja informacijskih sustava obično se propisuju i posebni standardi koji se primjenjuju na taj projekt. Navedeni posebni standardi trebali bi biti u skladu s internim aktima banke. Projekti koji se mogu promatrati kao izmjene već postojećih sustava moraju biti u skladu s postupcima definiranim u poglavlju "Upravljanje promjenama".

8.1.1. Planiranje i formalna organizacija projekta razvoja informacijskih sustava

Planiranje projekta je kritično razdoblje životnog ciklusa informacijskog sustava. Propusti u procesu planiranja često se manifestiraju kao pomicanje rokova, povećanje troškova, neadekvatno ispunjavanje ciljeva ili čak odustajanje od projekta. Stoga je potrebno definirati sve parametre koji se moraju analizirati i dokumentirati u ovom procesu.

Prije započinjanja projekta odgovorne osobe u banci trebale bi izraditi formalni plan koji će definirati standarde i postupke koji će se primjenjivati u svim fazama razvoja informacijskog sustava. Detaljnost i formalnost projektnog plana trebaju biti razmjerne opsegu projekta i procjeni rizika. Dobre prakse nalažu da projektni plan obuhvaća barem sljedeće:

- jasan prikaz sadašnjeg stanja (uključujući međuovisnosti s postojećim sustavom) te potreba korisnika i preciznu definiciju ciljeva projekta
- analizu isplativosti projekta koja će identificirati očekivane koristi i troškove razvoja sustava te procijeniti moguća alternativna rješenja
- definiranje uloga i odgovornosti osoba koje će biti uključene u razvoj i isporuku sustava
- jasno razdvajanje dužnosti između osoba koje će biti zadužene za implementaciju informacijskog sustava i osoba koje će biti zadužene za kontrolu te implementacije;
- propisivanje postupaka komunikacije i izvješćivanja svih osoba koje će biti uključene u razvoj i isporuku sustava
- identifikaciju potrebne dokumentacije koja treba nastati u sklopu projekta razvoja informacijskog sustava

- definiranje standarda za pisanje dokumentacije, koji će precizno opisati svrhu i formu svakog potrebnog dokumenta te uvjete pod kojima navedeni dokument nastaje
- planove testiranja
- planove izobrazbe osoba uključenih u projekt kako bi se on dovršio unutar planiranih vremenskih i financijskih okvira te da bi se uspješno održavao novonastali sustav
- definiranje kontrolnih mehanizama koji će pratiti tijek projekta i aktivnosti koje se moraju poduzeti u slučaju odstupanja od projektnog plana.

8.1.2. Programski razvoj i isporuka sustava

Programski razvoj informacijskih sustava može se podijeliti (neovisno o odabranoj razvojnoj metodologiji i tehnologiji), između ostalog, na sljedeće procese:

- analizu i projektiranje
- programiranje
- testiranje
- uvođenje u produkcijski rad.

U svakom od navedenih procesa moraju se primjenjivati odgovarajuće procedure definirane pri planiranju i organizaciji projekta. Standardi programskog razvoja informacijskih sustava trebali bi biti dovoljno fleksibilni, kako se njima ne bi ograničavala kreativna i kvalitetna rješenja.

Dobre prakse nalažu da razvojna, testna i produkcijska okolina budu međusobno odvojene na odgovarajući način.

8.1.2.1. Analiza i projektiranje

U postupku analize i projektiranja informacijskog sustava odgovorne osobe trebale bi podijeliti projekt u projektne zadatke koje će zaposlenici i druge osobe moći samostalno rješavati (primjerice programeri). Pri analizi i projektiranju posebnu pozornost potrebno je posvetiti kontrolama sigurnosti. Isto tako, prilikom podjele projekta u projektne zadatke potrebno je izgraditi odgovarajuću dokumentaciju svakoga projektnog zadatka, koja bi morala sadržavati barem sljedeće:

- opis poslovnog procesa ili dijela poslovnog procesa koji će se implementirati projektnim zadatkom
- opis potrebnih funkcionalnosti procesa opisanog u projektnom zadatku uključujući (gdje je to moguće) i grafičke prikaze
- međuovisnosti s postojećim poslovnim procesima i sustavom
- opis svih kontrola koje moraju biti ugrađene u sustav
- opis ulaznih i izlaznih vrijednosti projektnog zadatka
- specifikaciju procesa koje treba zabilježiti u operativnim i sistemskim zapisima
- popis osoba koje su zadužene za provedbu projektnog zadatka
- vremenski plan obavljanja projektnog zadatka

- osnovni plan testiranja koji će pokazati da realizirani projektni zadatak daje očekivane rezultate.

8.1.2.2. Programiranje

Dobre prakse nalažu propisivanje standarda programiranja koji bi trebali obuhvatiti barem sljedeće:

- principe i pravila pisanja programskog koda, nazivanja programskih dijelova, varijabla, elemenata baza podataka i slično
- obavezne kontrole koje treba ugraditi neovisno o specifičnostima određenoga projektnog zadatka
- principe i pravila upotrebe i dokumentiranja standardiziranih programskih rutina kako bi se izbjeglo dupliciranje programskoga koda.

Aktivnosti programera trebale bi biti jasno definirane. Pristup programima izvan programerovih osobnih odgovornosti potrebno je ograničiti. Izvorni programski kod morao bi biti adekvatno zaštićen s obzirom na potrebu za održavanjem temeljnih načela informacijskog sustava.

8.1.2.3. Testiranje

Prije puštanja informacijskog sustava u produkcijski rad potrebno je provesti testiranje. Testiranje razvijenog sustava trebalo bi biti detaljno i na adekvatan način kontrolirano, kako bi se utvrdilo odgovara li razvijeni sustav postavljenim ciljevima. Potrebno je propisati procedure testiranja te prije samog početka testiranja izraditi detaljni testni plan. Testni plan trebao bi obuhvaćati kombinacije kojima će se analizirati ponašanje sustava:

- u standardnim uvjetima
- u graničnim slučajevima
- u svim realno zamislivim neregularnim situacijama.

Testove je potrebno provoditi u kontroliranim uvjetima i upotrijebiti prethodno definirane podatke. Testni podaci trebali bi biti što sličniji pravim, produkcijskim podacima. Pri testiranju potrebno je voditi računa o povjerljivosti informacija. Dobre prakse nalažu verifikaciju rezultata testiranja tako da se usporede s unaprijed definiranim očekivanim rezultatima. Rezultati testova trebali bi se dokumentirati u standardiziranoj, propisanoj formi. Konačne rezultate trebale bi prekontrolirati sve uključene strane te pisano potvrditi njihovu prihvatljivost.

8.1.2.4. Uvođenje informacijskog sustava u produkcijski rad

Banka bi trebala propisati postupke uvođenja novih ili izmijenjenih sustava u produkcijski rad. Navedene procedure trebale bi definirati ovlasti, odgovornosti i način prijenosa s testnog na produkcijsko okruženje. Prije uvođenja sustava u produkcijski rad potrebno je:

- organizirati izobrazbu svih zaposlenika koji će se tim sustavom služiti
- svim korisnicima omogućiti pristup potpunoj korisničkoj dokumentaciji s jednostavnim, netehničkim opisom svih funkcionalnosti kojima će se služiti u radu.

8.1.3. Održavanje informacijskih sustava

Banka bi trebala definirati postupke održavanja informacijskih sustava i promjena tih sustava. Sve programske promjene trebale bi se strogo kontrolirati i dokumentirati kako bi se spriječile bilo kakve neovlaštene promjene te osiguralo održavanje temeljnih načela informacijskog sustava. Provođenje promjena trebalo bi biti u skladu s propisanim internim aktima banke vezanim uz upravljanje promjenama. Programske promjene većeg opsega treba tretirati kao zasebne projekte i na njih valja primijeniti već navedene procese planiranja i formalne organizacije te programskog razvoja i isporuke informacijskih sustava. Banka bi trebala propisati standardne postupke za dokumentiranje programskih promjena informacijskih sustava koji trebaju obuhvatiti barem sljedeće:

- identifikaciju programa ili sustava
- identifikaciju osobe koja je inicirala promjenu sustava
- datum kada je zatražena promjena sustava
- opis tražene promjene
- odobrenje zatražene promjene.

Prilikom izrade traženih promjena valja slijediti sve navedene smjernice za programski razvoj i isporuku informacijskih sustava. U sklopu analize, projektiranja, programiranja i testiranja sustava treba analizirati i dokumentirati sigurnosne rizike i negativne utjecaje koji mogu nastati na sustavu kao posljedica programske promjene.

U određenim uvjetima može se pojaviti potreba za hitnom promjenom programa, zaobilaženjem standardnih postupaka provođenja promjena, odnosno izradom izvanrednih ili privremenih programskih promjena. Banka bi trebala propisati takve postupke koji će obuhvatiti barem sljedeće:

- opis situacija u kojima se smiju provoditi izvanredne ili privremene programske promjene
- popis osoba ovlaštenih za odobravanje izvanrednih ili privremenih programskih promjena
- kontrolne postupke za sprječavanje zloporabe.

Nakon što je sustav izmijenjen po hitnoj proceduri, izvanredne ili privremene programske promjene potrebno je dokumentirati kao i ostale promjene.

8.2. Eksternalizacija (dijela) informacijskog sustava

Nastojanje da se smanje troškovi poslovanja te potreba za visokom razinom usluga i vrlo visokom stručnom osposobljenošću zaposlenika često nameću potrebu da banke eksternaliziraju poslovne procese (ili dio poslovnih procesa) te da se koriste uslugama pružatelja usluga kako bi ostvarile svoje strateške ciljeve.

Korištenje usluga koje čine sastavni dio poslovnih procesa banke, a koje na temelju ugovora banci pružaju pružatelji usluga na kontinuiranoj osnovi i kojima se podržava pružanje bankovnih, financijskih i/ili pomoćnih bankovnih usluga od strane same banke, naziva se *eksternalizacija* (engl. *outsourcing*). Postupak nabave robe te ugovor(i) o nabavi robe (primjerice nabavi informacijske, hardverske i softverske imovine) ne smatraju se eksternalizacijom.

Različiti modeli eksternalizacije prisutni su ne samo u bankarskom sektoru nego u svim ostalim poslovnim sektorima. S obzirom na velik utjecaj eksternalizacije u svakodnevnom poslovanju banaka i rizik vezan uz eksternalizaciju, banke bi trebale na adekvatan način upravljati odnosom s pružateljem usluga i nadzirati pružanje usluga u skladu s odredbama ugovora. Nadalje, banke bi trebale poduzeti potrebne korake kako bi se rizik eksternalizacije smanjio na prihvatljivu razinu s obzirom na to da se obujam aktivnosti i poslovnih procesa banaka koji su predmet eksternalizacije, uključujući i aktivnosti vezane uz informacijski sustav sve više povećava.

Predmetom eksternalizacije mogu biti različite aktivnosti vezane uz informacijski sustav, primjerice:

- usluge održavanja hardvera
- usluge obrade podataka
- usluge razvoja poslovnih aplikacija
- usluge održavanja poslovnih aplikacija
- usluge upravljanja operativnim sustavima i usluge održavanja tih sustava
- usluge upravljanja telekomunikacijskim mrežama i održavanja tih mreža
- usluge upravljanja bazama podataka i održavanja tih baza
- usluge upravljanja sigurnosnom infrastrukturom i održavanja te infrastrukture
- usluge upravljanja internetskim stranicama i održavanja tih stranica
- usluge e-bankarstva
- usluge upravljanja pozivnim centrima (engl. *call-center*) i održavanja tih centara
- usluge upravljanja centrima za pomoć korisnicima (engl. *help-desk*) i održavanja tih centara
- usluge upravljanja podacima (skladištenje podataka, pronalaženje podataka - tzv. rudarenje - engl. *data mining*) i održavanja tih podataka.

Za potrebe ovog dokumenta eksternalizacija aktivnosti vezanih uz informacijski sustav smatra se eksternalizacijom (dijela) informacijskog sustava. U nastavku teksta pojam eksternalizacija odnosi se na eksternalizaciju (dijela) informacijskog sustava.

Odluka o eksternalizaciji strateška je odluka banke, koja treba biti usklađena s poslovnom strategijom i ciljevima banke te, između ostaloga, ovisi:

- o sposobnosti banke da upravlja rizikom vezanim uz eksternalizaciju (dijela) poslovnih procesa
- o načinu nadzora i kontrole ugovorenih aktivnosti
- o usklađenosti s važećim propisima.

Pružatelji usluga bankama mogu biti rezidenti i nerezidenti. S tim u svezi treba napomenuti da izravni nadzor koji provodi Hrvatska narodna banka u odnosu na pružanje usluga od strane pružatelja usluga rezidenta i/ili nerezidenta ne smije ni na koji način i ni u kojem trenutku biti onemogućen, ograničen ili otežan bez obzira na to obavlja li se na teritoriju Republike Hrvatske ili izvan njega.

Radi postizanja prethodno navedenoga, ako je pružatelj usluga nerezident, banke bi svakako trebale prije donošenja odluke o izboru pojedinog pružatelja usluga utvrditi da li zakonodavstvo odnosno propisi države u kojima dotični pružatelj usluga posluje, omogućavaju Hrvatskoj narodnoj banci da ostvari cjelovit i neograničen pristup djelatnostima i poslovima u svezi s kojima obavlja nadzor.

Ugovor(i) i nalazi odnosno izvješća unutarnjih i vanjskih revizora vezani uz eksternalizaciju (dijela) poslovnih procesa trebali bi biti dostupni na hrvatskom jeziku zbog njihove bolje razumljivosti kako bi se točnije provelo analiziranje, ocjenjivanje i revidiranje aktivnosti koje su predmet eksternalizacije.

Rizik u poslovanju postoji bez obzira na to hoće li banke same obavljati aktivnosti vezane uz informacijski sustav ili će se koristiti uslugama pružatelja usluga. Pri razmatranju svrhovitosti eksternalizacije aktivnosti vezanih uz informacijski sustav banke trebaju:

- biti svjesne rizika vezanog uz eksternalizaciju aktivnosti vezanih uz informacijski sustav
- osigurati da odnos između banke i pružatelja usluga bude prihvatljiv sa stajališta rizika i u skladu s poslovnim ciljevima banke
- implementirati adekvatne zaštitne mjere i kontrole kojima bi se smanjili identificirani rizici
- osigurati kontinuirano praćenje rizika kako bi se identificirale i procijenile promjene u odnosu na inicijalnu procjenu rizika
- regulirati sve elemente i postupke koji se odnose na eksternalizaciju aktivnosti vezanih uz informacijski sustav svojim internim aktima.

Upravljanje rizikom eksternalizacije uključuje:

- procjenu rizika vezanog uz eksternalizaciju
- dubinsko ispitivanje (engl. *due diligence*) pružatelja usluga pri njegovu odabiru
- definiranje sadržaja ugovora s pružateljem usluga
- osiguravanje kontinuiranog nadzora pružanja usluga u skladu s ugovornim obvezama
- osiguravanje neograničenoga i svakodobnog pristupa informacijama povezanim s uslugom koja je predmet eksternalizacije.

8.2.1. Procjena rizika vezanog uz eksternalizaciju

Prije sklapanja ugovora s pružateljem usluga banka bi trebala procijeniti rizik eksternalizacije i mogućnosti kontrole tog rizika. Pri toj procjeni potrebno je osobitu pozornost posvetiti procjeni rizika koji bi mogli utjecati na financijske rezultate, financijsku poziciju, kontinuitet poslovanja ili reputaciju banke. Za svaki pojedinačni slučaj eksternalizacije (dijela) poslovnih procesa banka treba procijeniti rizik eksternalizacije.

Kao dio procjene rizika eksternalizacije banka bi trebala procijeniti primjerice: strateški rizik, operativni rizik (npr. rizik gubitka podataka i kontrole nad značajnim poslovnim procesima, rizik povezan s korištenjem informacijske tehnologije, rizik povezan s raspoloživošću usluge, rizik prekida kontinuiteta poslovanja, transakcijski rizik i sl.), financijski rizik (primjerice rizik povećanja troškova), reputacijski rizik, pravni rizik (primjerice neusklađenost s propisima) te rizik zemlje podrijetla pružatelja usluga. Isto tako, banka treba procijeniti na koji će način odnos s pružateljem usluga pomoći ostvarivanju strateških ciljeva i zadovoljavanju poslovnih potreba banke.

Pri procjeni rizika vezanog uz eksternalizaciju aktivnosti vezanih uz informacijski sustav banka bi trebala procijeniti sljedeće:

- mogućnost pružatelja usluga da osigura pružanje usluga u skladu sa strateškim ciljevima i poslovnim potrebama banke,
- pouzdanost, ekonomsku održivost i sposobnost pružatelja usluga,
- način na koji će banka nadzirati pružanje usluga,
- adekvatnost stručnog osoblja u banci, odnosno je li ono u stanju provoditi kvalitetan nadzor nad pružateljem usluga i na adekvatan način upravljati odnosom s pružateljem usluga,
- važnost, opseg i složenost (dijelova) poslovnih procesa koji su predmet eksternalizacije,
- mogućnost "vraćanja" u banku (engl. *reinsourcing*) aktivnosti vezanih uz informacijski sustav koje će se eksternalizirati, za slučaj da pružatelj usluga ne postupa u skladu s odredbama ugovora ili ne održava ugovorenu kvalitetu pružene usluge.

8.2.2. Dubinsko ispitivanje pružatelja usluga pri njegovu odabiru

Nakon što je napravljena procjena rizika eksternalizacije banka bi trebala provesti dubinsko ispitivanje pružatelja usluga kako bi se utvrdilo može li pružatelj usluga (financijski i operativno) pružiti banci zahtijevane usluge. Odabir sposobnoga i kvalitetnog pružatelja

usluga osobito je važan kako bi se smanjio rizik eksternalizacije. Ovisno o utvrđenim rizicima, banka bi trebala pri provedbi dubinskog ispitivanja uzeti u obzir sljedeće:

- iskustvo pružatelja usluga i mogućnosti pružanja potrebnih usluga radi ispunjenja postojećih i očekivanih potreba banke
- reputaciju i tržišni udio pružatelja usluga
- eventualne podizvođače pružatelja usluga koji će pružati podršku pružatelju usluga u ispunjavanju ugovornih obveza prema banci
- eventualnu potrebu za dodatnim sustavima, konverzijama podataka i uslugama
- sposobnost pružatelja usluga da na odgovarajući način postupi u slučaju privremene nemogućnosti pružanja usluga iz bilo kojeg razloga
- stručnu osposobljenost odgovornih osoba koje će biti određene za pružanje podrške banci
- lokaciju pružanja usluga kako bi se utvrdili uvjeti pod kojima pružatelj usluga djeluje i pruža svoje usluge,
- revizorska i posljednja financijska izvješća pružatelja usluga
- mogućnost neograničenog i svakodobnog pristupa svojim informacijama
- poznavanje propisa relevantnih za pružanje usluga koje su predmet eksternalizacije.

Nadalje, banka bi trebala pri provedbi dubinskog ispitivanja pružatelja usluga čije je pružanje usluga vrlo važno za banku, uzeti u obzir i sljedeće:

- adekvatnost internih akata pružatelja usluga koji se odnose:
  - na upravljanje informacijskim sustavom
  - na sigurnost informacijskog sustava
  - na upravljačke, logičke i fizičke kontrole
  - na planiranje kontinuiteta poslovanja
  - na upravljanje operativnim i sistemskim zapisima
  - na razvoj i održavanje informacijskog sustava,
- adekvatnost kontrola primijenjenih kod pružatelja usluga
- financijske mogućnosti investiranja i pružanja zahtijevane podrške od strane pružatelja usluga
- postojanje odgovarajućeg osiguranja, ugovorenog od strane pružatelja usluga.

8.2.3. Definiranje sadržaja ugovora s pružateljem usluga

Uprava banke odgovorna je prema ZOB-u za svaku aktivnost koju za potrebe banke provodi pružatelj usluga.

U ugovoru između banke i pružatelja usluga treba definirati poslovne potrebe banke te regulirati čimbenike rizika identificirane pri procjeni rizika eksternalizacije i dubinskog ispitivanja. Uprava banke dužna je ugovornim odredbama osigurati zaštitu bankovne i poslovne tajne, povjerljivost bančinih podataka te omogućiti Hrvatskoj narodnoj banci obavljanje nadzora.

Ugovori trebaju biti u pisanom obliku, jasno sastavljeni i dovoljno detaljni kako bi osigurali ispunjavanje preuzetih obveza koje se odnose na pružanje usluga. Isto tako, ugovori trebaju jasno definirati sve relevantne pojmove, uvjete, prava i obveze te odgovornosti ugovornih strana, pri čemu minimalno trebaju sadržavati sljedeće odredbe:

- detaljan opis usluga koje su predmet ugovora te način ispunjenja ugovornih obveza
- odgovornost za štetu u slučaju povrede ugovornih obveza
- obvezu pružatelja usluga da prije zaključenja ugovora s podizvođačem zatraži prethodnu pismenu suglasnost banke
- obvezu zaštite bankovne i poslovne tajne te povjerljivosti bančinih podataka
- detaljan opis prava i obveza ugovornih strana za slučaj prestanka ugovora, i to na način koji će osigurati kontinuitet poslovanja banke
- pravo banke na pristup informacijama i vlasništvo nad informacijama
- način na koji će banka obavljati nadzor nad pružateljem usluga
- osigurati zaposlenicima Hrvatske narodne banke izravni nadzor djelatnosti i poslova u svezi s kojima Hrvatska narodna banka obavlja nadzor
- osigurati zaposlenicima Hrvatske narodne banke fizički pristup resursima pružatelja usluga koji su neophodni za izvršenje usluga koje su predmet ugovora
- odgovornost pružatelja usluga za neobavljene, nepravodobne i neispravne transakcije i ostale ugovorene aktivnosti
- detaljan opis prava i obveza ugovornih strana koje će osigurati kontinuitet poslovanja banke u slučaju raskida ugovora
- identifikaciju ključnih kontrola, vremena odgovora na incidente, procedura i stupnjeva eskalacije u slučaju pojave nepredviđenih događaja, pokrivenosti osiguranjem, mogućnosti oporavka te drugih mjera upravljanja rizicima koje bi pružatelj usluga trebao primijeniti
- osigurati uvid u financijska izvješća, izvješća unutarnje i vanjske revizije kao i u ostala izvješća vezana uz poslovanje pružatelja usluga, a koja bi mogla biti relevantna za banku.

8.2.4. Osiguravanje kontinuiranog nadzora pružanja usluga u skladu s ugovornim obvezama

Nakon sklapanja ugovora s pružateljem usluga banka bi trebala uvesti adekvatan sustav nadzora i kontinuirano ga provoditi kako bi kontrolirala način pružanja usluga i kvalitetu pruženih usluga.

Isto tako, banka treba utvrditi je li pružatelj usluga implementirao i primjenjuje li kontinuirano adekvatne kontrole vezane uz pružanje usluga koje su predmet ugovora. Kontrole trebaju biti barem jednake kontrolama koje bi bile primijenjene kad bi se dotične aktivnosti obavljale u banci.

Banka treba osigurati stručno osoblje koje je u stanju omogućiti kvalitetan nadzor nad pružateljem usluga i koje će na adekvatan način upravljati odnosom s pružateljem usluga.

Kontinuirani nadzor pružanja usluga u skladu s ugovornim obvezama treba obuhvaćati barem sljedeće:

- praćenje i analiziranje kvalitete obavljanja usluga
- praćenje svih činjenica i okolnosti koje mogu utjecati na potrebu da se izmijeni ugovor
- praćenje i analiziranje financijskog stanja te priljeva i odljeva kadrova kod pružatelja usluga kako bi se na vrijeme uočile financijske poteškoće i izbjegli rizici za banku koji proizlaze iz nemogućnosti pružanja ugovorenih usluga

- procjenjivanje kvalitete revizorskih izvješća pružatelja usluga kako bi se ustanovilo jesu li opseg i dubina revizije adekvatni i u skladu s pravilima struke

Nadalje, banka bi trebala u sklopu provedbe nadzora pružatelja usluga čije je pružanje usluga vrlo važno za banku, obuhvatiti i sljedeće:

- praćenje i analiziranje sadržaja i kvalitete internih akata pružatelja usluga kako bi se uočila eventualna odstupanja od zadanih smjernica i ugovornih obveza
- neposredan uvid na lokaciji pružanja usluga kako bi se utvrdila primjenjivost donesenih internih akata pružatelja usluga
- procjenjivanje rezultata testiranja plana kontinuiteta poslovanja i plana oporavka
- praćenje postojanja odgovarajućeg osiguranja, ugovorenog od strane pružatelja usluga.

8.2.5. Osiguravanje neograničenoga i svakodobnog pristupa informacijama

Banci mora biti osiguran neograničen i svakodobni pristup informacijama koje su predmet eksternalizacije ili su na bilo koji način povezane s eksternalizacijom (dijela) poslovnih procesa. Isto tako, banke bi trebale imati adekvatan plan kako bi se osigurao kontinuirani pristup informacijama i kontinuitet poslovnih procesa u slučaju neočekivanog prekida ili ograničenja pružanja usluga od strane pružatelja usluga.

9. E-bankarstvo

9.1. Uvod

Za potrebe ovog dokumenta elektroničko bankarstvo (u nastavku teksta: e-bankarstvo) definira se kao neposredna ponuda novih i tradicionalnih proizvoda i usluga klijentima putem elektroničkih interaktivnih komunikacijskih kanala. E-bankarstvo uključuje sustave koji klijentima banke pružaju bankarske proizvode i usluge (to su primjerice pristup financijskim informacijama, vođenje poslovanja, informiranje o proizvodima i uslugama, personalizirani financijski portali, agregirani računi, elektroničko plaćanje, elektronički novac i slično).

Budući da je uslugama i proizvodima e-bankarstva većim dijelom podrška informacijska infrastruktura banke koja je podrška i tradicionalnim distribucijskim kanalima, sve navedeno u ostalim poglavljima ovog dokumenta odnosi se i na e-bankarstvo. U ovom poglavlju naglasit će se specifičnosti pojedinih zahtjeva koji proizlaze iz potrebe za adekvatnim upravljanjem rizicima povezanima s e-bankarstvom.

E-bankarstvo možemo podijeliti u tri kategorije:

1. **informativno:** odnosi se na pružanje informacija klijentima o proizvodima i uslugama; iako rizik za banku u ovom slučaju nije velik, potrebno je uvesti kontrole kako bi se spriječile neautorizirane promjene informacija koje se prezentiraju klijentima;
2. **komunikacijsko:** odnosi se na interakciju banke i klijenata (primjerice obuhvaća promjene osobnih podataka, traženje informacija o financijskim računima kao što su stanja i transakcije, podnošenje zahtjeva za kreditom i slično); rizik je za banku bitno veći, posebice zato što u većini slučajeva postoji veza između infrastrukture e-bankarstva koja prezentira informacije i usluge klijentu te ostalih dijelova infrastrukture informacijskog sustava banke;
3. **transakcijsko:** odnosi se na provođenje transakcija (primjerice prijenos novca s računa na račun, kupnja vrijednosnih papira i slično); rizik je najveći i u skladu s time trebaju biti primijenjene adekvatne kontrole.

Stalne tehnološke inovacije, širenje telekomunikacijskih kanala, a posebice interneta, te sve veća konkurencija na tržištu omogućili su ubrzan razvoj postojećih i novih bankarskih proizvoda, usluga te načina isporuke, što stvara nove poslovne mogućnosti za banke i njihove klijente. Iako samo e-bankarstvo nije uzrok nastanka novih rizika u poslovanju banaka, razvidno je da e-bankarstvo utječe na povećanje i promjenu karakteristika već poznatih rizika u bankarskom poslovanju (primjerice strateškog, operativnog, pravnog i reputacijskog rizika). Neka od specifičnih svojstava e-bankarstva, između ostalog, uključuju:

- izrazito brze promjene vezane uz informacijsku tehnologiju
- promjenu očekivanja klijenata
- sve veću konkurenciju
- široku dostupnost telekomunikacijskih mreža (primjerice interneta)
- sve manje tradicionalne komunikacije između klijenta i banke
- integraciju aplikacija koje podržavaju e-bankarstvo s tradicionalnim bankarskim aplikacijama
- veliku ovisnost banaka o dobavljačima i pružateljima usluga
- ubrzanu pojavu prijetnja i ranjivosti povezanih s telekomunikacijskim mrežama.

Iz prije navedenog može se zaključiti da postojeći sustav upravljanja rizikom u banci mora biti prilagođen kako bi adekvatno obuhvatio posebnosti rizika koje proizlaze iz specifičnih svojstava e-bankarstva, opsega e-bankarstva u ukupnom poslovanju te mogućnosti banke da upravlja rizicima. Sve navedeno povećava potrebu da se i prije uvođenja (nove) e-bankarske usluge provede procjena rizika e-bankarstva i izradi (ažurira) strategija e-bankarstva.

9.2. Rizici povezani s e-bankarstvom

Brzim napretkom informacijske tehnologije i njezinim uvođenjem kao i tehnološkom složenošću poslova e-bankarstva posebno su povećani rizici povezani s e-bankarstvom odnosno operativni, reputacijski, pravni i strateški rizik. Banka bi trebala osigurati adekvatnost usluga e-bankarstva s obzirom na temeljna načela informacijskih sustava kako bi se smanjili prije navedeni rizici. Budući da klijenti banke očekuju svakodobnu raspoloživost usluge, banka bi trebala osigurati dovoljan kapacitet i redundanciju resursa informacijskog sustava kako bi usluge bile pouzdane i raspoložive.

Nadalje, kako bi se banka zaštitila od pravnog i reputacijskog rizika, usluge e-bankarstva moraju biti pružene na dosljedan i pravodoban način u skladu s važećim propisima i u skladu s korisničkim očekivanjima da će usluge biti brze i neprekidne. Isto tako, banka je dužna pružiti svojim klijentima sigurnost s obzirom na povjerljivost i integritet podataka.

Čuvanje povjerljivosti podataka klijenata zakonska je obveza banke pa postupanje protivno važećim propisima izlaže banku pravnom i reputacijskom riziku. Banka bi trebala na temelju procjene rizika primijeniti adekvatne zaštitne mjere i kontrole koje će osiguravati zaštitu povjerljivosti podataka o klijentima te donijeti pripadajuće interne akte i standarde.

Čimbenici koji određuju pravni i reputacijski rizik povezan s e-bankarstvom proizlaze i iz činjenice da je e-bankarstvo relativno nov distribucijski kanal kao i iz izrazito velikog povećanja upotrebe e-bankarstva. Neki od čimbenika koji imaju utjecaj na pravni i reputacijski rizik jesu:

- neovlašteno (namjerno ili slučajno) otkrivanje, mijenjanje ili uništavanje informacija
- gubitak povjerenja klijenata i javnosti zbog neovlaštenih radnja na računima klijenata
- neovlašteno objavljivanje povjerljivih podataka
- nenamjerne greške i propusti
- poremećaji rada informacijskog sustava
- nemogućnost pružanja usluge na očekivani način (primjerice nezadovoljavajuća funkcionalnost, raspoloživost i slično)
- pritužbe klijenata na teškoće pri korištenju usluge e-bankarstva
- neprimjereno upravljanje informacijskim sustavom
- nemogućnost adekvatnog i pravodobnog odgovora banke na pritužbe klijenata.

Strateški rizik može proizaći iz nedostatka jasno definiranih poslovnih ciljeva prema kojima se vrednuje uspjeh provedbe strategije e-bankarstva, loših i proturječnih poslovnih odluka, neadekvatne primjene poslovnih odluka te neprilagođivanja promjenama u okruženju. Prije donošenja odluke o uvođenju e-bankarstva banka bi trebala biti upoznata s rizicima povezanima s e-bankarstvom te napraviti analizu isplativosti odnosno procijeniti cjelokupne troškove uvođenja e-bankarstva i upravljanja njime.

9.3. Upravljanje rizikom e-bankarstva

Kao što je već navedeno, upravljanje rizikom je proces procjene rizika, poduzimanja radnja za smanjenje rizika na prihvatljivu razinu i održavanja te razine rizika. Banka bi trebala osigurati da je upravljanje rizikom e-bankarstva sastavni dio sveobuhvatnog upravljanja rizicima kojima je banka u svom poslovanju izložena.

Proces upravljanja rizikom i nadzor e-bankarstva trebaju provoditi osobe s adekvatnim stručnim znanjima, bez obzira je li e-bankarstvo podržano u banci ili od strane pružatelja usluga. Isto tako, banka bi trebala nadzirati razvoj, implementaciju i održavanje sigurnosne infrastrukture koja će učinkovito štititi resurse e-bankarstva od unutarnjih i vanjskih prijetnja. Sigurnosna infrastruktura e-bankarstva i upravljanje njome uključuju barem sljedeće:

- detaljne interne akte vezane uz e-bankarstvo
- logičke i fizičke kontrole, osobito kontrole pristupa
- primjerenu infrastrukturu koja ograničava aktivnosti korisnika informacijskog sustava
- dodjelu odgovornosti za nadzor razvoja, implementacije i održavanja pojedinih dijelova sigurnosne infrastrukture
- praćenje aktivnosti radi sprječavanja i otkrivanja neovlaštenog pristupa i radnja na informacijskom sustavu
- kontinuirano revidiranje zaštitnih mjera i kontrola (uključujući neprekidno praćenje novih sigurnosnih trendova te instalaciju programskih ispravaka i nadogradnja).

Budući da je uprava banke, između ostalog, odgovorna i za razvoj poslovne strategije i djelotvorno upravljanje svim rizicima kojima je u svom poslovanju izložena, prije uvođenja usluge e-bankarstva trebala bi o tome donijeti eksplicitnu stratešku odluku.

Banka bi trebala provesti analizu isplativosti koja će biti podloga za donošenje odluke o uvođenju usluga i proizvoda e-bankarstva. Pri provođenju analize isplativosti potrebno je uzeti u obzir procijenjene rizike, troškove primjene zaštitnih mjera i kontrola, vrijeme, tehničku kompetentnost i ostale resurse neophodne za adekvatno upravljanje i nadzor aktivnosti e-bankarstva (primjerice osoblje te hardversku, softversku i komunikacijsku podršku). Prilikom provođenja analize isplativosti uvođenja usluga i proizvoda e-bankarstva, potrebno je uzeti u obzir i sljedeće čimbenike:

- promjene u internim aktima banke i praksama
- utjecaj na funkcionalnost i sigurnost informacijskog sustava
- postizanje i održavanje primjerene mrežne infrastrukture
- postizanje i održavanje kompetentnosti na području sigurnosti, sustava za podršku raspoloživosti sustava kao i sustava za otkrivanje neovlaštenog pristupa i radnja na informacijskom sustavu
- praćenje i nadzor pružatelja usluga i dobavljača.

Na temelju navedenog potrebno je donijeti strategiju e-bankarstva koja bi trebala uzeti u obzir različite čimbenike (primjerice želje i potrebe klijenata, konkurenciju, kompetentnost, troškove uvođenja i održavanja te postojeća financijska sredstva) i biti u skladu s poslovnom strategijom banke.

Zbog specifičnosti rizika povezanih s e-bankarstvom u sklopu upravljanja tim rizicima potrebno je razmotriti sljedeće:

- nadzor i praćenje e-bankarstva
- uspostavljanje kontrola
- sigurnost klijenta.

9.3.1. Nadzor i praćenje e-bankarstva

Djelotvoran sustav nadzora i praćenja e-bankarstva nužan je za efikasno upravljanje i kontrolu nad e-bankarstvom te postizanje poslovnih ciljeva. Praćenje i nadzor e-bankarstva trebali bi obuhvatiti cjelokupni proces e-bankarstva uzimajući u obzir:

- konfiguraciju i sigurnost mreže
- međuovisnosti i veze s postojećim sustavom
- usuglašenost s važećim propisima
- usuglašenost s internim aktima (primjerice s politikom sigurnosti informacijskog sustava)
- zaštitne mjere i kontrole
- aktivnosti pružatelja usluga
- tehničku kompetentnost osoblja
- potrebu za održavanjem kontinuiteta poslovanja
- praćenje neuobičajenih aktivnosti.

Isto tako, banka bi trebala implementirati adekvatan sustav kontinuiranog nadzora u slučaju eksternalizacije (dijela) sustava e-bankarstva kako bi kontrolirala način i kvalitetu pružanja usluga.

9.3.1.1. Planiranje kontinuiteta pružanja usluge e-bankarstva

Banka bi trebala uspostaviti proces planiranja kontinuiteta pružanja usluge e-bankarstva koji bi trebao biti sastavni dio plana kontinuiteta poslovanja banke. Navedeno je potrebno kako bi se smanjio reputacijski, pravni i operativni rizik povezan s neraspoloživošću ili neadekvatnom kvalitetom pružanja usluga e-bankarstva.

U sklopu planiranja kontinuiteta pružanja usluge e-bankarstva banka bi trebala, između ostalog, osigurati sljedeće:

- analizu postojećih kapaciteta informacijskog sustava koji podržavaju e-bankarstvo, uključujući procjenjivanje kapaciteta procesiranja transakcija e-bankarstva
- mogućnost nadogradnje sustava e-bankarstva
- testiranje sustava e-bankarstva pod opterećenjem (s obzirom na očekivani broj korisnika)
- ponovnu uspostavu ili zamjenu e-bankarskih procesnih mogućnosti
- rekonstrukciju transakcija u slučaju potrebe
- procjenu ugovornih odnosa s dobavljačima i pružateljima usluga
- mogućnost korištenja pričuvnoga telekomunikacijskog kanala koji klijentima može pružiti adekvatnu razinu usluge.

Nadalje, pri planiranju kontinuiteta poslovanja banka bi trebala donijeti odgovarajući plan odgovora na incidente kako bi odgovorila na incidente koji nastaju zbog neočekivanih i

neželjenih događaja (kao što su unutarnji i vanjski napadi koji mogu imati negativne posljedice kad je riječ o pružanju usluga e-bankarstva) radi njihova rješavanja ili smanjenja. U slučaju nastanka incidenta, ukoliko su narušena prava određenih klijenata banke, klijente je potrebno o tome obavijestiti.

9.3.1.2. Praćenje neuobičajenih aktivnosti

Dobre prakse nalažu provođenje procjene rizika i razmatranje uvođenja djelotvornog i pravodobnog sustava praćenja neuobičajenih aktivnosti koje se odnose na e-bankarstvo kao što su:

- transakcije e-bankarstva s neaktivnih računa, veći broj transakcija u kraćem razdoblju prema računima s kojima do tada nije bilo transakcija (posebice ako ukupni preneseni iznos novca prelazi granični iznos novca koji podliježe odredbama Zakona o sprječavanju pranja novca, "Narodne novine", br. 69/1997., 106/1997, 67/2001., 114/2001., 117/2003., 142/2003.), transakcije u *offshore* zone i slično
- promjena osobnih podataka klijenata (primjerice adrese klijenta), nakon koje slijede aktivnosti kao što su novi čekovi, nove zaporke, PIN-ovi koji se šalju na tu adresu, povećanje limita, veći iznosi koji se prenose i ostalo. Navedeni slijed aktivnosti upućuje na moguću prijevaru.

Nadalje, u sklopu sustava praćenja neuobičajenih aktivnosti banka bi trebala razmotriti postupke komunikacije s klijentom te izvješćivanja odgovornih osoba i institucija.

9.3.2. Kontrole

Uprava banke je odgovorna za uspostavu adekvatnog sustava kontrola e-bankarstva. Navedeno uključuje uspostavu upravljačkih, logičkih i fizičkih kontrola na svim razinama.

Zbog specifičnosti rizika e-bankarstva posebnu pozornost valja posvetiti sljedećim čimbenicima:

- identifikaciji, autentifikaciji i autorizaciji
- povjerljivosti
- integritetu podataka i transakcija
- raspoloživosti
- razdvajanju dužnosti
- upravljanju operativnim i sistemskim zapisima
- sigurnoj i robusnoj infrastrukturi sustava e-bankarstva
- neporecivosti
- dokazivosti.

Neki od navedenih čimbenika detaljnije su razloženi u nastavku teksta.

9.3.2.1. Identifikacija, autentifikacija i autorizacija

Banka je dužna na temelju procjene rizika, koja obuhvaća i specifičnosti e-bankarstva, donijeti standarde i ostale interne akte te u skladu s tim:

- primijeniti sigurnu i djelotvornu tehnologiju autentifikacije za potvrdu identiteta i ovlasti osoba, procesa i sustava
- primjereno upravljati identifikacijskim i autentifikacijskim oznakama klijenata.

Prilikom procjene rizika potrebno je uzeti u obzir vrstu pojedine transakcije, osjetljivost informacija koje se prenose i pohranjuju te pouzdanost, sigurnost, provjerenost i način primjene pojedine autentifikacijske metode. Autentifikacija klijenata trebala bi biti "jaka" odnosno uključivati najmanje dva od tri načina utvrđivanja neospornosti korisničkog identiteta (detaljnije objašnjeno u poglavlju "Upravljanje kontrolama pristupa").

9.3.2.2. Povjerljivost, integritet i raspoloživost

E-bankarstvo povećava rizik od neovlaštenog pristupa informacijama pri prijenosu javno dostupnom ili privatnom telekomunikacijskom mrežom kao i onda kad su pohranjene u informacijskom sustavu banke. Kako bi se zaštitila povjerljivost informacija, banka bi trebala osigurati barem sljedeće:

- resursi informacijskog sustava trebaju biti dostupni samo ovlaštenim i autentificiranim osobama, procesima i sustavima;
- resursi informacijskog sustava trebaju biti zaštićeni od neovlaštenog otkrivanja ili mijenjanja za vrijeme prijenosa javno dostupnim i privatnim telekomunikacijskim mrežama kao i pri pohranjivanju i čuvanju informacija na sustavima banke;
- adekvatnu kontrolu pristupa pružatelja usluga koji imaju pristup povjerljivim informacijama;
- pristup osjetljivim informacijama ili bilo kakva modifikacija konfiguracije resursa informacijskog sustava (čija posljedica može biti otkrivanje, uništavanje ili mijenjanje informacija) trebali bi se zapisivati u operativne i sistemske zapise.

Neadekvatna zaštita integriteta sustava i podataka može dovesti do netočnosti, prijevara ili pogrešnih odluka, što može biti prvi korak u narušavanju povjerljivosti i raspoloživosti sustava i podataka te smanjiti povjerenje u usluge e-bankarstva općenito. Sve navedeno može rezultirati povećanjem svih rizika kojima je banaka u svom poslovanju izložena. Kako bi očuvala integritet podataka, banka bi trebala implementirati adekvatne zaštitne mjere i kontrole koje bi, uz potrebu očuvanja povjerljivosti, osigurale barem sljedeće:

- e-bankarske transakcije trebaju se provoditi na takav način da budu izrazito otporne na neovlaštene utjecaje tijekom cijelog procesa;
- e-bankarske transakcije te procesi upravljanja podacima trebali bi biti planirani i izvedeni tako da rizik neprimjećivanja neovlaštenih aktivnosti bude sveden na najmanju moguću mjeru;
- adekvatno upravljanje promjenama, uključujući praćenje i testiranje sustava;
- primjenu kriptografskih metoda (primjerice banka bi trebala za prijenos osjetljivih informacija razmotriti uvođenje enkripcije od polazišta do odredišta informacije bez prijelazne dekripcije);
- aplikativne kontrole (primjerice za provjeru usklađenosti iznosa nakon izvršenja transakcija, kao i provjeru integriteta podataka prenesenih između različitih sustava);
- praćenje neuobičajenih aktivnosti.

Isto tako, jedna od važnijih karakteristika e-bankarstva jest raspoloživost usluge. Pojam raspoloživosti odnosi se na svojstvo mogućnosti pristupa i upotrebljivosti na zahtjev

ovlaštenog korisnika usluge e-bankarstva. Kako bi pružila zadovoljavajuću kvalitetu usluge e-bankarstva, banka bi trebala osigurati primjerene kapacitete informacijske i telekomunikacijske infrastrukture te adekvatnu zaštitu od namjernog ili slučajnog uskraćivanja usluge.

Neporecivost i dokazivost moguće je promatrati i kao kombinaciju načela povjerljivosti, integriteta i raspoloživosti. Banka bi trebala koristiti autentifikacijske metode kojima se osigurava neporecivost i dokazivost transakcija e-bankarstva. Rizik poricanja transakcija već je prisutan pri tradicionalnim plaćanjima kreditnim karticama, a e-bankarstvo povećava taj rizik:

- zbog kompleksnosti identificiranja, autentificiranja i autoriziranja osoba, procesa ili sustava koji iniciraju transakciju
- zbog mogućnosti neovlaštene promjene ili "prisvajanja" transakcija
- zbog mogućnosti osporavanja transakcija e-bankarstva od strane korisnika.

S obzirom na sve navedeno banka bi trebala ovisno o vrsti e-bankarske transakcije osigurati barem sljedeće:

- sustavi e-bankarstva trebaju biti projektirani na način kojim se smanjuje vjerojatnost iniciranja nenamjernih transakcija od strane ovlaštenih korisnika;
- korisnici trebaju biti upoznati s rizicima povezanima s transakcijom koju započinju;
- osobe, procesi i sustavi trebaju biti identificirani i autentificirani;
- primjenu odgovarajućih kontrola nad autentificiranim kanalom.

9.3.2.3. Razdvajanje (segregacija) dužnosti

Razdvajanje dužnosti je vrsta upravljačke kontrole kojoj je cilj smanjiti rizik prijevare u poslovnim procesima te osigurati točnost i integritet podataka. Banka bi trebala primijeniti adekvatne kontrole radi djelotvornog razdvajanja dužnosti u procesu e-bankarstva. Uobičajene prakse koje se koriste prilikom razdvajanja dužnosti uključuju sljedeće:

- transakcijski procesi i sustavi trebali bi biti projektirani tako da ni jedan zaposlenik banke ili osoba zaposlena kod pružatelja usluga ne može samostalno započeti, autorizirati i završiti transakciju;
- dužnosti bi trebalo razdvojiti na dužnosti onih (osoba, procesa i sustava) koji iniciraju poslovni proces u sklopu e-bankarstva i onih koji su odgovorni za verifikaciju integriteta tog procesa;
- potrebno je testirati sustav e-bankarstva kako bi se isključila mogućnost zaobilaženja kontrola uvedenih radi razdvajanja dužnosti;
- dužnosti bi trebalo razdvojiti na dužnosti osoblja koje razvija, osoblja koje testira i dužnosti osoblja koje administrira sustav e-bankarstva.

9.3.2.4. Sigurnost aplikacija e-bankarstva

Neprimjerena arhitektura aplikacija e-bankarstva povećava rizik koji proizlazi iz neovlaštenih radnja. Banka bi stoga trebala osigurati primjerenu razinu sigurnosti sustava e-bankarstva adekvatnom arhitekturom aplikacije, imajući u vidu barem sljedeće:

- odabir softverskih alata i tehnologije za razvoj e-bankarskih aplikacija s obzirom na značajke sigurnosti;

- potrebno je provoditi detaljnu i djelotvornu provjeru ispravnosti podataka (dobivenih javno dostupnim telekomunikacijskim mrežama) u nadziranoj i sigurnoj okolini kako bi se smanjio rizik od obrađivanja neispravnih podataka ili neovlaštenog pristupa, radnja i slično;
- informacije koje sustav e-bankarstva uputi na sučelje klijenta ne bi smjele otkrivati osjetljive informacije koje se odnose na arhitekturu aplikacije ili drugih resursa sustava e-bankarstva;
- povjerljive informacije koje se prosljeđuju sa sustava e-bankarstva na sučelje klijenta ili u suprotnom smjeru ne bi se trebale pohranjivati u privremene ili trajne resurse za čuvanje podataka na uređaju klijenta bez njegova izričitog zahtjeva te ne bi smjele biti vidljive neovlaštenim osobama;
- upravljanje aktivnim komunikacijskim kanalom e-bankarstva trebalo bi biti sigurno, što primjerice uključuje i njegovo zatvaranje odnosno prekidanje nakon razdoblja neaktivnosti klijenta.

9.3.2.5. Sigurnosna infrastruktura koja podržava e-bankarstvo

Banka bi trebala uspostaviti adekvatno operativno okruženje koje podržava i štiti sustav e-bankarstva. Navedeno obuhvaća sigurnu infrastrukturu prema javno dostupnim telekomunikacijskim mrežama, adekvatne zaštitne mjere za lokalnu komunikacijsku mrežu i veze prema drugim poslovnim subjektima. Nadalje, banka bi trebala implementirati hardversku i softversku podršku koja će:

- djelotvorno ograničavati radnje koje nisu neophodne
- detaljno nadzirati sve radnje koje su dopuštene i upravljati njima (primjerice primjenom vatrozida i sustava za otkrivanje neovlaštenog pristupa i radnja na informacijskom sustavu).

Potrebno je proaktivno i kontinuirano pratiti i nadzirati infrastrukturu prema javno dostupnim i privatnim telekomunikacijskim mrežama kako bi se smanjio rizik koji proizlazi iz neprimjećivanja povreda sigurnosti, sumnjivih radnja, neovlaštenog pristupa sustavima banke te ostalih prijetnja.

9.3.3. Sigurnost klijenata

Kako bi banka smanjila pravni i reputacijski rizik, potrebno je prije započinjanja transakcije na distribucijskim kanalima osigurati adekvatnu informaciju o identitetu banke (primjerice ime banke i adresu sjedišta banke, opis načina na koji klijenti mogu kontaktirati banku u svezi s problemima, prijedlozima, pritužbama i slično). Isto tako, banka bi trebala osigurati adekvatnu potvrdu svog identiteta i autentičnosti (primjerice upotrebom digitalnog certifikata) kako bi se smanjila mogućnost neovlaštenog predstavljanja u ime banke putem elektroničkih distribucijskih kanala.

Banka ne bi smjela tražiti od klijenata informacije o identifikacijskim i autentifikacijskim oznakama putem komunikacijskih kanala koji ne osiguravaju održavanje temeljnih načela informacijskog sustava. Isto tako, banka bi svoje klijente trebala upoznati s mogućim načinima provjere da li komuniciraju s bankom putem adekvatno osiguranoga službenog elektroničkog kanala distribucije (npr. oznaka sigurne transakcije ili provjera certifikata).

Nadalje, dobre prakse nalažu da je klijente potrebno upoznati s činjenicom da banka poduzima sve potrebne radnje kako bi osigurala adekvatnu zaštitu usluge e-bankarstva.

Kako bi se klijentu pružila odgovarajuća sigurnost i kako bi se kontrolirao proces prijenosa novca kanalima e-bankarstva, dobre prakse nalažu razmatranje sljedećeg:

- definiranja graničnih iznosa transakcija (limita)
- odabira računa koji mogu sudjelovati u transakcijama
- ovlasti klijenta za promjenu parametara transakcija (primjerice graničnog iznosa, računa)
- revidiranja korisničkih ovlasti ovisno o dotadašnjem korištenju usluge e-bankarstva (primjerice izmjena graničnih iznosa transakcija ovisno o razdoblju korištenja usluge, uvjetima korištenja, broju transakcija i slično)
- primjena adekvatne tehnologije identifikacije, autentifikacije i autorizacije s obzirom na tip klijenata, granične iznose i slično.

Prilikom definiranja procesa odobravanja korištenja usluge e-bankarstva, kao i promjene parametara računa klijenta, potrebno je definirati kriterije, načine i postupke:

- podnošenja zahtjeva
- odobravanja korištenja usluge e-bankarstva
- slanja povjerljivih podataka klijentima banke
- promjene osobnih podataka klijenata
- primjene tehnologija autentifikacije i autorizacije za spomenute procese.

10. Zaključci i preporuke

Upravljanje informacijskim sustavom

1. Uprava banke trebala bi odrediti člana uprave koji će biti nadležan za nadzor i kontrolu procesa upravljanja informacijskim sustavom.

2. Uprava banke trebala bi uspostaviti adekvatnu organizacijsku strukturu, odgovarajuće funkcije i odbore te proces upravljanja rizikom informacijskog sustava kako bi se osiguralo primjereno upravljanje informacijskim sustavom.

3. Uprava banke trebala bi delegirati ovlasti u skladu s uspostavljenom organizacijskom i funkcionalnom strukturom.

4. Uprava banke trebala bi donijeti strategiju informacijskog sustava koja mora biti u skladu s poslovnom strategijom banke. Strategiju informacijskog sustava potrebno je razraditi u strateškim i operativnim planovima.

5. Uprava banke trebala bi donijeti interne akte kojima se uređuje upravljanje informacijskim sustavom.

6. Potrebno je definirati kriterije, načine i postupke izvješćivanja uprave banke.

7. Uprava banke trebala bi imenovati voditelja organizacijske jedinice informacijske tehnologije, koji bi trebao biti usmjeren na strateška pitanja, funkcionalnost i djelotvornost informacijskog sustava u cjelini, te bi trebala definirati njegove ovlasti, odgovornosti i djelokrug rada.

8. Uprava banke trebala bi uspostaviti neovisnu funkciju voditelja sigurnosti informacijskog sustava, koji bi trebao biti usmjeren na pitanja sigurnosti informacijskog sustava u cjelini, te bi trebala definirati njegove ovlasti, odgovornosti i djelokrug rada. Voditelj sigurnosti informacijskog sustava ne bi smio istodobno biti angažiran na drugim funkcijama koje mogu stvoriti sukob interesa.

9. Uprava banke trebala bi imenovati odbor za upravljanje informacijskim sustavom ili druge odbore čija je uloga praćenje i nadziranje informacijskog sustava i njegovih aktivnosti te koordinacija inicijativa vezanih uz informacijski sustav, a koje se tiču usklađenosti s poslovnim ciljevima i strateškim planom banke.

10. Banka bi trebala donijeti metodologiju upravljanja projektima kojom bi se definirali kriteriji, načini i postupci upravljanja projektima.

Upravljanje rizikom informacijskog sustava

1. Upravljanje rizikom potrebno je uspostaviti kao kontinuirani proces procjene rizika, poduzimanja radnja za smanjenje rizika na prihvatljivu razinu i održavanja prihvatljive razine rizika.

2. Banka bi trebala donijeti metodologiju upravljanja rizikom informacijskog sustava u kojoj bi se definirali kriteriji, načini i postupci upravljanja rizikom.

3. Uprava banke trebala bi biti pisanim putem obaviještena o najznačajnijim rezultatima procjene rizika.

4. Banka bi trebala odabrati i provesti mjere za smanjivanje rizika na prihvatljivu razinu.

5. Banka bi trebala pri provođenju odabranih mjera uvesti nove i/ili izmijeniti postojeće upravljačke, logičke ili fizičke kontrole. Nakon provođenja odabranih mjera potrebno je utvrditi preostale rizike.

6. Uprava banke trebala bi biti upoznata sa svim identificiranim preostalim rizicima te u skladu s time donijeti odluku o prihvaćanju preostalih rizika ili poduzimanju radnja za daljnje smanjenje rizika.

7. Banka bi trebala klasificirati informacije u različite grupe prema stupnju njihove osjetljivosti s obzirom na moguće posljedice narušavanja temeljnih načela informacijskog sustava.

8. Banka bi trebala donijeti interne akte kojima se definiraju kriteriji, postupci i odgovornosti za provođenje klasifikacije informacija.

9. Banka bi trebala zaštititi informacije na osnovi provedene klasifikacije informacija i procjene rizika.

Unutarnja revizija

1. Unutarnja revizija treba biti organizirana tako da se osigura sustavno obavljanje revizije informacijskog sustava.

2. Banka bi trebala donijeti metodologiju za provođenje unutarnje revizije informacijskog sustava temeljenu na procjeni rizika.

3. Banka treba na temelju godišnjeg programa rada unutarnje revizije donijeti i operativne planove rada za reviziju informacijskog sustava.

4. Banka bi trebala kontinuirano obavljati unutarnju reviziju informacijskog sustava i definirati razdoblje unutar kojeg će obaviti reviziju cjelokupnoga informacijskog sustava.

5. Izvješća o radu unutarnje revizije trebala bi sadržavati i izvješća o obavljenim revizijama informacijskog sustava.

Sigurnost informacijskog sustava

1. Banka bi trebala donijeti politiku sigurnosti informacijskog sustava, upoznati korisnike informacijskog sustava s njom te imenovati osobu odgovornu za kontrolu provođenja te politike.

2. Politika sigurnosti informacijskog sustava trebala bi sadržavati načela upravljanja sigurnošću informacijskih resursa te odgovornosti koje se odnose na sigurnost informacijskog sustava.

3. Na temelju politike sigurnosti informacijskog sustava banka bi trebala donijeti i primijeniti detaljne interne akte koji se odnose na sve aspekte sigurnosti informacijskog sustava.

4. Politiku sigurnosti informacijskog sustava potrebno je usklađivati s promjenama na informacijskom sustavu i u njegovoj okolini, u slučajevima narušavanja sigurnosti informacijskog sustava, te ovisno o rezultatima procjene rizika.

5. Banka bi trebala definirati kriterije na temelju kojih će kontrolirati pristup resursima informacijskog sustava, te u skladu s definiranim kriterijima i procjenom rizika uvesti adekvatne upravljačke, logičke i fizičke kontrole pristupa. Uvedene kontrole pristupa trebale bi biti u skladu sa standardima i pravilima struke.

6. Banka bi trebala uspostaviti sustav upravljanja korisničkim pravima pristupa koji obuhvaća procese evidentiranja, autorizacije, identifikacije i autentifikacije te nadzora.

7. Banka bi trebala posvetiti posebnu pozornost identifikaciji i autentifikaciji korisnika informacijskog sustava.

8. Banka bi trebala posvetiti posebnu pozornost povlaštenom i udaljenom pristupu resursima informacijskog sustava te ostalim pristupima koji, prema procjeni rizika, izlažu banku povećanom riziku.

9. Banka bi trebala u skladu s provedenom procjenom rizika odrediti adekvatne kriptografske metode čijom će se primjenom osigurati održavanje temeljnih načela informacijskog sustava.

10. Banka bi trebala definirati i primijeniti postupke generiranja, pohrane, distribucije, aktiviranja, upotrebe, arhiviranja, zamjene, deaktivacije i uništavanja kriptografskih ključeva.

11. Banka bi trebala, na osnovi provedene procjene rizika, primijeniti odgovarajuće upravljačke, logičke i fizičke kontrole radi fizičke zaštite prostorija s resursima informacijskog sustava, samih resursa, kao i sustava koji su podrška funkcioniranju informacijskog sustava.

12. Banka bi trebala osigurati izradu, praćenje i analizu operativnih i sistemskih zapisa kojima bi se omogućilo rekonstruiranje događaja, otkrivanje neovlaštenih pristupa i

radnja na informacijskom sustavu, identificiranje problema i utvrđivanje odgovornosti.

13. Operativni i sistemski zapisi moraju biti adekvatno zaštićeni od neovlaštenog pristupa, izmjena i brisanja.

14. Banka bi trebala primijeniti odgovarajuće upravljačke, logičke i fizičke kontrole kako bi se resursi informacijskog sustava zaštitili od malicioznog koda. Kontrole je potrebno neprekidno nadzirati i redovito nadopunjavati.

Održavanje informacijskog sustava

1. Banka bi trebala uspostaviti proces upravljanja imovinom informacijskog sustava koji obuhvaća detektiranje, evidentiranje, raspolaganje, praćenje, planiranje, obnavljanje, zaštitu i odlaganje imovine.

2. Banka bi trebala uspostaviti proces upravljanja promjenama hardverskih i softverskih komponenata informacijskog sustava banke koji obuhvaća postupke utvrđivanja početnih inačica softverskih i hardverskih komponenata informacijskog sustava te identifikacije i praćenja svih promjena u vezi s njima.

3. Banka bi trebala uspostaviti proces upravljanja konfiguracijama hardverskih i softverskih komponenata informacijskog sustava koji obuhvaća postupke analize, definiranja, dokumentiranja, testiranja, uvođenja u produkcijski rad, kontrole i praćenja izmjena svih osjetljivih postavka komponenata informacijskog sustava.

4. Banka bi trebala definirati postupke izrade, pohrane, održavanja i čuvanja dokumentacije koja se odnosi na informacijski sustav banke.

5. Dokumentacija bi trebala biti točna, potpuna i ažurna.

6. Banka bi trebala korisnicima informacijskog sustava osigurati pristup dokumentaciji koja je potrebna za obavljanje njihovih poslovnih zadataka.

7. Banka bi trebala osigurati primjerenu izobrazbu svih korisnika informacijskog sustava koja će navedenim osobama omogućiti djelotvorno obavljanje poslovnih zadataka te smanjiti mogućnost pojave neželjenih događaja na prihvatljivu razinu. Izobrazbu bi trebalo uspostaviti kao kontinuirani proces kako bi se osiguralo da znanja korisnika informacijskog sustava prate promjene u informacijskom sustavu i u njegovoj okolini.

Planiranje kontinuiteta poslovanja

1. Banka bi trebala uspostaviti proces planiranja kontinuiteta poslovanja kako bi osigurala postojanost kritičnih i/ili vitalnih poslovnih procesa.

2. Banka bi trebala izraditi i dokumentirati analizu utjecaja na poslovanje koja će odrediti utjecaj neraspoloživosti pojedinih poslovnih procesa odnosno resursa

informacijskog sustava potrebnih za odvijanje tih procesa na poslovanje banke. Analiza utjecaja na poslovanje trebala bi poslužiti kao podloga za planiranje kontinuiteta poslovanja.

3. Banka bi trebala usvojiti plan kontinuiteta poslovanja koji će osigurati ponovnu uspostavu kritičnih i/ili vitalnih poslovnih procesa u zahtijevanom vremenu te ograničiti i smanjiti gubitke koji mogu nastati kao posljedica prekida poslovnih procesa. Plan kontinuiteta poslovanja treba se temeljiti na analizi utjecaja na poslovanje i procjeni rizika.

4. Banka bi trebala usvojiti plan oporavka koji će osigurati raspoloživost resursa informacijskog sustava potrebnih za odvijanje kritičnih i/ili vitalnih poslovnih procesa u zahtijevanom vremenu. Plan oporavka treba se temeljiti na analizi utjecaja na poslovanje i procjeni rizika.

5. Banka bi trebala uspostaviti proces upravljanja incidentima te izraditi plan odgovora na incidente koji treba definirati procedure za postupanje u slučaju incidenata i odrediti osobe zadužene za odgovore na incidente te definirati njihov djelokrug rada, ovlasti i odgovornosti.

6. Banka bi trebala, u slučaju težih incidenata, obavijestiti Hrvatsku narodnu banku o incidentu, njegovim uzrocima, učinku te načinu rješavanja.

7. Banka bi trebala upravljati pričuvnom pohranom na način koji uključuje postupke izrade, pohrane i testiranja pričuvnih kopija te restauracije podataka kako bi se omogućila ponovna uspostava poslovnih procesa i osigurala temeljna načela informacijskog sustava.

8. Banka bi trebala osigurati postojanje ažurnih pričuvnih kopija kao i provjerenih i testiranih metoda restauriranja podataka. Pričuvne kopije trebale bi biti, u skladu s procjenom rizika, pohranjene i na udaljenu sigurnu lokaciju.

9. Banka bi trebala, u skladu s procjenom rizika i analizom utjecaja na poslovanje, osigurati raspoloživost pričuvnoga računalnog centra na udaljenoj lokaciji s odgovarajućom opremljenošću, funkcionalnošću i sigurnošću.

10. Banka bi trebala testirati plan kontinuiteta poslovanja, plan oporavka i plan odgovora na incidente nakon značajnih promjena u poslovnim procesima ili na informacijskom sustavu, a najmanje svakih 18 mjeseci. Potrebno je sastaviti pisana izvješća o rezultatima testiranja.

11. Postupke izrade i pohrane pričuvnih kopija potrebno je periodično, a najmanje jednom godišnje, revidirati, kako bi se osigurala usklađenost navedenih postupaka sa zahtjevima koji proizlaze iz plana kontinuiteta poslovanja i plana oporavka.

12. Postupke restauracije podataka s pričuvnih kopija potrebno je periodično testirati, a najmanje jednom godišnje, kako bi se osigurala usklađenost navedenih postupaka sa zahtjevima koji proizlaze iz plana kontinuiteta poslovanja i plana oporavka. Potrebno je sastaviti pisano izvješće o rezultatima testiranja.

13. Banka bi trebala testirati funkcionalnost i sigurnost pričuvnoga računalnog centra najmanje svakih 18 mjeseci. Potrebno je sastaviti pisano izvješće o rezultatima testiranja.

Razvoj sustava i eksternalizacija

1. Banka bi trebala definirati način, kriterije, postupke i standarde razvoja informacijskih sustava, imajući u vidu funkcionalne i sigurnosne aspekte.

2. Banka bi trebala proces razvoja informacijskog sustava organizirati kroz projekte. Projekte razvoja potrebno je planirati i formalno organizirati.

3. Banka bi trebala projekte razvoja informacijskih sustava planirati i formalno organizirati kao sastavni dio procesa razvoja informacijskih sustava.

4. Banka bi trebala uspostaviti i dokumentirati proces programskog razvoja i isporuke informacijskog sustava koji obuhvaća postupke analize i projektiranja, programiranja, testiranja i uvođenja u produkcijski rad.

5. Banka bi trebala uspostaviti proces upravljanja programskim promjenama informacijskih sustava radi održavanja temeljnih načela informacijskog sustava.

6. Banka bi trebala adekvatno razdvojiti razvojnu, testnu i produkcijsku okolinu.

7. Prije donošenja odluke o eksternalizaciji banka bi trebala utvrditi da li zakonodavstvo odnosno propisi države u kojima pružatelj usluga posluje omogućavaju Hrvatskoj narodnoj banci da ostvari cjelovit i neograničen pristup djelatnostima i poslovima u svezi s kojima Hrvatska narodna banka obavlja nadzor.

8. Izravni nadzor od strane Hrvatske narodne banke u odnosu na pružanje usluga na teritoriju Republike Hrvatske i izvan njega od strane pružatelja usluga rezidenata ili nerezidenata ne smije ni na koji način i ni u kojem trenutku biti onemogućen, ograničen ili otežan.

9. Prije donošenja odluke o eksternalizaciji (dijela) informacijskog sustava banka bi trebala procijeniti rizik eksternalizacije.

10. Banka bi prije sklapanja ugovora s pružateljem usluga trebala provesti dubinsko ispitivanje pružatelja usluga.

11. Banka bi trebala osigurati da odnos između banke i pružatelja usluga bude prihvatljiv sa stajališta rizika i u skladu s poslovnim ciljevima banke.

12. Ugovori između Banke i pružatelja usluga trebaju biti u pisanom obliku, jasno sastavljeni i dovoljno detaljni kako bi osigurali ispunjavanje preuzetih obveza pružanja usluga. Isto tako, ugovori trebaju jasno definirati sve relevantne pojmove, uvjete, prava i obveze te odgovornosti ugovornih strana.

13. Banka bi trebala kontinuirano nadzirati pružanje ugovorenih usluga i upravljati rizikom eksternalizacije, uključujući i primjenu adekvatnih zaštitnih mjera i kontrola kako bi se rizik eksternalizacije smanjio na prihvatljivu razinu.

14. Banka bi trebala svojim internim aktima regulirati sve elemente i postupke vezane uz eksternalizaciju.

15. Banci bi trebao biti osiguran neograničen i svakodoban pristup informacijama koje su predmet eksternalizacije ili su na bilo koji način povezane s eksternalizacijom.

E-bankarstvo

1. Banka bi trebala donijeti strategiju e-bankarstva kao sastavni dio poslovne strategije banke.

2. Banka bi trebala prije donošenja odluke o uvođenju e-bankarstva ili novih usluga procijeniti rizike povezane s e-bankarstvom i tim uslugama.

3. Banka bi trebala osigurati djelotvoran sustav nadzora i praćenja e-bankarstva.

4. Banka bi trebala uspostaviti sigurnosnu infrastrukturu koja će djelotvorno štititi resurse e-bankarstva. Navedeno uključuje i uspostavu slojevitih upravljačkih, logičkih i fizičkih kontrola.

5. Banka bi trebala primijeniti sigurne i učinkovite autentifikacijske metode za potvrdu identiteta i ovlasti osoba, procesa i sustava. Autentifikacija osoba trebala bi biti "jaka" odnosno uključivati najmanje dva načina utvrđivanja neospornosti identiteta.

6. Banka bi trebala zaštititi informacije od neovlaštenog otkrivanja, mijenjanja ili brisanja za vrijeme unosa, obrade, prijenosa preko telekomunikacijskih mreža kao i pri pohrani i čuvanju informacija na sustavima banke i klijenata.

7. Banka bi trebala osigurati adekvatnu potvrdu svog identiteta na distribucijskom kanalu e-bankarstva kako bi klijent mogao provjeriti i potvrditi identitet i izvornost banke.

8. Banka bi trebala osigurati postojanje operativnih i sistemskih zapisa za sve financijske i nefinancijske transakcije e-bankarstva.

9. Banka bi trebala upoznati korisnike e-bankarstva s rizicima korištenja e-bankarstvom.