UPUTSTVO

ZA IZVJEŠTAVANJE O UPRAVLJANJU INFORMACIONIM SISTEMIMA

Sarajevo, decembar / prosinac 2017. godine

Na osnovu člana 5. stav (1) tačka h) i člana 23. stav (1) Zakona Zakona o Agenciji za bankarstvo FBiH („Službene novine Federacije BiH“ br. 75/17) i člana 33. stav (1) Odluke o upravljanju informacionim sistemom u banci („Službene novine Federacije BiH“ br. 81/17), direktor Agencije za bankarstvo Federacije Bosne i Hercegovine dana 22.12.2017. godine donosi

UPUTSTVO
ZA IZVJEŠTAVANJE O UPRAVLJANJU INFORMACIONIM SISTEMIMA

Član 1.
Opće odredbe

Ovim Uputstvom za izvještavanje o upravljanju informacionim sistemima (u daljem tekstu: Uputstvo) se detaljnije propisuje izvještavanje, obrasci, način i metodologija popunjavanja obrazaca, koje banke dostavljaju Agenciji za bankarstvo Federacije Bosne i Hercegovine (u daljem tekstu: Agencija).

Član 2.
Vrste izvještaja

(1) U skladu sa članom 33. Odluke o upravljanju informacionim sistemom u banci (u daljem tekstu: Odluka), banka dostavlja sljedeće izvještaje:
   a) Izvještaj – Opšti podaci o banci i upravljanju informacionim sistemom sa pripadajućim tabelama (3 tabele):
      1) BA 42.01 Opšti podaci (OP),
      2) BA 42.02 Opšti podaci o odgovornim licima (OP1) i
      3) BA 42.03 Fluktuacija kadrova u organizacionoj jedinici nadležnoj za upravljanje informacionim sistemom (OP2)
   b) Izvještaj – Strategija i operativni planovi informacionog sistema: BA 43.00 Strateški i operativni ciljevi (SOP),
   c) Izvještaj – Upravljanje rizicima informacionog sistema: BA 44.00 Plan tretiranja rizika informacionog sistema (RIS),
   d) Izvještaj – Sigurnost informacionog sistema: BA 45.00 Rezultati penetracionih testiranja/testova ranjivosti (SIS),
   e) Izvještaj – Interna revizija sa pripadajućim tabelama (2 tabele):
      1) BA 46.01 Pregled planiranih i provedenih revizija informacionog sistema (ITR) i
      2) BA 46.02 Pregled preporuka (interne revizije, eksterne revizije i Agencije za bankarstvo FBiH) (ITR1)
   f) Izvještaj – Budžet informacionog sistema: BA 47.00 Budžet informacionog sistema (BIS),
   g) Izvještaj – Razvoj informacionog sistema: BA 48.00 Razvoj i održavanje software-a (ROS)
   h) Izvještaj – Značajne promjene u informacionom sistemu banke: BA 49.00 Značajne promjene u informacionom sistemu banke (PIS)
   i) Izvještaj – Upravljanje zapisima iz informacionog sistema banke sa pripadajućim tabelama (4 tabele):
      1) BA 50.01 Pregled upravljanja zapisima iz Aktivnog Direktorija (ZIS1),
      2) BA 50.02 Pregled upravljanja zapisima iz produkcione baze podataka ključne bankarske aplikacije (ZIS2),
      3) BA 50.03 Pregled upravljanja zapisima sa ključnih mrežnih komponenti (ZIS3) i
      4) BA 50.04 Udaljeni pristup prema resursima informacionog sistema (ZIS4)
   j) Izveštaj – Pregled incidenata/zastoja u informacionom sistemu banke sa pripadajućim tabelama (5 tabela):
      1) BA 51.01 Kategorizacija incidenata (PI1),

2) BA 51.02 Broj incidenata/zastoja po poslovnim procesima (PI2),
3) BA 51.03 Broj prema vrstama incidenata (PI3),
4) BA 51.04 Cyber incidenti (PI4) i
5) BA 51.05 Elektronsko bankarstvo i kartično poslovanje – moguće zloupotrebe (PI5)

k) Izvještaj – Upravljanje sistemom elektronskog bankarstva sa pripadajućim tabelama (2 tabele).
1) BA 52.01 Obim elektronskog bankarstva (UEB1) i
2) BA 52.02 Sredstva autentifikacije i autorizacije u sistemu elektronskog bankarstva (UEB2)

l) Izvještaj – Kartično poslovanje sa pripadajućim tabelama (2 tabele):
1) BA 53.01 Obim kartičnog poslovanja (KP1) i
2) BA 53.02 Broj POS i ATM uređaja (KP2)

m) Izvještaj – Plan oporavka informacionog sistema sa pripadajućim tabelama (4 tabele):
1) BA 54.01 Načini testiranja (POIS1),
2) BA 54.02 Scenariji za testiranje (POIS2),
3) BA 54.03 Testirani poslovni procesi (POIS3) i
4) BA 54.04 Ostali podaci o oporavku informacionog sistema (POIS4).

(2) Izvještaji iz stava (1) ovog člana su dati u Prilogu ovog Uputstva i čine njegov sastavni dio.

Član 3.

Izvještaj Opšti podaci o banci i upravljanju informacionim sistemom

(1) Izvještaj Opšti podaci o banci i upravljanju informacionim sistemom sadrži podatke o banci, organizacionom dijelu zaduženom za upravljanje informacionim sistemom u banci, organizacionom dijelu zaduženom za sigurnost informacionog sistema, kao i internoj reviziji informacionog sistema banke.

(2) Izvještaj se sastoji od tri tabele:
a) BA 42.01 Opšti podaci (OP),
b) BA 42.02 Opšti podaci o odgovornim licima (OP1) i
c) BA 42.03 Fluktuacija kadrova u organizacionoj jedinici nadležnoj za upravljanje informacionim sistemom (OP2).

(3) Tabela BA 42.01 Opšti podaci (OP) sadrži osnovne podatke o ukupnom broju zaposlenih u organizacionoj jedinici za upravljanje informacionim sistemom, kao i o nazivima organizacione jedinice nadležne za upravljanje informacionim sistemom i organizacione jedinice nadležne za sigurnost informacionog sistema.

(4) Tabela BA 42.02 Opšti podaci o odgovornim licima (OP1) sadrži podatke o odgovornim licima. Potrebno je popuniti odgovarajuće podatke (ime i prezime, naziv radnog mjesta, stručna sprema i datum početka obavljanja funkcije) o članu Uprave nadležnom za upravljanje informacionim sistemom, Rukovodiocu organizacione jedinice nadležne za upravljanje informacionim sistemom, Licu odgovornom za sigurnost informacionog sistema i Licu koje obavlja internu reviziju informacionog sistema. Ukoliko se funkcija internog revizora informacionog sistema eksternalizuje prema vanjskom pružaocu usluga, u kolonu Ime i prezime je potrebno navesti naziv pružaoca usluga sa kojim Banka ima zaključen ugovorni odnos.

(5) Tabela BA 42.03 Fluktuacija kadrova u organizacionoj jedinici nadležnoj za upravljanje informacionim sistemom (OP2) sadrži podatke (ime i prezime, naziv radnog mjesta, stručna sprema i datum promjene) o zaposlenicima koji su zasnovali odnosno prekinuli radni odnos u organizacionoj jedinici nadležnoj za upravljanje informacionim sistemom u toku izvještajne kalendarske godine.

Član 4.

Izvještaj Strategija i operativni planovi informacionog sistema

(1) Izvještaj Strategija i operativni planovi informacionog sistema sadrži podatke o povezanosti strategije informacionog sistema i strategije banke, te realizaciju strategije kroz operativne planove informacionog sistema.
   a) Izvještaj se sastoji od jedne tabele: BA 43.00 Strateški i operativni ciljevi (SOP).

(2) Tabela 43.00 Strateški i operativni ciljevi (SOP) sadrži osnovne podatke o Strategiji informacionog sistema i Operativnim planovima odnosno projektima/aktivnostima organizacione jedinice nadležne za upravljanje informacionim sistemom u banci.

(3) Kolona I (strateški cilj banke) treba da sadrži ciljeve iz strategije banke, koji su navedeni u okviru usvojene Strategije banke. Kolona II (strateški cilj informacionog sistema) sadrži ciljeve informacionog sistema koji su navedeni u okviru usvojene Strategije informacionog sistema, a koji su povezani sa strateškim ciljevima banke. Kolona III (Operativni plan – projekat/aktivnost) sadrži projekte/aktivnosti navedene u okviru Operativnih planova, a koji proizilaze iz Strategije informacionog sistema. Kolona IV (status) treba da sadrži status projekta/aktivnosti iz Operativnog plana na dan slanja izvještaja. Kolona V (trajanje projekta/aktivnosti) se sastoji od dvije podkolone (početak projekta/aktivnosti i kraj projekta/aktivnosti), a koji predstavljaju planirani period izvršenja projekta/aktivnosti iz Operativnog plana.

(4) Pored gore navedenog, Banka je dužna dostavljati kopije Izvještaja Odbora za upravljanje informacionim sistemom, definisane članom 5. stav (1) tačka a) Odluke.

Član 5.

Izvještaj Upravljanje rizicima informacionog sistema

(1) Izvještaj Upravljanje rizicima informacionog sistema sadrži sažetak godišnje procjene rizika informacionog sistema banke.

(2) Izvještaj se sastoji od jedne tabele:
   a) BA 44.00 Plan tretiranja rizika informacionog sistema (RIS).

(3) Tabela BA 44.00 Plan tretiranja rizika informacionog sistema (RIS) predstavlja pregled ključnih rizika informacionog sistema, razvrstanih u pet kategorija: rizik dostupnosti i kontinuiteta, rizik sigurnosti, rizik upravljanja izmjenama, rizik integriteta podataka i rizik eksternalizacije.

(4) Kolona I (kategorija rizika) predstavlja kategoriju rizika, kolona II (rizik) predstavlja naziv rizika, dok kolona III (opis rizika) predstavlja detaljniji opis rizika. Kolona IV (nivo rizika) predstavlja ocijenjeni nivo rizika sa ocjenama od 1 do 4, pri čemu ocjena 1 predstavlja najniži nivo rizika, dok ocjena 4 predstavlja najviši nivo rizika. Ukoliko se bančina ocjena nivoa rizika prema internim metodologijama razlikuje od prethodno navedene, potrebno je da banka izvrši adekvatno mapiranje i transformaciju ocjena prema internim metodologijama u prethodno navedene ocjene od 1 do 4. Kolona V (način tretiranja rizika) predstavlja način tretiranja rizika od strane banke (naprimjer, prihvaćen, umanjen, izbjegnut i slično), dok kolona VI (opis mjere) predstavlja kratki opis poduzetih mjera za umanjenje rizika. Kolona VII (planirani period implementacije mjere) predstavlja planirani vremenski period implementacije mjere (kvartal), dok kolona VIII (status) predstavlja status implementacije mjere (naprimjer, završen, u toku i slično) na dan slanja izvještaja.

(5) Navedena tabela sadrži samo ključne rizike koje je banka obavezna analizirati. Banka je dužna, u skladu sa svojom analizom i procjenom rizika, dodati i ostale prepoznate rizike informacionog sistema specifične za informacioni sistem banke.

(6) Pored gore navedenog, Banka je dužna dostavljati:
   a) Metodologiju upravljanja rizicima informacionog sistema, definisanu članom 11. stav (2) Odluke i

b) kopije Izvještaja o upravljanju rizicima informacionih sistema, definisane članom 11. stav (3) tačka d) Odluke.

Član 6.
Izvještaj Sigurnost informacionog sistema

(1) Izvještaj Sigurnost informacionog sistema sadrži informacije vezane uz rezultate penetracionih testiranja/testiranja ranjivosti.
(2) Izvještaj se sastoji od jedne tabele:
   a) BA 45.00 Rezultati penetracionih testiranja/testova ranjivosti (SIS).
(3) Tabela BA 45.00 Rezultati penetracionih testiranja/testova ranjivosti (SIS) predstavlja pregled rizika identifikovanih penetracionim testiranjem/testom ranjivosti.
(4) Kolona I (naziv izvještaja) sadrži podatak o nazivu izvještaja u okviru kojeg su navedeni rizici. Kolona II (rizik) definiše slabost, ranjivost odnosno rizik otkriven tokom testiranja. Kolona III (nivo rizika) predstavlja ocijenjeni nivo rizika sa ocjenama od 1 do 4, pri čemu ocjena 1 predstavlja najniži nivo rizika, dok ocjena 4 predstavlja najviši nivo rizika. Ukoliko se bančina ocjena nivoa rizika prema internim metodologijama razlikuje od prethodno navedene, potrebno je da banka izvrši adekvatno mapiranje i transformaciju ocjena prema internim metodologijama u prethodno navedene ocjene od 1 do 4. Kolona IV (prijedlog načina tretiranja rizika) predstavlja način tretiranja rizika od strane banke (naprimjer, umanjenje, prihvatanje, izbjegavanje i slično). Kolona V (opis) predstavlja opis tretiranja rizika odnosno mjere koje će banka poduzeti na umanjenju rizika. Kolona VI (planirani period izvršenja) predstavlja definisani rok za otklanjanje uočenog rizika (po kvartalima), dok kolona VII (aktuelni završetak aktivnosti) predstavlja aktuelni rok završetka implementacije mjere za umanjenje na dan slanja izvještaja.
(5) Tabela BA 45.00 se popunjava za sva obavljena penetraciona testiranja/testove ranjivosti pojedinačno, bilo da su isti provedeni od strane vanjskog angažovanog pružaoca usluga ili od strane internog tima banke. Za svako obavljeno penetraciono testiranje/test ranjivosti potrebno je popuniti posebnu tabelu.
(6) Tabelu BA 45.00 je potrebno dostavljati Agenciji za sve penetracione testove dok se sve otkrivene slabosti odnosno rizici ne otklone odnosno dok se ne postupi u skladu sa usvojenom odlukom o tretiranju rizika.
(7) Pored gore navedenog, Banka je dužna dostavljati:
   a) kopije Izvještaja o stanju i aktivnostima vezanim uz sigurnost informacionog sistema, definisan članom 12. stav (2) Odluke i
   b) kopije Izvještaja penetracionog testiranja/testiranja ranjivosti definisane članom 8. Odluke.

Član 7.
Izvještaj Interna revizija

(1) Izvještaj Interna revizija sadrži sadrži podatke o planiranim, obavljenim revizijama i praćenju nalaza od strane interne revizije informacionog sistema banke.
(2) Izvještaj se sastoji od dvije tabele:
   a) BA 46.01 Pregled planiranih i provedenih revizija informacionog sistema (ITR) i
   b) BA 46.02 Pregled preporuka (interne revizije, eksterne revizije i Agencije za bankarstvo FBiH) (ITR1).
(3) Tabela BA 46.01 Pregled planiranih i provedenih revizija informacionog sistema (ITR) sadrži podatke o planiranim i provedenim revizijama informacionog sistema.
(4) Kolona I (oblast informacionog sistema po regulativi) navodi oblasti revizije informacionog sistema kojoj oblast pripada u skladu sa važećom regulativom. Kolona II (oblast revizije informacionog sistema po metodologiji banke) sadrži sve definisane oblasti revizije informacionog sistema u skladu sa metodologijom za obavljanje revizije informacionog sistema banke, a koje korespondiraju definisanim oblastima po regulativi. Kolona III

(jedinstvena oznaka predmetne revizije) predstavlja jedinstvenu identifikaciju revizije. Kolona IV (revizijski ciklus) predstavlja definisani revizijski ciklus za datu oblast u skladu sa procjenom rizika (da li se revizija navedene oblasti obavlja svake godine, jednom u dvije ili jednom u tri godine). Kolona V (oblast uključena u period za koji se dostavlja izvještaj DA/NE) predstavlja oznaku da li je definisana oblast sadržana u planu revizije za godinu u kojoj se dostavlja izvještaj. Kolona VI (detaljniji opis predmeta, cilja i opsega revizije) predstavlja detaljniji opis, ciljeve i opseg revizije. Kolona VII (trajanje revizije) se sastoji od dvije podkolone u kojima je naveden period provođenja revizije odnosno početak i kraj revizijskih aktivnosti. Kolona VIII (ocjena oblasti) predstavlja ocjenu navedene oblasti od strane internog revizora informacionog sistema, u skladu sa vlastitom metodologijom interne revizije informacionog sistema banke.

(5) Tabela BA 46.02 Pregled preporuka (interne revizije, eksterne revizije i Agencije za bankarstvo FBiH) (ITR1) sadrži podatke o svim uočenim nedostacima odnosno izdatim preporukama u okviru određenih izvještaja revizije informacionog sistema zajedno sa pratećim mjerama za korekciju, rokovima za implementaciju mjera i stepenom realizacije.

(6) Kolona I (jedinstvena oznaka predmetne revizije) predstavlja jedinstvenu identifikaciju predmetne revizije. Kolona II (uočeni nedostaci) sadrži uočene nedostatke, slabosti i/ili rizike u provedenoj reviziji. Kolona III (nivo rizika) predstavlja ocijenjeni nivo rizika sa ocjenama od 1 do 4, pri čemu ocjena 1 predstavlja najniži nivo rizika, dok ocjena 4 predstavlja najviši nivo rizika. Ukoliko se bančina ocjena nivoa rizika prema internim metodologijama razlikuje od prethodno navedene, potrebno je da banka izvrši adekvatno mapiranje i transformaciju ocjena prema internim metodologijama u prethodno navedene ocjene od 1 do 4. Kolona IV (mjere za korekciju) sadrži preporučene mjere za otklanjanje odnosno umanjenje uočenih rizika. Kolona V (rok za implementaciju mjere) predstavlja definisani rok za otklanjanje rizika. Kolona VI (praćenje izvršenja mjere (follow-up) – opis) sadrži podatke o provedenom praćenju izvršenja naložene mjere. Kolona VII (status izvršenja mjere) sadrži status izvršenja mjere na dan slanja izvještaja.

(7) Tabela BA 46.02 treba da sadrži podatke o praćenju izvršenja naloženih mjera od strane interne revizije informacionog sistema banke, eksterne revizije informacionog sistema, odnosno izdatih naloga Agencije za bankarstvo FBiH koji se odnose na kontrolu informacionog sistema banke.

(8) Tabele BA 46.01 i BA 46.02 je potrebno popuniti bez obzira da li se interna revizija informacionog sistema obavlja od strane internog revizora informacionog sistema banke, grupe ili eksternalizovanog internog revizora informacionog sistema.

Član 8.
Izvještaj Budžet informacionog sistema

(1) Izvještaj Budžet informacionog sistema sadrži sadrži podatke o ukupnom budžetu banke, kao i o planiranim i realizovanim budžetima za definisana područja informacionog sistema.

(2) Izvještaj se sastoji od jedne tabele:
   a) BA 47.00 Budžet informacionog sistema (BIS).

(3) Tabela BA 47.00 sadrži podatke o planiranom i realizovanom budžetu banke (u 000 KM), zatim ukupnom budžetu za definisana područja informacionog sistema, uključujući troškove i investicije koje se odnose na IT, za kalendarsku godinu sa stanjem na dan slanja izvještaja.

Član 9.
Izvještaj Razvoj informacionog sistema

(1) Izvještaj Razvoj informacionog sistema sadrži podatke o razvoju i održavanju aplikacija koje se koriste u okviru informacionog sistema banke.

(2) Izvještaj se sastoji od jedne tabele:
   a) BA 48.00 Razvoj i održavanje software-a (ROS).

(3) Tabela BA 48.00 Razvoj i održavanje software-a (ROS) sadrži opšte podatke o načinu održavanja aplikacija koje se koriste u okviru informacionog sistema banke (interno ili od strane vanjskog pružaoca usluga).
(4) U slučaju da banka određenu aplikaciju ili sistem razvija odnosno održava interno, potrebno je u koloni II (Interno) odabrati odgovor DA, dok je u slučaju angažovanja pružaoca usluga potrebno u koloni II (Interno) odabrati odgovor Ne, te u koloni III (Eksterno-naziv pružaoca usluga) navesti naziv pružaoca usluga. Ukoliko se za pojedinačnu aplikaciju ili sistem pojavljuje više pružaoca usluga, potrebno ih je sve navesti i pojasniti predmetni razvoj/ održavanje.
(5) U tabeli su navedene određene aplikacije i sistemi koji se najčešće koriste u banci. Ukoliko banka posjeduje i druge značajne aplikacije ili sisteme, potrebno je dopuniti listu i osigurati neophodne podatke u zavisnosti od specifičnosti informacionog sistema banke.

Član 10.
Izvještaj Značajne promjene u informacionom sistemu banke

(1) Izvještaj Značajne promjene u informacionom sistemu banke sadrži podatke o značajnim izmjenama informacionog sistema banke.
(2) Izvještaj se sastoji od jedne tabele:
   a) BA 49.00 Značajne promjene u informacionom sistemu banke (PIS).
(3) Tabela BA 49.00 Značajne promjene u informacionom sistemu banke (PIS) sadrži podatke o značajnim promjenama u okviru informacionog sistema banke (naprimjer, aplikacije, hardware, mreža i drugo), bez obzira da li su iste planirane ili ne.
(4) Kolona I (dio informacionog sistema) sadrži podatke o nazivu dijela informacionog sistema na koji se odnosi izmjena (naprimjer, ključna bankarska aplikacija, elektronsko bankarstvo, operativni sistem, aplikacije za podršku, hardware, mreža i slično). Kolona II (opis izmjene) sadrži kratki opis izmjene. Kolona III (hitnost izmjene) sadrži podatak da li je izmjena bila hitna ili planirana. Kolona IV (status) sadrži podatak o statusu izmjene odnosno da li je izmjena završena, u toku ili u pripremi odnosno da li je otkazana.
(5) Tabela BA 49.00 treba da obuhvati i hitne izmjene u informacionom sistemu, prouzrokovane uočenim incidentima, problemima u radu i greškama u radu aplikacija.

Član 11.
Izvještaj Upravljanje zapisima iz informacionog sistema banke

(1) Izvještaj Upravljanje zapisima iz informacionog sistema banke sadrži podatke o načinu upravljanja operativnim i sistemskim zapisima iz informacionog sistema banke.
(2) Izvještaj se sastoji od četiri tabele:
   a) BA 50.01 Pregled upravljanja zapisima iz Aktivnog Direktorija (ZIS1),
   b) BA 50.02 Pregled upravljanja zapisima iz produkcione baze podataka ključne bankarske aplikacije (ZIS2),
   c) BA 50.03 Pregled upravljanja zapisima sa ključnih mrežnih komponenti (ZIS3) i
   d) BA 50.04 Udaljeni pristup prema resursima informacionog sistema (ZIS4).
(3) Tabela BA 50.01 Pregled upravljanja zapisima iz Aktivnog Direktorija (ZIS1) sadrži pregled osnovnih zapisa o aktivnostima na Aktivnom Direktoriju.
(4) U koloni I (predmet zapisa) je dat naziv vrste aktivnosti koja se prati. U koloni II (vrste zapisa) je data lista sa izborom (uepješni, neuspješni, uspješni i neuspješni, nije konfigurisano) aktivnosti koja se bilježi, te je potrebno odabrati način konfiguracije koji je banka implementirala. Kolona III (učestalost pregleda/analize) označava period učestalosti pregleda nastalih zapisa (na primjer, dnevno, sedmično, mjesečno, polugodišnje, po potrebi nakon incidenta ili drugo). Kolona IV (datum zadnje analize) označava datum kada je zadnji put pregledan i analiziran zapis.

(5) Tabela BA 50.02 Pregled upravljanja zapisima iz produkcione baze podataka ključne bankarske aplikacije (ZIS2) sadrži pregled osnovnih zapisa o aktivnostima na bazi podataka. Ukoliko se ključna bankarska aplikacija nalazi na više od jedne baze podataka, tabelu je potrebno popuniti za svaku bazu podataka odvojeno.
(6) U koloni I (predmet zapisa) je dat naziv vrste aktivnosti koja se prati. U koloni II (praćenje aktivnosti) je potrebno naznačiti da li banka prati navedene aktivnosti ili ne. Kolona III (učestalost pregleda/analize) označava vremenski period učestalosti pregleda nastalih zapisa (na primjer, dnevno, sedmično, mjesečno, polugodišnje, po potrebi nakon incidenta ili drugo). Kolona IV (datum zadnje analize) označava datum kada je zadnji put pregledan i analiziran zapis.
(7) Tabela BA 50.03 Pregled upravljanja zapisima sa ključnih mrežnih komponenti (ZIS3) sadrži pregled aktivnosti nad aktivnim mrežnim uređajima, a koji se odnose na aktivnosti izmjene konfiguracija i neuspješnih prijava na navedene uređaje.
(8) U koloni I (predmet aktivnosti) je dat naziv aktivnosti koje se evidentiraju u okviru zapisa. U koloni II (praćenje aktivnosti – DA/NE) je potrebno navesti oznaku DA ili NE u zavisnosti da li se aktivnosti iz kolone I prate ili ne. U koloni III (učestalost pregleda/analize) je potrebno navesti vremenski period u okviru kojeg se pregledaju navedeni zapisi. Kolona IV (datum zadnje analize) označava datum kada je zadnji put pregledan i analiziran zapis.
(9) Tabela BA 50.04 Udaljeni pristup prema resursima informacionog sistema (ZIS4) sadrži pregled ostvarenih udaljenih pristupa prema informacionom sistemu banke.
(10) U koloni I (korisnik koji je ostvario pristup) je potrebno navesti ime i prezime uposlenika banke odnosno ime i prezime uposlenika – pružaoca usluga koji je ostvario udaljeni pristup. U koloni II (resurs kojem je pristupio) navodi se IT resurs prema kojem je ostvaren udaljeni pristup. U koloni III (broj pristupa) je potrebno naznačiti broj realizovanih udaljenih pristupa od strane korisnika za vremenski period za koji se izvještava.
(11) Tabele BA 50.01 Pregled upravljanja zapisima iz Aktivnog Direktorija (ZIS1), BA 50.02 Pregled upravljanja zapisima iz produkcione baze podataka ključne bankarske aplikacije (ZIS2) i BA 50.03 Pregled upravljanja zapisima sa ključnih mrežnih komponenti (ZIS3) je potrebno popuniti zasebno za sve ključne resurse informacionog sistema, te je potrebno navesti naziv resursa i opis funkcije.

Član 12.
Izvještaj Pregled incidenata/zastoja u informacionom sistemu banke

(1) Izvještaj Pregled incidenata/zastoja u informacionom sistemu banke sadrži pregled incidenata i zastoja u radu informacionog sistema u banci.
(2) Izvještaj se sastoji od pet tabela:
   a) BA 51.01 Kategorizacija incidenata (PI1),
   b) BA 51.02 Broj incidenata/zastoja po poslovnim procesima (PI2),
   c) BA 51.03 Broj prema vrstama incidenata (PI3),
   d) BA 51.04 Cyber incidenti (PI4) i
   e) BA 51.05 Elektronsko bankarstvo i kartično poslovanje – moguće zloupotrebe (PI5).
(3) Tabela BA 51.01 Kategorizacija incidenata (PI1) definiše nivoe incidenata od I-IV, pri čemu kategorija I označava najviši stepen incidenta, dok kategorija IV predstavlja najniži stepen incidenta. Ukoliko se bančina kategorizacija incidenata prema internim metodologijama razlikuje od prethodno navedene, potrebno je da banka izvrši adekvatno mapiranje i transformaciju ocjena prema internim metodologijama u prethodno navedene ocjene od 1 do 5.
(4) BA 51.02 Broj incidenata/zastoja po poslovnim procesima (PI2) sadrži pregled incidenata po definisanim poslovnim procesima.
(5) U koloni I (poslovni proces) su navedeni određeni poslovni procesi u banci. Kolone II – V sadrže broj incidenata prema usvojenoj kategorizaciji. Kolona VI (broj problema/zastoja koji nisu kategorisani kao incidenti) sadrži broj zastoja koji nisu procijenjeni kao incidenti u banci.

Kolona VII (ukupno vrijeme prekida/zastoja rada – trajanje u minutama) sadrži ukupno vrijeme zastoja za sve navedene incidente i zastoje. U kolonu VIII (način rješavanja – interno ili eksterno) se unosi podatak da li je predmetni incident riješen od strane IT uposlenika banke ili pružaoca usluga (ukoliko je incident riješen od strane pružaoca usluga, potrebno je navesti naziv pružaoca usluga). Kolona IX (napomena/opis) sadrži opis odnosno napomenu za predmetni incident odnosno zastoj.

(6) Tabela BA 51.03 Broj prema vrstama incidenata (PI3) sadrži broj incidenata prema definisanim vrstama incidenata.

(7) Tabela BA 51.04 Cyber incidenti (PI4) sadrži broj cyber incidenata prema definisanim vrstama incidenata.

(8) Tabela BA 51.05 Elektronsko bankarstvo i kartično poslovanje – moguće zloupotrebe (PI5) sadrži incidente koji se odnose na moguće zloupotrebe sistema elektronskog bankarstva i kartičnog poslovanja. U koloni I (vrste događaja) su navedeni događaji koje je potrebno evidentirati i pratiti. U kolonu II (broj transakcija u elektronskom bankarstvu) se unosi ukupan broj transakcija u domaćem i inostranom platnom prometu za period za koji se dostavlja izvještaj. U kolonu III (iznos u KM) se unosi ukupan iznos (u 000 KM) protuvrijednosti za domaći i inostrani platni promet prema vrstama događaja. U kolonu IV (broj transakcija u kartičnom poslovanju) se unosi ukupan broj transakcija za period za koji se dostavlja izvještaj. U kolonu V (iznos u KM) se unosi ukupan iznos (u 000 KM) protuvrijednosti za domaći i inostrani platni promet prema vrstama događaja.

(9) Pored gore navedenog, Banka je dužna dostavljati kopije Izvještaja o incidentima i analizi incidenata, definisane članom 25. st. (1) i (3) Odluke.

Član 13.

Izvještaj Upravljanje sistemom elektronskog bankarstva

(1) Izvještaj Upravljanje sistemom elektronskog bankarstva sadrži podatke o obimu elektronskog i mobilnog bankarstva u banci, kao i podatke o načinima autentifikacije.

(2) Izvještaj se sastoji od dvije tabele:
   a) BA 52.01 Obim elektronskog bankarstva (UEB1) i
   b) BA 52.02 Sredstva autentifikacije i autorizacije u sistemu elektronskog bankarstva (UEB2).

(3) Tabela BA 52.01 Obim elektronskog bankarstva (UEB1) sadrži podatke o obimu (broju i iznosu transakcija) elektronskog bankarstva (odvojeno za elektronsko i mobilno bankarstvo), za fizička i pravna lica, u odnosu na ukupan broj i iznos transakcija banke u UPP i IPP prometu.

(4) U koloni I su navedene vrste prometa prema kojima je potrebno izvještavati Agenciju, kao i učešće prometa elektronskog i mobilnog bankarstva u ukupnom platnom prometu na nivou banke.

(5) U kolonu II (broj klijenata) se unosi broj klijenata na dan izvještavanja za pravna lica. Kolona III (Realizovane transakcije UPP) se sastoji od dvije podkolone: Realizovane transakcije UPP – broj koja sadrži podatak o broju transakcija za pravna lica u domaćem platnom prometu za period kalendarske godine za koju se izvještava i Realizovane transakcije UPP – iznos u 000 KM koja sadrži podatak o realizovanim transakcijama za pravna lica u domaćem platnom prometu za period kalendarske godine za koju se izvještava. Kolona IV (Realizovane transakcije IPP) se sastoji od dvije podkolone: Realizovane transakcije IPP – broj koja sadrži podatak o broju transakcija za pravna lica u ino platnom prometu za period kalendarske godine za koju se izvještava i Realizovane transakcije IPP – iznos u 000 KM koja sadrži podatak o realizovanim transakcijama za pravna lica u ino platnom prometu za period kalendarske godine za koju se izvještava.

(6) U kolonu V (broj klijenata) se unosi broj klijenata na dan izvještavanja za fizička lica. Kolona VI (Realizovane transakcije UPP) se sastoji od dvije podkolone: Realizovane transakcije UPP – broj koja sadrži podatak o broju transakcija za fizička lica u domaćem platnom prometu za period kalendarske godine za koju se izvještava i Realizovane transakcije UPP – iznos u 000

KM koja sadrži podatak o realizovanim transakcijama za fizička lica u domaćem platnom prometu za period kalendarske godine za koju se izvještava. Kolona VII (Realizovane transakcije IPP) se sastoji od dvije podkolone: Realizovane transakcije IPP – broj koja sadrži podatak o broju transakcija za fizička lica u ino platnom prometu za period kalendarske godine za koju se izvještava i Realizovane transakcije IPP – iznos u 000 KM koja sadrži podatak o realizovanim transakcijama za fizička lica u ino platnom prometu za period kalendarske godine za koju se izvještava.

(7) BA 52.02 Sredstva autentifikacije i autorizacije u sistemu elektronskog bankarstva (UEB2) sadrže podatke o načinima autentifikacije i autorizacije koje banka koristi u sistemu elektronskog odnosno mobilnog bankarstva, za fizička i pravna lica.

(8) U kolonu I (naziv sistema) se unosi podatak o nazivu sistema elektronskog ili mobilnog bankarstva koje banka pruža svojim klijentima. U kolonu II (naziv pružaoca usluga u slučaju eksternalizacije) se unosi naziv pružaoca usluga sistema elektronskog ili mobilnog bankarstva. Kolona III (vrsta elektronskog bankarstva) sadrži podatak o vrsti elektronskog bankarstva (naprimjer, elektronsko bankarstvo za fizička lica, elektronsko bankarstvo za pravna lica, mobilno bankarstvo za fizička lica i slično). Kolona IV (način autentifikacije) se sastoji od dvije podkolone: Elementi autentifikacije koji sadrži predefinisane elemente autentifikacije (naprimjer, pametna kartica + PIN, USB certifikat + PIN, jednokratna lozinka OTP i slično), zatim Broj klijenata (fizička i pravna lica) u koje je potrebno unijeti podatak o broju fizičkih odnosno pravnih lica na dan izvještavanja.

Član 14.
Izvještaj Kartično poslovanje

(1) Izvještaj Kartično poslovanje sadrži podatke o obimu kartičnog poslovanja u banci i broju aktivnih POS i ATM uređaja.

(2) Izvještaj se sastoji od dvije tabele:
   a) BA 53.01 Obim kartičnog poslovanja (KP1) i
   b) BA 53.02 Broj POS i ATM uređaja (KP2).

(3) Tabela BA 53.01 Obim kartičnog poslovanja (KP1) sadrži podatke o obimu (broju i iznosu transakcija) kartičnog poslovanja za fizička i pravna lica.

(4) U koloni I (vrsta kartice) su navedene kartice koje se najčešće koriste. Kolona II (pravna lica) se sastoji od dvije podkolone: Broj kartica koja sadrži podatak o broju kartica za pravna lica na dan izvještavanja i Iznos transakcija koja sadrži podatak o ukupnom iznosu transakcija za pravna lica za period kalendarske godine za koju se izvještava. Kolona III (fizička lica) se sastoji od dvije podkolone: Broj kartica koja sadrži podatak o broju kartica za fizička lica na dan izvještavanja i Iznos transakcija koja sadrži podatak o ukupnom iznosu transakcija za fizička lica za period kalendarske godine za koju se izvještava.

(5) Tabela BA 53.02 Broj POS i ATM uređaja (KP2) sadrži podatke o broju POS i ATM uređaja u banci i izvan banke.

(6) U koloni I (vrsta uređaja) su navedene vrste uređaja za koju se izvještava. U kolonu II (broj uređaja u banci) se unosi podatak o broju uređaja u banci na dan izvještavanja, dok se u kolonu III (broj uređaja izvan banke) unosi podatak o broju uređaja izvan banke na dan izvještavanja.

Član 15.
Izvještaj Plan oporavka informacionog sistema

(1) Izvještaj Plan oporavka informacionog sistema sadrži podatke o načinima i scenarijima testiranja funkcionalnosti rezervnog informatičkog centra, kao i testiranim poslovnim procesima.

(2) Izvještaj se sastoji od četiri tabele:
   a) BA 54.01 Načini testiranja (POIS1),
   b) BA 54.02 Scenariji za testiranje (POIS2),

c) BA 54.03 Testirani poslovni procesi (POIS3) i
d) BA 54.04 Ostali podaci o oporavku informacionog sistema (POIS4).

(3) Tabela BA 54.01 Načini testiranja (POIS1) sadrži podatke o načinima testiranja, uključenosti centrale banke u testiranje, kao i o broju uključenih poslovnih jedinica.

(4) U koloni I (poslovni procesi) su navedeni poslovni procesi za koje je potrebno dati više podataka u vezi načina testiranja poslovnih procesa. U kolonu III (proces testiran) je potrebno unijeti podatak da li je navedeni proces testiran ili ne, dok je u kolonu IV (uključenost centrale banke u testiranje) potrebno unijeti podatak da li je centrala banke bila uključena u testiranje ili ne. Kolona V (broj uključenih poslovnih jedinica) sadrži podatak o broju uključenih poslovnih jedinica u predmetno testiranje.

(5) Tabela BA 54.02 Scenariji za testiranje (POIS2) sadrži podatke o scenarijima testiranja funkcionalnosti rezervnog informatičkog centra.

(6) U koloni I (scenarij) su navedeni najčešći scenariji testiranja. U kolonu II (DA/NE) je potrebno unijeti podatak da li je navedena vrsta scenarija bila uključena u predmetno testiranje.

(7) Tabela BA 54.03 Testirani poslovni procesi (POIS3) sadrži podatke o pojedinačnim poslovnim procesima odnosno da li su isti bili uključeni u testiranje funkcionalnosti rezervnog informatičkog centra zajedno sa podacima o korespondirajućim RTO, RPO i MTO parametrima.

(8) Kolona I (poslovni proces) sadrži podatke o najčešćim poslovnim procesima unutar banke. U kolonu II (DA/NE) je potrebno unijeti podatak da li je navedeni poslovni proces bio uključen u predmetno testiranje. U kolonu III (RTO) se unosi podatak o prihvatljivom vremenu neraspoloživosti poslovnog procesa banke koji je definisan Analizom uticaja na poslovanje. U kolonu III (RPO) se unosi podatak o prihvatljivom gubitku podataka u slučaju prekida operacija koji je definisan Analizom uticaja na poslovanje. U kolonu IV (MTO) se unosi podatak o maksimalnom prihvatljivom vremenu neraspoloživosti poslovnog procesa banke, ukoliko je isti definisan.

(9) Tabela BA 54.04 Ostali podaci o oporavku informacionog sistema (POIS4) sadrži ostale potrebne podatke o oporavku informacionog sistema.

(10) U koloni I (predmet) su navedeni podaci o kojima je potrebno izvještavati Agenciju. Pitanja pod rednim brojevima 1-4 sadrže predefinisane odgovore koje je potrebno odabrati. Za pitanje pod rednim brojem 1 potrebno je odabrati jedan od sljedećih odgovora: 1 – nisu korišteni uopšte, 2 – djelimično su korišteni, 3 – korištena je telekomunikaciona veza preko primarnog centra, 4 – ostalo (navesti objašnjenje). Za pitanje pod rednim brojem 2 potrebno je odabrati jedan od sljedećih odgovora: 1 – dnevno, 2 – sedmično, 3 – mjesečno, 4 – polugodišnje, 5 – godišnje, 6 – po potrebi, 7 – nikako, 8 – ostalo (navesti objašnjenje). Za pitanje pod rednim brojem 3 potrebno je odabrati jedan od sljedećih odgovora: 1 – identični centar primarnom centru, što uključuje replikaciju podataka u realnom vremenu i kompletne duple resurse (hardware, komunikacione linije i slično), 2 – hot site, raspoloživost svih resursa sa potrebom oporavka podataka (apliciranja arhivskih logova, kopija podataka i slično), 3 – warm site, raspoloživost hardware-a i telekomunikacionih linija, sa potrebom kompletnog oporavka podataka sa kopija podataka, 4 – cold site, raspoloživost prostora i provedenih instalacija, sa potrebom nabavke i instalacije hardware-a, software-a, te oporavka podataka, 5 – ne posjeduje rezervni informatički centar, 6 – ostalo (navesti objašnjenje). Za pitanje pod rednim brojem 4 potrebno je odabrati jedan od sljedećih odgovora: 1 – sinhrono, 2 – asinhrono, sa zakašnjenjem manjim od dva sata, 3 – asinhrono, sa zakašnjenjem većim od dva sata, 4 – ne provodi se, 5 – ostalo (navesti objašnjenje). Za pitanja pod rednim brojevima 5 – 10 potrebno je upisati odgovore.

(11) Pored gore navedenog, Banka je dužna dostavljati kopije Izvještaja o testiranju rezervnog odnosno lokalnog informatičkog centra, definisane članom 31. stav (2) i članom 32. stav (1) tačka c) Odluke.

Član 16.
Rokovi izvještavanja

(1) Banka je dužna da godišnje (kalendarski), a najkasnije do 05. marta naredne godine za prethodnu godinu, dostavlja Agenciji sljedeće izvještaje:
   a) Izvještaj – Opšti podaci o banci i upravljanju informacionim sistemom sa pripadajućim tabelama (3 tabele),
   b) Izvještaj – Strategija i operativni planovi informacionog sistema,
   c) Izvještaj – Upravljanje rizicima informacionog sistema,
   d) Izvještaj – Budžet informacionog sistema,
   e) Izvještaj – Razvoj informacionog sistema,
   f) Izvještaj – Upravljanje zapisima iz informacionog sistema banke sa pripadajućim tabelama (4 tabele),
   g) Izvještaj – Upravljanje sistemom elektronskog bankarstva sa pripadajućim tabelama (2 tabele),
   h) Izvještaj – Kartično poslovanje sa pripadajućim tabelama (2 tabele) i
   i) Izvještaj – Plan oporavka informacionog sistema sa pripadajućim tabelama (4 tabele).

(2) Banka je dužna da kvartalno (kalendarski), a najkasnije do kraja narednog mjeseca po isteku kvartala, dostavlja Agenciji sljedeće izvještaje:
   a) Izvještaj – Sigurnost informacionog sistema,
   b) Izvještaj – Interna revizija sa pripadajućim tabelama (2 tabele),
   c) Izvještaj – Značajne promjene u informacionom sistemu banke i
   d) Izveštaj – Pregled incidenata/zastoja u informacionom sistemu banke sa pripadajućim tabelama (5 tabela).

(3) Podaci u navedenim izvještajima treba da sadrže podatke iz izvještajnog perioda, sa statusima na zadnji dan izvještajnog perioda.

(4) Forma i obrasci izvještaja su dati u Prilogu ovog Uputstva, te su njegov sastavni dio.

(5) Izvještaji banke trebaju biti potpisani od strane dva lica ovlaštena i odgovorna za predstavljanje banke, od kojih je jedno lice odgovorno i ovlašteno za predstavljanje banke, a drugo lice odgovorno za segment poslovanja na koji se izvještaj odnosi (naprimjer, član Uprave, rukovodilac organizacione jedinice za upravljanje informacionim sistemom u banci, voditelj za sigurnost informacionog sistema, interni revizor i slično).

(6) Osim izvještaja navedenih u stavu (1) ovog člana, banka je dužna dostavljati Agenciji uz godišnje izvještaje i sljedeće izvještaje i dokumente:
   a) Metodologiju upravljanja rizicima informacionog sistema, definisanu članom 11. stav (2) Odluke i
   b) kopije Izvještaja o upravljanju rizicima informacionih sistema, definisane članom 11. stav (3) tačka d) Odluke.

(7) Osim izvještaja navedenih u stavu (2) ovog člana, banka je dužna dostavljati Agenciji uz kvartalne izvještaje i sljedeće izvještaje i dokumente:
   a) kopije Izvještaja Odbora za upravljanje informacionim sistemom, definisane članom 5. stav (1) tačka a) Odluke i
   b) kopije Izvještaja o stanju i aktivnostima vezanim uz sigurnost informacionog sistema, definisane članom 12. stav (2) Odluke.

(8) Osim prethodno navedenih izvještaja, banka je dužna dostavljati Agenciji i sljedeće kopije izvještaja po njihovom usvajanju od strane nadležnih tijela:
   a) kopije Izvještaja penetracionog testiranja/testiranja ranjivosti definisane članom 8. Odluke,
   b) kopije Izvještaja o incidentima i analizi incidenata, definisane članom 25. st. (1) i (3) Odluke i
   c) kopije Izvještaja o testiranju rezervnog odnosno lokalnog informatičkog centra, definisane članom 31. stav (2) i članom 32. stav (1) tačka c) Odluke.

Član 17.
Prelazne i završne odredbe

Ovo Uputstvo stupa na snagu danom njegovog donošenja i objavljuje se na službenoj web stranici Agencije.

Broj: 01-4923/17
Sarajevo, 22.12.2017. godine

DIREKTOR

Jasmin Mahmuzić s.r.

Izvještaj Opšti podaci o banci i upravljanju informacionim sistemom

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 42.01 Opšti podaci (OP)

Ukupan broj zaposlenih u IT	
Naziv organizacione jedinice nadležne za upravljanje informacionim sistemom	
Naziv organizacione jedinice nadležne za sigurnost informacionog sistema	

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

BA 42.02 Opšti podaci o odgovornim licima (OP1)

	Ime i prezime	**Naziv radnog mjesta**	**Stručna sprema**	**Datum početka obavljanja funkcije**
Član Uprave Banke nadležan za upravljanje informacionim sistemom				
Rukovodilac organizacione jedinice nadležne za upravljanje informacionim sistemom				
Lice odgovorno za sigurnost informacionog sistema				
Lice koje obavlja internu reviziju informacionog sistema				

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

BA 42.03 Fluktuacija kadrova u organizacionoj jedinici nadležnoj za upravljanje informacionim sistemom (OP2)

Zasnovali radni odnos (DA/NE)	**Raskinuli radni odnos (DA/NE)**	**Ime i prezime**	**Naziv radnog mjesta**	**Stručna sprema**	**Datum promjene**

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

Izvještaj Strategija i operativni planovi informacionog sistema

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 43.00 Strateški i operativni ciljevi (SOP)

Strateški cilj banke	Strateški cilj informacionog sistema	Operativni plan - projekat/aktivnost	Status	Trajanje projekta/aktivnosti	
				Početak projekta/aktivnosti	Kraj projekta/aktivnosti

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

Izvještaj Upravljanje rizicima informacionog sistema

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 44.00 Plan tretiranja rizika informacionog sistema (RIS)

Kategorija rizika	Rizik	Opis rizika	Nivo rizika	Način tretiranja rizika	Opis mjere	Planirani period implementacije mjere	Status
Rizik dostupnosti i kontinuiteta	neadekvatno upravljanje kapacitetom informacionog sistema	nedostatak resursa (hardware, software, osoblje, pružatelji usluga i drugo) može prouzrokovati nemogućnost održavanja sistema na potrebnom nivou, poteškoće u ispunjavanju poslovnih potreba, prekide u radu sistema i pojavu grešaka					
	greške u radu informacionog sistema	nedostupnost sistema uslijed hardware-skih grešaka					
		nedostupnost sistema uslijed grešaka u software-u					
	neadekvatno planiranje kontinuiteta rada i oporavka informacionog sistema	greške u planiranju, arhitekturi i testiranju kontinuiteta rada i oporavka informacionog sistema					
	cyber napadi koji uzrokuju prekid ili usporenje rada informacionog sistema	razni vidovi napada, koji mogu rezultirati prevelikim opterećenjem informacionog sistema i mreže, prouzrokujući nedostupnost, sporost i ostale probleme u radu i dostupnosti sistema korisnicima					

Rizik sigurnosti	cyber napadi i drugi eksterni napadi na informacioni sistem banke	napadi na informacioni sistem banke sa interneta ili drugih vanjskih mreža, koristeći različite tehnike, koji rezultiraju u preuzimanju kontrole nad dijelom informacionog sistema banke					
		izvršavanje lažnih, zloupotrebljenih plaćanja od strane hakera kroz kršenje ili zaobilaženje sigurnosnih kontrola u sistemu elektronskog bankarstva i drugim kanalima plaćanja i/ili napadi i iskorištavanje sigurnosnih ranjivosti u internom platnom sistemu banke					
		prevare putem lažnih transakcija od strane hakera kroz kršenje ili zaobilaženje sigurnosnih kontrola u elektronskom bankarstvu koje omogućava pristup klijentovim računima					
		napadi na komunikacione linije i ostale vidove komunikacije sa ciljem prikupljanja informacija i zloupotrebe					
	neadekvatna interna sigurnost sistema	neautorizovan pristup kritičnim dijelovima informacionog sistema iz mreže banke, u svrhu zloupotrebe					
		neautorizovane izmjene nad informacionim sistemom uslijed neadekvatnog upravljanja pristupom, procedura i prakse					
		sigurnosne prijetnje uslijed nedostatka svjesti o sigurnosnim rizicima, gdje uposlenici ne razumiju, odbijaju ili ne poštuju politike sigurnosti					
		neautorizovano pohranjivanje ili iznošenje, objavljivanje povjerljivih podataka izvan banke					

		zloupotreba ili krađa resursa informacionog sistema putem fizičkog pristupa, koja može prouzrokovati oštećenja, gubitak resursa i podataka odnosno prouzrokovati druge prijetnje					
	neadekvatna fizička sigurnost informacionog sistema	namjerno ili slučajno fizičko oštećenje resursa informacionog sistema prozrokovano terorizmom, nesrećama, neadekvatnom upotrebom od strane uposlenika banke ili pružatelja usluga i slično					
		nedovoljna fizička zaštita od prirodnih nepogoda koja može prouzrokovati djelimično ili kompletno uništenje resursa informacionog sistema					
Rizik upravljanja izmjenama	neadekvatna kontrola nad razvojem i izmjenama informacionog sistema	incidenti prouzrokovani nedetektovanim greškama ili ranjivostima koje su nastale kao rezultat izmjena nad sistemom					
	neadekvatna arhitektura informacionog sistema	neadekvatno upravljanje arhitekturom informacionog sistema prilikom njegovog dizajna, razvoja i održavanja, koje može vremenom rezultirati kompleksnom, otežanom, skupom održavanju i upravljanju, te koje više nije u mogućnosti zadovoljiti poslovne potrebe					
	neadekvatno upravljanje životnim ciklusom i nadogradnjama informacionog sistema	neadekvatno održavanje registra resursa informacionog sistema, upravljanja životnim ciklusom i nadogradnjama, može voditi ka nepravovremenoj i neadekvatnoj nadogradnji, ažuriranju informacionog sistema, te sistemu koji ne može zadovoljiti poslovne potrebe					

Rizik integriteta podataka	greške pri upravljanju i obradi podataka	uslijed sistemskih, komunikacijskih i/ili aplikativnih grešaka, pogrešno procesiranih podataka, procesa prijenosa i unosa podataka, podaci mogu biti korumpirani ili izgubljeni					
	neadekvatan dizajn kontrola na validaciji podataka	greške koje se odnose na nedostatak ili neefikasnost automatizovanih kontrola unosa i prihvata podataka, transfera podataka, procesiranja i izlaznih kontrola					
	neadekvatna kontrola nad izmjenom podataka	greške u podacima uslijed nedostatka kontrola nad izmjenama podataka					
	neadekvatno dizajnirana arhitektura podataka, tok podataka, model podataka ili riječnik podataka	neadekvatno upravljanje arhitekturom podataka i modelom, može rezultirati nekonzistentnošću podataka					
Rizik eksternalizacije	neadekvatne mjere zaštite i upravljanje od strane pružaoca usluga	nedostupnost kritičnih eksternalizovanih servisa, telekomunikacionih servisa i usluga; gubitak ili korupcija kritičnih/osjetljivih podataka koje su povjerene pružaocu usluga					
	neadekvatno upravljanje eksternalizacijom od strane banke	značajna degradacija sistema ili greške uslijed nedovoljne pripremljenosti ili kontrolnih procesa kod pružaoca usluga; neadekvatno upravljanje eksternalizacijom može rezultirati u nedostatku odgovarajućih znanja i kapaciteta u cilju identifikacije, pristupa, umanjenja i nadzora nad rizikom informacionih sistema i ograničavanju bančinih operativnih kapaciteta					

	neadekvatne kontrole sigurnosti informacionog sistema kod pružaoca usluga	napadi hakera na sisteme pružaoca usluga, sa direktnim uticajem na izvršavanje eksternalizovanih aktivnosti i/ili pristup kritičnim/povjerljivim informacijama kod pružaoca usluga; osoblje pružaoca usluga ima omogućen neautorizovan pristup kritičnim/osjetljivim podacima banke koji se nalaze kod pružaoca usluga					

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

Izvještaj Sigurnost informacionog sistema

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 45.00 Rezultati penetracionih testiranja/testova ranjivosti (SIS)

Naziv izvještaja	Rizik	Nivo rizika	Prijedlog načina tretiranja rizika	Opis	Planirani period izvršenja - kvartal	Aktuelni završetak aktivnosti

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

Izvještaj Interna revizija

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 46.01 Pregled planiranih i provedenih revizija informacionog sistema (ITR)

Oblast IS po regulativi	Oblast revizije informacionog sistema (metodologija banke)	Jedinstvena oznaka predmetne revizije	Revizijski ciklus	Oblast uključena u period za koji se dostavlja izvještaj (DA/NE)	Detaljniji opis predmeta, cilja i opsega revizije	Trajanje revizije		Ocjena oblasti (u skladu sa metodologijom banke)
						Početak	Kraj	
Upravljanje strategijom informacionog sistema								
Upravljanje politikom sigurnosti i internim aktima								
Adekvatnost organizacije upravljanja IS								
Voditelj sigurnosti informacionog sistema								
Upravljanje rizicima informacionog sistema								
Upravljanje pristupom operativnom sistemu								
Upravljanje pristupom bankarskoj aplikaciji								
Upravljanje pristupom bazi podataka								
Upravljanje pristupom mrežnim komponentama								
Kontrole cyber sigurnosti								
Upravljanje zapisima								
Kontrole pristupa ostalo (email, antivirusna zaštita, USB i slično)								

Upravljanje resursima informacionog sistema								
Upravljanje dokumentacijom								
Upravljanje edukacijom								
Upravljanje incidentima								
Upravljanje korisničkim zahtjevima								
Upravljanje razvojem								
Upravljanje promjenama								
Upravljanje integritetom podataka								
Upravljanje backup-om								
Upravljanje planom kontunuiteta poslovanja								
Fizičke kontrole resursa informacionog sistema								
Elektronsko bankarstvo								
Kartično poslovanje								
SWIFT kontrole								
Revizija eksternalizovanih aktivnosti								
Ostalo - navesti								

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 46.02 Pregled preporuka (interne revizije, eksterne revizije i Agencije za bankarstvo FBiH) (ITR1)

Jedinstvena oznaka predmetne revizije	Uočeni nedostaci	Nivo rizika	Mjere za korekciju	Rok za implementaciju mjera	Praćenje izvršenja mjere (follow-up) - opis	Status izvršenja mjere

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

Izvještaj Budžet informacionog sistema

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 47.00 Budžet informacionog sistema (BIS)

	(u 000 KM)	**(u 000 KM)**	
Opis	**Planirano**	**Realizovano**	**%**
Ukupni budžet banke			
Ukupni budžet IT			
Održavanje ključne bankarske aplikacije			
Razvoj ključne bankarske aplikacije			
Razvoj sistema elektronskog bankarstva			
Održavanje sistema elektronskog bankarstva			
Razvoj sistema mobilnog bankarstva			
Održavanje sistema mobilnog bankarstva			
Razvoj sistema podrške kartičnom poslovanju			
Održavanje sistema kartičnog poslovanja			
Razvoj ostalih aplikacija za podršku			
Održavanje ostalih aplikacija za podršku			
Održavanje hardware			
Ulaganje u novi hardware			
Telekomunikacione usluge			
Ostale investicije			
Ostali troškovi			

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

Izvještaj Razvoj informacionog sistema

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 48.00 Razvoj i održavanje software-a (ROS)

Predmet	**Interno**	**Eksterno - naziv pružaoca usluga**
Razvoj ključne bankarske aplikacije		
Održavanje ključne bankarske aplikacije		
Razvoj sistema elektronskog bankarstva		
Održavanje sistema elektronskog bankarstva		
Razvoj sistema podrške kartičnom poslovanju		
Održavanje sistema podrške kartičnom poslovanju		
Razvoj ostalih aplikacija za podršku		
Održavanje ostalih aplikacija za podršku		
Ostalo		

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

Izvještaj Značajne promjene u informacionom sistemu banke

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 49.00 Značajne promjene u informacionom sistemu banke (PIS)

Dio informacionog sistema	Opis izmjene	Hitnost izmjene	Status

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

Izvještaj Upravljanje zapisima iz informacionog sistema banke

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 50.01 Pregled upravljanja zapisima iz Aktivnog Direktorija (ZIS1)

Naziv resursa i opis funkcije: _____

Predmet zapisa	**Vrste zapisa**	**Učestalost pregleda/analize**	**Datum zadnje analize**
Događaji logiranja računa (eng. Audit account logon events)			
Izmjena računa (eng. Audit account management)			
Pristup direktoriju (eng. Audit directory service access)			
Događaji logiranja (eng. Audit logon events)			
Pristup objektima (eng. Audit object access)			
Promjena politika (eng. Audit policy change)			
Upotreba privilegovanih računa (eng. Audit privilege use)			
Praćenje procesa (eng. Audit process tracking)			
Sistemski događaji (eng. Audit system events)			
Ostalo (opisati)			

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

BA 50.02 Pregled upravljanja zapisima iz produkcione baze podataka ključne bankarske aplikacije (ZIS2)

Naziv resursa i opis funkcije: _____

Predmet zapisa	**Praćenje aktivnosti**	**Učestalost pregleda/analize**	**Datum zadnje analize**
Aktivnosti računa sa administratorskim ovlastima			
Aktivnosti računa sa povlaštenim sistemskim privilegijama (kreiranje tabela i slično)			
Aktivnosti sistemskih računa (sys, system i slično)			
Aktivnosti generičkih računa			
Aktivnosti servisnih računa			
Aktivnosti računa sa povlaštenim privilegijama nad podacima (unos, izmjena, brisanje podataka izvan aplikacije)			
Izmjene nad bazom podataka koje se odnose na konfiguracijske parametre			
Promjene privilegija dodijeljenih sistemskim i generičkim računima			
Izmjene nad upravljanjem korisničkim računima (kreiranje, brisanje)			
Izmjene nad upravljanjem privilegijama korisnika (dodjela, izmjena i slično)			
Događaji zaključavanja/otključavanja računa na bazi podataka			
Događaji prijavljivanja na bazu podataka			
Događaji odjavljivanja sa baze podataka			

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 50.03 Pregled upravljanja zapisima sa ključnih mrežnih komponenti (ZIS3)

Naziv resursa i opis funkcije: _____

Predmet aktivnosti	**Praćenje aktivnosti (Da/Ne)**	**Učestalost pregleda/analize**	**Datum zadnje analize**
Aktivnosti izmjene konfiguracija			
Aktivnosti neuspješne prijave na uređaj			

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

BA 50.04 Udaljeni pristup prema resursima informacionog sistema (ZIS4)

Korisnik koji je ostvario pristup	**Resurs kojem je pristupio**	**Broj pristupa**

Ovlašteno lice (ime i prezime, potpis i telefonski broj) Predsjednik Uprave

Izvještaj Pregled incidenata/zastoja u informacionom sistemu banke

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 51.01 Kategorizacija incidenata (PI1)

Nivo	Opis
I	
II	
III	
IV	

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 51.02 Broj incidenata/zastoja po poslovnim procesima (PI2)

Poslovni proces	Broj incidenata kategorije I	Broj incidenata kategorije II	Broj incidenata kategorije III	Broj incidenata kategorije IV	Broj problema/zastoja koji nisu kategorisani kao incidenti	Ukupno vrijeme prekida/zastoja rada (trajanje u minutama)	Način rješavanja (interno ili eksterno)	Napomena/opis	UKUPNO
Ključna bankarska aplikacija									0
Elektronsko bankarstvo									0
Mobilno bankarstvo									0
Kartično poslovanje									0
Hardware									0
Mrežna infrastruktura									0
Telekomunikacione veze									0
Električno napajanje									0
Druge poslovne aplikacije									0
Upravljanje promjenama									0
Maliciozni kod									0
Ostalo									0
UKUPNO	**0**	**0**	**0**					**0**	**0**

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 51.03 Broj prema vrstama incidenata (PI3)

Vrsta	Broj
Prekidi u radu hardware-skih i software-skih komponenti	
Smanjenje performansi servisa	
Neautorizovani pristup resursima informacionog sistema	
Odliv podataka	
Maliciozni kod	
Krađa	
Neuspješan proces izrade rezervne kopije podataka	
Narušavanje integriteta podataka	
Ostalo	
UKUPNO	**0**

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 51.04 Cyber incidenti (PI4)

Vrsta	Broj
Ransomware napadi	
DDOS napad	
Phishing napadi	
Krađa indentiteta klijenta	
Man in the middle napad	
UKUPNO	**0**

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 51.05 Elektronsko bankarstvo i kartično poslovanje – moguće zloupotrebe (PI5)

Vrsta događaja	Broj transakcija u elektronskom bankarstvu	Iznos (u 000 KM)	Broj transakcija u kartičnom poslovanju	Iznos (u 000 KM)
sumnjive transakcije – prevenirane				
sumnjive transakcije – otvorene				
sumnjive transakcija – isplaćene				
sumnjive transakcije – ostalo				

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

Izvještaj Upravljanje sistemom elektronskog bankarstva

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 52.01 Obim elektronskog bankarstva (UEB1)

	PRAVNA LICA					FIZIČKA LICA					UKUPNO				
	Broj klijenata	Realizovane transakcije UPP		Realizovane transakcije IPP		Broj klijenata	Realizovane transakcije UPP		Realizovane transakcije IPP		Broj klijenata	Realizovane transakcije UPP		Realizovane transakcije IPP	
		broj	iznos u (000) KM	broj	iznos u (000) KM		broj	iznos u (000) KM	broj	iznos u (000) KM		broj	iznos u (000) KM	broj	iznos u (000) KM
Platni promet banke											**0**	**0**	**0**	**0**	**0**
Elektronsko bankarstvo											**0**	**0**	**0**	**0**	**0**
%															
Mobilno bankarstvo											**0**	**0**	**0**	**0**	**0**
%															

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 52.02 Sredstva autentifikacije i autorizacije u sistemu elektronskog bankarstva (UEB2)

Naziv sistema	Naziv pružaoca usluge u slučaju eksternalizacije	Vrsta elektronskog bankarstva	Način autentifikacije		
			Elementi autentifikacije	Broj klijenata	
				Fizička lica	Pravna lica
			pametna kartica + PIN		
			USB certifikat + PIN		
			jednokratna lozinka (OTP)		
			HW token + PIN		
			SW token + PIN		
			PIN + TAN		
			korisničko ime i lozinka		
			...		

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

Izvještaj Kartično poslovanje

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 53.01 Obim kartičnog poslovanja (KP1)

Vrsta kartice	Pravna lica		Fizička lica	
	Broj kartica	Iznos transakcija	Broj kartica	Iznos transakcija
Visa – debit				
Visa – credit				
MasterCard – debit				
MasterCard – credit				
American				
Diners				
BamCard				
Prepaid				
Ostalo				
UKUPNO	**0**	**0,00**	**0**	**0,00**

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 53.02 Broj POS i ATM uređaja (KP2)

Vrsta uređaja	Broj uređaja u banci	Broj uređaja izvan banke	Ukupno
POS			
ATM			

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

Izvještaj Plan oporavka informacionog sistema

Naziv banke: _____ Matični broj: _____

Datum: _____

BA 54.01 Načini testiranja (POIS1)

Poslovni proces	**Proces testiran**	**Uključenost centrale banke u testiranje**	**Broj uključenih poslovnih jedinica**
Simulacija (1 kritični poslovni proces)			
Simulacija (1 - 5 kritičnih poslovnih procesa)			
Simulacija (više od 5 kritičnih poslovnih procesa)			
Simulacija (svi kritični poslovni procesi)			
Stvarni rad banke sa rezervne informatičke lokacije (1 kritični poslovni proces)			
Stvarni rad banke sa rezervne informatičke lokacije (od 1 - 5 kritičnih poslovnih procesa)			
Stvarni rad banke sa rezervne informatičke lokacije (više od 5 kritičnih poslovnih procesa)			
Stvarni rad banke sa rezervne informatičke lokacije (svi kritični poslovni procesi)			

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 54.02 Scenariji za testiranje (POIS2)

Scenarij	DA/NE
Nedostupnost ključnog IT osoblja	
Epidemija ili drugi scenariji nedostupnosti većeg broj zaposlenika	
Nedostupnost centralne lokacije (i ostale prirodne katastrofe)	
Kvar programske podrške i korupcija podataka	
Nedostupnost električne energije, telekomunikacija i ostalih standardnih usluga	
Nedostupnost ključnog pružaoca usluga	
Cybernapad	
Ostalo	

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 54.03 Testirani poslovni procesi (POIS3)

Poslovni proces	DA/NE	RTO	RPO	MTO (ukoliko je definisan)
Domaći platni promet				
Devizni platni promet				
Mobilno bankarstvo za fizička lica				
Mobilno bankarstvo za pravna lica				
Elektronsko bankarstvo za fizička lica				
ELektronsko bankarstvo za pravna lica				
Kartično poslovanje				
Trezorsko poslovanje				
Računovodstvo (glavna knjiga)				
Šaltersko poslovanje				
Krediti za fizička lica				
Krediti za pravna lica				
Depoziti za fizička lica				
Depoziti za pravna lica				
Izvještavanje (regulatorno i interno)				
Sprečavanje pranja novca i finansiranja terorizma				
Skrbništvo				
Akreditivi i garancije				
SWIFT				
Komunikacija sa Centralnom bankom				
Upravljanje rizicima				
Ostalo				

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave

BA 54.04 Ostali podaci o oporavku informacionog sistema (POIS4)

R.br.	Predmet	Odabrati odgovor (pitanja 1-4):
1.	Prilikom testiranja resursi sa primarnog informatičkog centra su:	
2.	Testiranje oporavka sa kopija podataka se vrši:	
3.	Rezervni informatički centar je:	
4.	Osvježavanje podataka na rezervnom informatičkom centru se vrši:	
5.	Broj IT osoblja uključen u testiranje rezervne lokacije:	
6.	Broj osoblja poslovne strane uključen u testiranje rezervne lokacije	
7.	Navesti pružaoce usluga koji su bili uključeni u testiranje rezervne lokacije:	
8.	Lokacija primarnog informatičkog centra:	
9.	Lokacija rezervnog informatičkog centra:	
10.	Lokacija lokalnog informatičkog centra:	

Ovlašteno lice (ime i prezime, potpis i telefonski broj)

Predsjednik Uprave