BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
AGENCIJA ZA BANKARSTVO
FEDERACIJE BOSNE I HERCEGOVINE

UPUTSTVO

ZA IZVJEŠTAVANJE O UPRAVLJANJU INFORMACIONIM SISTEMIMA

Sarajevo, januar / siječanj 2021. godine

Na osnovu člana 5. stav (1) tačka h) i člana 23. stav (1) Zakona o Agenciji za bankarstvo Federacije Bosne i Hercegovine („Službene novine Federacije BiH“, broj 75/17), člana 16. stav (1) tačka (k) Statuta Agencije za bankarstvo Federacije Bosne i Hercegovine („Službene novine Federacije BiH“, broj 3/18) i člana 8. Odluke o izvještajima koje banka dostavlja Agenciji za bankarstvo Federacije Bosne i Hercegovine u nadzorne i statističke svrhe („Službene novine Federacije BiH“, broj 86/20), direktor Agencije za bankarstvo Federacije Bosne i Hercegovine dana 18.01.2021. godine donosi

UPUTSTVO
ZA IZVJEŠTAVANJE O
UPRAVLJANJU INFORMACIONIM SISTEMIMA

I UVODNE ODREDBE

Član 1.
Predmet

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

Član 2.
Struktura i pravila

(1) Izvještajni okviru o upravljanju informacionim sistemom u banci se sastoji od sljedećih izvještaja:
   a) Izvještaj Opšti podaci sa pripadajućim obrascima (5 obrazaca):
      1) BA 42.01 Opšti podaci o organizacionoj strukturi (OP1),
      2) BA 42.02 Opšti podaci o odgovornim osobama (OP2),
      3) BA 42.03 Opšti podaci o fluktuaciji kadra (OP3),
      4) BA 42.04 Opšti podaci o vanjskim IT saradnicima (OP4) i
      5) BA 42.05 Opšti podaci o internoj reviziji informacionog sistema (OP5),
   b) Izvještaj Opšti podaci o informacionom sistemu banke sa pripadajućim obrascima (7 obrazaca):
      1) BA 43.01 Resursi IT – infrastruktura sistema (RIT1),
      2) BA 43.02 Resursi IT – serveri (RIT2),
      3) BA 43.03 Resursi IT – mrežni uređaji (RIT3),
      4) BA 43.04 Resursi IT – radne stanice (RIT4),
      5) BA 43.05 Resursi IT – bankomati (RIT5),
      6) BA 43.06 Resursi IT – podrška (RIT6),
      7) BA 43.07 Resursi IT – udaljeni pristup (RIT7),
   c) Izvještaj Strategija i operativni planovi informacionog sistema: BA 44.00 Strateški i operativni ciljevi (SOP),
   d) Izvještaj Upravljanje rizicima informacionog sistema: BA 45.00 Plan tretiranja rizika informacionog sistema (RIS),
   e) Izvještaj Sigurnost informacionog sistema: BA 46.00 Rezultati penetracionog testiranja /testova ranjivosti (PEN),
   f) Izvještaj Interna revizija sa pripadajućim obrascima (2 obrasca):
      1) BA 47.01 Pregled planiranih i provedenih revizija informacionog sistema (ITR1),
      2) BA 47.02 Pregled preporuka/naloga revizije informacionog sistema (ITR2),

g) Izvještaj Budžet informacionog sistema sa pripadajućim obrascima (2 obrasca):
   1) BA 48.01 Budžet informacionog sistema (BIS1),
   2) BA 48.02 Budžet FinTech (BIS2),
h) Izvještaj Značajne promjene u informacionom sistemu banke: BA 49.00 Značajne promjene u informacionom sistemu banke (PIS)
i) Izvještaj Pregled incidenata/zastoja u informacionom sistemu banke sa pripadajućim obrascima (5 obrazaca):
   1) BA 50.01 Kategorizacija incidenata (INC1),
   2) BA 50.02 Broj incidenata/zastoja po poslovnim procesima (INC2),
   3) BA 50.03 Broj prema vrstama incidenata (INC3),
   4) BA 50.04 Cyber incidenti (INC4) i
   5) BA 50.05 Elektronsko bankarstvo i kartično poslovanje – moguće zloupotrebe (INC5),
j) Izvještaj Upravljanje sistemom elektronskog bankarstva sa pripadajućim obrascima (2 obrasca):
   1) BA 51.01 Obim elektronskog bankarstva (EB1) i
   2) BA 51.02 Sredstva autentifikacije i autorizacije u sistemu elektronskog bankarstva (EB2),
k) Izvještaj Kartično poslovanje sa pripadajućim obrascima (2 obrasca):
   1) BA 52.01 Obim kartičnog poslovanja (KP1) i
   2) BA 52.02 Broj POS i ATM uređaja (KP2),
l) Izvještaj Upotreba novih tehnologija : BA 53.01 Obim korištenja novih tehnologija (OFT),
m) Izvještaj Plan oporavka informacionog sistema sa pripadajućim obrascima (4 obrasca):
   1) BA 54.01 BCM - Načini testiranja (BCM1),
   2) BA 54.02 BCM - Scenariji za testiranje (BCM2),
   3) BA 54.03 BCM - Testirani poslovni procesi (BCM3) i
   4) BA 54.04 BCM - Ostali podaci o oporavku informacionog sistema (BCM4).

(2) Obrasci navedeni u stavu (1) ovog člana su sastavni dio ovog Uputstva i objavljuju se na službenoj web stranici Agencije.

II OBRASCI ZA UPRAVLJANJE INFORMACIONIM SISTEMOM

Član 3.
Izvještaj Opšti podaci

(1) Izvještaj Opšti podaci o banci sadrži podatke o banci, organizacionom dijelu zaduženom za upravljanje informacionim sistemom u banci, organizacionom dijelu zaduženom za sigurnost informacionog sistema, fluktuaciji kadra u ova dva organizaciona dijela, vanjskim IT saradnicima, kao i o internoj reviziji informacionog sistema banke.

(2) Izvještaj se sastoji od pet obrazaca:
   a) BA 42.01 Opšti podaci o organizacionoj strukturi (OP1),
   b) BA 42.02 Opšti podaci o odgovornim osobama (OP2),
   c) BA 42.03 Opšti podaci o fluktuaciji kadra (OP3),
   d) BA 42.04 Opšti podaci o vanjskim IT saradnicima (OP4) i
   e) BA 42.05 Opšti podaci o internoj reviziji informacionog sistema (OP5),

(3) Obrazac BA 42.01 Opšti podaci o organizacionoj strukturi (OP1) sadrži podatke o broju zaposlenih i nazivu organizacionih jedinica nadležnih za upravljanje informacionim sistemom i sigurnosti informacionog sistema. Obrazac se dostavlja na godišnjem nivou i sadrži podatke, koji se odnose na ukupan broj zaposlenih, broj zaposlenih na određeno, broj zaposlenih na neodređeno i broj otvorenih pozicija (naspram ukupno planiranih pozicija za navedeni odjel prema sistematizaciji banke) za navedene dvije organizacione jedinice. U okviru broja zaposlenika u sigurnosti informacionog sistema, potrebno je navesti broj uposlenika koji se

bave sigurnosti informacionog sistema, a ne općenito sigurnosti banke, kao što je fizička sigurnost i slično.

(4) Za organizacionu jedinicu nadležnu za upravljanje informacionim sistemom, pored prethodno navedenih podataka, potrebno je upisati i broj zaposlenih koji se odnosi na uposlenike koji obavljaju poslove administracije ključnih dijelova informacionog sistema banke, kao što su administracija operativnih sistema, baze podataka i mreže banke.

(5) Obrazac BA 42.02 Opšti podaci o odgovornim osobama (OP2) sadrži podatke o licima odgovornim za upravljanje informacionim sistemom. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji se odnose na (ime i prezime, naziv radnog mjesta, stručna sprema i datum početka obavljanja funkcije) člana uprave nadležnog za segment upravljanja informacionim sistemom, člana uprave nadležnog za segment upravljanja sigurnošću informacionog sistema, rukovodioca organizacione jedinice nadležne za upravljanje informacionim sistemom i Lice odgovorno za sigurnost informacionog sistema (u slučaju više uposlenika koji se bave poslovima sigurnosti informacionog sistema, potrebno je navesti podatke o najviše rangiranoj osobi u okviru sistematizacije banke).

(6) Obrazac BA 42.03 Opšti podaci o fluktuaciji kadra (OP3) sadrži podatke o zaposlenicima banke koji su zasnovali, odnosno prekinuli ili promijenili radno mjesto u toku izvještajne kalendarske godine, u organizacionoj jedinici nadležnoj za upravljanje informacionim sistemom i organizacionoj jedinici nadležnoj za sigurnost informacionog sistema. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji se odnose na ime i prezime, naziv radnog mjesta, zanimanje, vrstu promjene i datum promjene. U slučaju promjene radnog mjesta, u podatku o nazivu radnog mjesta, potrebno je navesti naziv novog radnog mjesta/naziv starog radnog mjesta. Podaci u obrascu se popunjavaju za svaki kvartal za koji se obrazac i dostavlja.

(7) Obrazac BA 42.04 Opšti podaci o vanjskim IT saradnicima (OP4) sadrži podatke o saradnicima koji nisu uposlenici banke i firmama koje obavljaju poslove u organizacionoj jedinici nadležnoj za upravljanje informacionim sistemom, a koji banci pružaju podršku u okviru poslova iz domena informacionih tehnologija. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji se odnose na: naziv firme/ime i prezime saradnika, opis poslova, datum početka obavljanja usluge, datum potpisivanja ugovora, trajanje ugovora i završetak ugovora.

(8) Obrazac BA 42.05 Opšti podaci o internoj reviziji informacionog sistema (OP5) sadrži podatke o licima/firmi koja obavlja funkciju interne revizije informacionog sistema banke. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji se odnose na: ime i prezime/naziv, zanimanje, certifikat i datum angažmana (od-do). U slučaju da funkciju interne revizije informacionog sistema obavlja eksterna firma, potrebno je upisati puni naziv firme u koloni „Ime i prezime/Naziv“ za red „Naziv pružaoca usluge“, a zatim za red „Lica koja obavljaju internu reviziju informacionog sistema (interno/eksterno)“ upisati ime i prezime svih osoba koje će ispred eksterne firme obavljati reviziju. Zatim je potrebno popuniti i ostale kolone (zanimanje, certifikat i datum angažmana od-do).

Član 4.
Izvještaj Opšti podaci o informacionom sistemu banke

(1) Izvještaj Opšti podaci o informacionom sistemu banke sadrži podatke o resursima informacionog sistema banke koji se odnose na infrastrukturu sistema, servere, mrežne uređaje, radne stanice, bankomate, software i udaljeni pristup.

(2) Izvještaj se sastoji od sedam obrazaca:
   a) BA 43.01 Resursi IT – infrastruktura sistema (RIT1),
   b) BA 43.02 Resursi IT – serveri (RIT2),
   c) BA 43.03 Resursi IT – mrežni uređaji (RIT3),
   d) BA 43.04 Resursi IT – radne stanice (RIT4),
   e) BA 43.05 Resursi IT – bankomati (RIT5),

f) BA 43.06 Resursi IT – podrška proizvođača (RIT6) i
g) BA 43.07 Resursi IT – udaljeni pristup (RIT7).

(3) Obrazac BA 43.01 Resursi IT – infrastruktura sistema (RIT1) sadrži generalne podatke o broju resursa informacionog sistema. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.

(4) Sadržaj obrasca:
a) Kolona Resurs – sadrži pobrojane resurse za koje je u koloni II potrebno upisati broj, a odnose se na: broj data centara lociranih u banci i izvan banke, ukupan broj kritičnih IT sistema, broj fizičkih/logičkih platformi, broj aplikacija, broj aplikacija u Excel-u, MS Db i sličnim alatima, a koje podržavaju kritične operacije uključujući i izvještaje.
b) Kolona Broj resursa – sadrži broj koji se odnosi na resurse pobrojane u koloni I, gdje je za resurs:
1) „Broj data centara lociranih u banci“ - potrebno upisati broj data centara koji su u vlasništvu banke, a u kojima se nalaze resursi informacionog sistema banke koji pokreću ključni produkcioni sistem; u navedeni broj nije potrebno ubrajati rezervni DR centar,
2) „Broj data centara lociranih izvan banke“ - potrebno upisati broj data centara koji su u vlasništvu pružaoca usluga, a u kojima se nalaze resursi informacionog sistema banke koji pokreću ključni produkcioni sistem; u navedeni broj nije potrebno ubrajati rezervni DR centar,
3) „Ukupan broj kritičnih IT sistema“ – upisati broj kritičnih IT sistema koji su od strane banke definisani u okviru Analize uticaja na poslovanje,
4) „Broj fizičkih/logičkih platformi“ – odnosi se na broj fizičkih i/ili logičkih platformi koje se koriste kao podrška kritičnim poslovnim procesima,
5) „Broj aplikacija“ – upisati broj ključnih aplikacija koje podržavaju ključne poslovne procese i koje su definisane od strane banke u okviru Analize uticaja na poslovanje,
6) „Broj aplikacija u Excel-u, MS Db i sličnim alatima, a koje podržavaju kritične operacije uključujući i izvještavanje“ – odnosi se na broj aplikacija koje su razvijene u Excel-u, MS Db i sličnim alatima, a koji se koriste kao podrška kritičnim operacijama, kao što je izvještavanje i manje obrade, a koje nisu ubrojane u prethodne aplikacije.

(5) Obrazac BA 43.02 Resursi IT – serveri (RIT2) sadrži podatke o serverima koji podržavaju kritične/ključne poslovne procese banke, među koje spadaju i serveri koji se nalaze kod vanjskih pružaoca usluga. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.

(6) Sadržaj obrasca:
a) Kolona Naziv servera – potrebno upisati oznaku servera u IT sistemu banke, a odnosi se na servere koji podržavaju kritične/ključne poslovne procese, a nalaze se u banci ili kod vanjskog pružaoca usluga,
b) Kolona Namjena servera – sadrži podatak o namjeni servera, gdje je potrebno upisati namjenu servera, kao što je na primjer: aplikativni server ključne bankarske aplikacije, server ključne bankarske aplikacije sa bazom podataka, backup server i slično,
c) Kolona Fizički/virtuelni – sadrži podatak o tome da li je server fizički ili virtualni,
d) Kolona Naziv i verzija operativnog sistema – potrebno upisati naziv operativnog sistema i verziju koja se nalazi na serveru i
e) Kolona Lokacija – podatak o tome da li se server nalazi u banci i u kojem data centru ili se nalazi kod vanjskog pružaoca usluga i na kojoj lokaciji; u slučaju da se server nalazi kod vanjskog pružaoca usluga potrebno je navesti podatak o nazivu pružaoca usluga i fizičkoj lokaciji servera (grad/država).

(7) Obrazac BA 43.03 Resursi IT – mrežni uređaji (RIT3) sadrži podatke o mrežnim uređajima, koji podržavaju kritične/ključne poslovne procese, a nalaze se u mreži banke, kao i kod vanjskih pružaoca usluga. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.

(8) Sadržaj obrasca:
   a) Kolona Vrsta mrežnog uređaja – ovdje je potrebno navesti mrežne uređaje koji se nalaze u banci, kao i mrežne uređaje koji se nalaze kod pružaoca usluga, a potrebni su kao podrška za odvijanje ključnih/kritičnih poslovnih procesa banke; u slučaju da je banka eksternalizovala data centar, potrebno je uključiti sve mrežne uređaje koji podržavaju odvijanje ključnih poslovnih procesa banke, kako su ocijenjeni u Analizi uticaja na poslovanje,
   b) Kolona Model – sadrži podatak o modelu mrežnog uređaja,
   c) Kolona Proizvođač – sadrži podatak o proizvođaču mrežnog uređaja,
   d) Kolona OS/Firmware – sadrži podatak o operativnom sistemu i firmware-u koji se nalazi na mrežnom uređaju,
   e) Kolona Količina – potrebno upisati broj mrežnih uređaja koji zadovoljavaju podatke koji su upisani u prethodnim poljima,
   f) Kolona Lokacija - u okviru lokacije potrebno je navesti da li se mrežni uređaji nalaze u okviru banke ili u okviru fizičke lokacije pružaoca usluga, za navedenu vrstu mrežne opreme.

(9) Obrazac BA 43.04 Resursi IT – radne stanice (RIT4) sadrži podatke o aktivnim radnim stanicama koje se koriste u banci. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji se odnose na broj aktivnih radnih stanica, te naziv i verziju operativnog sistema koji se nalazi na njima.

(10) Obrazac BA 43.05 Resursi IT - bankomati (RIT5) sadrži podatke o bankomatima koje banka koristi (u vlasništvu banke ili u vlasništvu pružaoca usluga u slučaju eksternalizacije). Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.

(11) Sadržaj obrasca:
   a) Kolona Naziv proizvođača – sadrži podatak o nazivu proizvođača bankomata,
   b) Kolona Broj bankomata – upisuje se broj/količina bankomata prethodno navedenog proizvođača,
   c) Kolona Operativni sistem – upisuje se naziv i verzija operativnog sistema za prethodno navedeni broj bankomata od navedenog proizvođača,
   d) Kolona Software – upisuje se naziv i verzija software-skog programa koji se nalazi na bankomatu navedenog proizvođača,
   e) Kolona Vlasništvo- sadrži podatak da li se bankomati nalaze u vlasništvu banke ili pružaoca usluga, u slučaju pružaoca usluga navesti naziv pružaoca usluga,
   f) Kolona Eksternalizovana usluga održavanja bankomata – sadrži podatak o tome da li je održavanje bankomata eksternalizovano, izborom opcije DA ili NE,
   g) Kolona Naziv pružaoca usluge – u slučaju da je u koloni VI odgovoreno sa DA potrebno je upisati naziv pružaoca usluge koji održava bankomate,
   h) Kolona Opis eksternalizovane aktivnosti - u slučaju da se aktivnost održavanja bankomata eksternalizuje, potrebno je navesti opis vrste aktivnosti za koju je pružaoc usluga zadužen (održavanje, nadzor, servisiranje i slično).

(12) Obrazac BA 43.06 Resursi IT – podrška proizvođača (RIT6) sadrži podatke o software-u, licenci i hardware-u za mrežne uređaje, servere, radne stanice, bankomate koji su navedeni u prethodnim obrascima ovog izvještaja, a za koje je podrška proizvođača istekla u toku godine za koju se izvještaj popunjava, kao i one kojima podrška ističe u narednih 12 mjeseci (od dana dostave izvještaja). Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji se odnose na: naziv software-a/licence/hardware-a, broj uređaja na kojima se nalaze software/licenca/hardware iz prethodne kolone, datum prestanka podrške za istu i planirani datumu zamjene.

(13) Obrazac BA 43.07 Resursi IT – udaljeni pristup (RIT7) sadrži podatke o udaljenom pristupu koji se može uspostaviti prema ključnim resursima informacionog sistema banke od strane eksternih kompanija/pružaoca usluga. Obrazac se dostavlja na godišnjem nivou i sadrži

podatke koji se odnose na: naziv eksterne kompanije/pružaoca usluga, vrsta pristupa (gdje je potrebno izabrati jednu od opcija site to site ili client to site), tip enkripcije, broj uposlenika eksterne kompanije koji imaju pristup IS banke, te navesti da li je pristup personalizovan (DA/NE).

Član 5.

Izvještaj Strategija i operativni planovi informacionog sistema

(1) Izvještaj Strategija i operativni planovi informacionog sistema sadrži podatke o povezanosti strategije banke i strategije informacionog sistema, te realizaciji strategije informacionog sistema kroz operativne planove informacionog sistema.
(2) Izvještaj se sastoji od jednog obrasca i to: BA 44.00 Strateški i operativni ciljevi (SOP).
(3) Obrazac iz stava (2) ovog člana sadrži osnovne podatke o strateškim ciljevima banke i korespondirajućim strateškim ciljevima informacionog sistema i odgovarajućim operativnim planovima odnosno projektima/aktivnostima organizacione jedinice nadležne za upravljanje informacionim sistemom u banci. Obrazac se dostavlja na godišnjem nivou i treba da sadrži podatke o svim planiranim strateškim/operativnim aktivnostima za izvještajnu godinu za koju se dostavlja, njihov status realizacije, kao i planirane strateške/operativne aktivnosti za narednu poslovnu godinu.
(4) Sadržaj obrasca:
   a) Kolona Strateški cilj banke - sadrži naziv i kratki opis cilja iz strategije banke, a za koji je dalje potrebna podrška iz informacionog sistema,
   b) Kolona Strateški cilj informacionog sistema - sadrži naziv i kratki opis cilja informacionog sistema, koji su navedeni u okviru usvojene Strategije informacionog sistema, a koji su povezani sa strateškim ciljevima banke,
   c) Kolona Operativni plan – projekt/aktivnost - sadrži projekte/aktivnosti navedene u okviru Operativnih planova, a koji proizilaze iz navedenog cilja u okviru Strategije informacionog sistema; ukoliko se određeni strateški cilj realizuje kroz više operativnih planova, potrebno je navesti pojedinačno sve operativne planove,
   d) Kolona Status - treba da sadrži status projekta/aktivnosti iz Operativnog plana na dan slanja izvještaja,
   e) Kolona Planirani vremenski rokovi projekta/aktivnosti - se sastoji od dvije podkolone (početak projekta/aktivnosti i kraj projekta/aktivnosti), a koji predstavljaju planirani vremenski period početka, odnosno završetka projekta/aktivnosti iz Operativnog plana,
   f) Kolona Realizovani vremenski rokovi projekta/aktivnosti - se sastoji od dvije podkolone (realizovani početak projekta/aktivnosti i realizovani kraj projekta/aktivnosti), a koji predstavljaju stvarni početak odnosno završetak aktivnosti u realizaciji.

Član 6.

Izvještaj Upravljanje rizicima informacionog sistema

(1) Izvještaj Upravljanje rizicima informacionog sistema sadrži sažetak godišnje procjene rizika informacionog sistema banke.
(2) Izvještaj se sastoji od jednog obrasca i to: BA 45.00 Plan tretiranja rizika informacionog sistema (RIS).
(3) Obrazac iz stava (2) ovog člana 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. U okviru navedenih kategorija, nabrojani su osnovni, ključni rizici. U slučaju dodatno identifikovanih rizika u okviru navedenih kategorija, potrebno je da banka doda identifikovani rizik u odgovarajuću kategoriju. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji se odnose na identifikovane rizike u okviru posljednje izvršene procjene rizika informacionog sistema, te statuse implementacije na zadnji dan kvartala za koji se dostavlja izvještaj.

(4) Sadržaj obrasca:
   a) Kolona Kategorija rizika - predstavlja šest ključnih kategorija rizika,
   b) Kolona Rizik - predstavlja naziv identifikovanog pojedinačnog rizika iz kategorije u koloni „Kategorija rizika“,
   c) Kolona Opis rizika - predstavlja detaljniji opis rizika, iz kolone II,
   d) Kolona Nivo rizika- predstavlja ocijenjeni nivo rizika od strane banke, 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,
   e) Kolona Način tretiranja rizika - predstavlja način tretiranja navedenog rizika od strane banke (na primjer: prihvaćen, umanjen, izbjegnut i slično),
   f) Kolona Opis mjere - predstavlja kratki opis poduzetih mjera za umanjenje rizika,
   g) Kolona Inicijalni planirani period implementacije mjere - predstavlja prvi definisani period kada je planirano da se mjera za navedeni rizik implementira, te je potrebno upisati kvartal i godinu,
   h) Kolona Produženi rok implementacije - predstavlja novi/nove rokove za implementaciju mjere u slučaju da vremenski rok u koloni „Inicijalni planirani period implementacije mjere“ nije ispoštovan, a ako se vremenski rok više puta pomjerao, sve podatke o pomjerenim vremenskim rokovima je potrebno upisati u koloni jedan ispod drugog u vidu kvartal/godina,
   i) Kolona Ukupni broj mjeseci kašnjenja od inicijalno predviđenog roka implementacije do završetka - predstavlja broj mjeseci kašnjenja implementacije definisane mjere, koji se računa od inicijalnog perioda navedenog u koloni „Inicijalni planirani period implementacije mjere“ do zadnjeg roka navedenog u koloni „Produženi rok implementacije“ (ako je u pitanju više rokova pomjeranja, računati prema zadnjem unesenom roku),
   j) Kolona Status - predstavlja status implementacije mjere na dan slanja izvještaja.

(5) Navedeni Obrazac 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.

Član 7.
Izvještaj Sigurnost informacionog sistema

(1) Izvještaj Sigurnost informacionog sistema sadrži informacije vezane uz rezultate penetracionih testiranja/testiranja ranjivosti.
(2) Izvještaj se sastoji od jednog obrasca i to: BA 46.00 Rezultati penetracionih testiranja/testova ranjivosti (PEN).
(3) Obrazac iz stava (2) ovog člana predstavlja pregled rizika identifikovanih penetracionim testiranjem/testom ranjivosti. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji su opisani u nastavku.
(4) Sadržaj obrasca:
   a) Kolona Jedinstvena oznaka penetracionog testa - predstavlja oznaku penetracionog testa, na način kako banka isti označava u svom sistemu,
   b) Kolona naziv izvještaja - predstavlja podatak o nazivu izvještaja u okviru kojeg su navedeni rizici,
   c) Kolona Interni test/eksterni test (naziv kompanije) - predstavlja podatak o tome da li je test interno izvršen (od strane uposlenika banke) ili eksterno od strane angažovane kompanije za koju je potrebno navesti naziv,
   d) Kolona Datum penetracionog testa - predstavlja datum/period kada je izvršen test,

e) Kolona Opis uočene slabosti/ranjivosti - definiše slabost, ranjivost odnosno rizik otkriven tokom navedenog testiranja; potrebno je navesti odvojeno u svakom redu tablice sve uočene rizike; Kolone navedene od a) do d) je potrebno upisati jednom za određeni penetracioni test, dok kolone navedene od e) do l) treba da sadrže detalje u vezi svih identifikovanih slabosti. Dakle, kolone od e) do l) se ponavljaju više puta za jedan odrađeni penetracioni test, u ovisnosti o broju identifikovani slabosti,
f) Kolona 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 ocjena nivoa rizika u okviru urađenog testa razlikuje od prethodno navedene, potrebno je da banka izvrši adekvatno mapiranje i transformaciju ocjena u prethodno navedene ocjene od 1 do 4,
g) Kolona Način tretiranja rizika - predstavlja način tretiranja rizika od strane banke (na primjer: umanjenje, prihvatanje, transfer i potpuno otklanjanje),
h) Kolona Opis mjere za umanjenje - predstavlja opis tretiranja rizika odnosno mjere koju će banka poduzeti na umanjenju rizika,
i) Kolona Planirani inicijalni period implementacije - predstavlja inicijalno definisani rok za umanjenje identifikovanog rizika, gdje je potrebno upisati kvartal i godinu,
j) Kolona Eventualno produženje roka - predstavlja novi rok implementacije mjere u slučaju da inicijalni iz kolone „Planirani inicijalni period implementacije“ nije zadovoljen, ako se rok više puta produžava potrebno je navesti i sve prethodne rokove u obliku kvartala i godine,
k) Kolona Završetak implementacije – predstavlja podatak kada je završeno implementiranje mjere, predstavljeno u obliku kvartala i godine,
l) Kolona Trenutni status izvršenja - predstavlja status implementacije mjere (na primjer: otvoren, zatvoren i u toku) na dan slanja izvještaja.

(5) Obrazac BA 46.00 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.

(6) Obrazac BA 46.00 je potrebno dostavljati Agenciji za sve penetracione testove/testove ranjivosti dok se sve identifikovane slabosti odnosno rizici ne zatvore (mjere implementiraju), odnosno dok se ne postupi u skladu sa usvojenom odlukom o tretiranju rizika.

Član 8.
Izvještaj Interna revizija

(1) Izvještaj Interna revizija sadrži podatke o planiranim i provedenim revizijama, kao i praćenju nalaza od strane interne revizije informacionog sistema banke.

(2) Izvještaj se sastoji od dva obrasca:
a) BA 47.01 Pregled planiranih i provedenih revizija informacionog sistema (ITR1) i
b) BA 47.02 Pregled preporuka/naloga revizije informacionog sistema (ITR2).

(3) Obrazac BA 47.01 Pregled planiranih i provedenih revizija informacionog sistema (ITR1) sadrži podatke o planiranim i provedenim revizijama informacionog sistema. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji se odnose na sve planirane i izvršene revizije za kvartal za koji se dostavlja, kao i za godinu kojoj navedeni kvartal pripada.

(4) Sadržaj obrasca:
a) Kolona Oblast IS po regulativi - navodi naziv oblasti revizije informacionog sistema kojoj oblast pripada u skladu sa važećom regulativom Agencije,
b) Kolona Oblast revizije informacionog sistema po metodologiji banke - predstavlja naziv oblasti revizije u skladu da metodologijom/matricom banke, a koje korespondiraju definisanim oblastima po regulativi u koloni I, te je isto potrebno popuniti za sve oblasti, a ne samo one koje su planirane u kvartalu za koji se obrazac dostavlja,

c) Kolona Jedinstvena oznaka predmetne revizije - predstavlja jedinstvenu identifikaciju revizije za koju će se obaviti revizija navedene oblasti, te se popunjava za revizije koje su izvršene u kvartalu za koji se obrazac dostavlja,
d) Kolona Revizijski ciklus - predstavlja izračunati revizijski ciklus za datu oblast u skladu sa procjenom u okviru metodologije banke (da li se revizija navedene oblasti obavlja svake godine, jednom u dvije ili jednom u tri godine), te se popunjava za sve oblasti,
e) Kolona Oblast uključena u period za koji se dostavlja izvještaj DA/NE - predstavlja oznaku da li je definisana oblast sadržana u planu revizije za kvartal u kojem se izvještaj dostavlja,
f) Kolona Detaljniji opis predmeta, cilja i opsega revizije - predstavlja detaljniji opis, ciljeve i opseg revizije, te se popunjava za oblasti za koje je revizija izvršena u kvartalu za koje se obrazac dostavlja,
g) Kolona Trajanje revizije - se sastoji od dvije podkolone u kojima je naveden realizovani period provođenja revizije odnosno početak i kraj revizijskih aktivnosti, te se popunjava za oblasti za koje je revizija izvršena u kvartalu za koji se obrazac dostavlja,
h) Kolona Ocjena oblasti - predstavlja ocjenu navedene oblasti od strane internog revizora informacionog sistema, u skladu sa vlastitom metodologijom interne revizije informacionog sistema banke, te se popunjava za oblasti za koje je revizija izvršena u kvartalu za koji se obrazac dostavlja,
i) Kolona Poslovna godina kada je oblast zadnji put revidirana - predstavlja godinu kada je zadnji put izvršena revizija navedene oblasti (potrebno popuniti za sve oblasti).

(5) Obrazac BA 47.02 Pregled preporuka/naloga revizije informacionog sistema (ITR2) sadrži podatke o svim uočenim nedostacima odnosno izdatim preporukama u okviru izvještaja revizije informacionog sistema, zajedno sa pratećim mjerama za korekciju, rokovima za implementaciju mjera i stepenom realizacije. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji se odnose sve uočene slabosti u okviru navedenih revizija. Podatke o uočenoj slabosti i identifikovanim mjerama je potrebno uključiti u obrazac sve do momenta implementacije mjere odnosno izvršenja preporuke/naloga. Dakle, obrazac treba da sadrži sve preporuke/naloge revizije koji nisu potpuno zatvoreni na zadnji dan kvartala za koji se dostavlja izvještaj, kao i sve ostale preporuke/naloge koji su izdati u okviru predmetne poslovne godine na koju se izvještavanje odnosi.

(6) Sadržaj obrasca:
a) Kolona Jedinstvena oznaka predmetne revizije - predstavlja jedinstvenu identifikaciju predmetne revizije,
b) Kolona Vrsta revizije - sadrži podatak o tome da li je preporuka/nalog izdata od strane interne revizije, eksterne revizije ili Agencije,
c) Kolona Datum izdavanja preporuke/naloga - sadrži podatak o datumu kada je preporuka/nalog izdata,
d) Kolona Preporuka/nalog - sadrži kratak opis uočenog nedostatka, slabosti i/ili rizika u provedenoj reviziji,
e) Kolona 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,
f) Kolona Mjere za korekciju - sadrži kratak opis preporučene mjere za otklanjanje odnosno umanjenje uočenih rizika,
g) Kolona Inicijalni rok za implementaciju mjere - predstavlja definisani inicijalni/prvi rok za implementaciju mjere,
h) Kolona Eventualno produženje roka za implementaciju mjere - predstavlja novi rok implementacije mjere u slučaju da inicijalni rok iz kolone „Inicijalni rok za implementaciju

mjere“ nije zadovoljen, ako se rok više puta produžava potrebno je navesti i sve prethodne rokove,

i) Kolona Ukupni broj mjeseci od roka za implementaciju do datuma izvršenja - predstavlja ukupni broj proteklih mjeseci, koji se računa od inicijalnog perioda navedenog u koloni „Inicijalni rok za implementaciju mjere„ do zadnjeg roka navedenog u koloni „Eventualno produženje roka za implementaciju mjere“ (ako je u pitanju više rokova produženja, računati prema zadnjem unesenom roku),
j) Kolona Praćenje izvršenja mjere (follow-up) – opis - sadrži podatke o provedenom praćenju izvršenja naložene mjere,
k) Kolona Status izvršenja mjere - sadrži status izvršenja mjere (otvoren, zatvoren ili u toku) na dan slanja izvještaja.

(7) Obrazac BA 47.02 treba da sadrži podatke o praćenju izvršenja naloženih mjera od strane interne revizije informacionog sistema banke, eksterne revizije informacionog sistema, odnosno izdatih naloga Agencije koji se odnose na kontrolu informacionog sistema banke.
(8) Obrasce BA 47.01 i BA 47.02 je potrebno popuniti bez obzira da li se interna revizija informacionog sistema obavlja od strane internog revizora informacionog sistema banke ili eksternalizovanog internog revizora informacionog sistema.

Član 9.
Izvještaj Budžet informacionog sistema

(1) Izvještaj Budžet informacionog sistema sadrži podatke o ukupnom budžetu banke, kao i o planiranim i realizovanim budžetima za definisana područja informacionog sistema i FinTech.
(2) Izvještaj se sastoji od dva obrasca:
a) BA 48.01 Budžet informacionog sistema (BIS1) i
b) BA 48.02 Budžet FinTech (BIS2).
(3) Obrazac BA 48.01 Budžet informacionog sistema (BIS1) sadrži podatke o planiranom i realizovanom godišnjem budžetu banke za definisana područja informacionog sistema. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji uključuju troškove i investicije koje se odnose na resurse informacionog sistema, za kalendarsku godinu sa stanjem na dan slanja izvještaja, kao i planiranom usvojenom budžetu za narednu godinu.
(4) Sadržaj obrasca:
a) Kolona Opis - sadrži oblasti: licence, software, hardware, komunikacione linije i ostalo, za koje je potrebno popuniti pojedinačne nazive; u slučaju ostalih troškova/investicija, potrebno je da banka navede pod Ostalo i naziv investicije/troška,
b) Kolona Vrsta - sadrži podatak da li je navedena stavka trošak ili investicija,
c) Kolona JIB pružaoca usluga – popunjava se u slučaju da se trošak/investicija odnose na eksternog pružaoca usluge/dobavljača i predstavlja Jedinstveni identifikacioni broj pružaoca usluge,
d) Kolona Naziv pružaoca usluga – dobavljača - predstavlja informaciju o nazivu pružaoca usluge/ dobavljača i popunjava se u slučaju da se navedeni trošak/investicija plaća eksternom pružaocu usluge/dobavljaču,
e) Kolona Eksternalizacija - predstavlja podatak o tome da li se navedeni trošak/investicija odnosi na aktivnost koja je eksternalizovana, te je na isto potrebno odgovoriti sa DA ili NE,
f) Kolona Planirano u - predstavlja podatak o planiranom budžetu za godinu za koju se godišnji izvještaj popunjava (izvještajnu godinu), a sastoji se od dvije podkolone u koje se za svaku od aktivnosti unosi planirani iznos u zavisnosti da li je interni ili eksterni trošak/investicija; iznos se unosi u KM valuti,
g) Kolona Realizovano u - predstavlja podatak o realizovanom budžetu za godinu za koju se godišnji izvještaj popunjava (izvještajnu godinu), a sastoji se od dvije podkolone u koje se

za svaku od stavki unosi realizovani iznos u zavisnosti da li je interni ili eksterni trošak/investicija; iznos se unosi u KM valuti,

h) Kolona Planirano u 1. godini - predstavlja podatak o planiranom budžetu za narednu godinu, a sastoji se od dvije podkolone u koje se za svaki trošak/investiciju unosi planirani iznos u zavisnosti da li je interni ili eksterni trošak/investicija; iznos se unosi u KM valuti.

(5) Godine koje se nalaze u kolonama pod f), g) i h) se automatski popunjavaju, nakon što se unese izvještajna godina u zaglavlju obrasca.

(6) Ukupan iznos budžeta za informacioni sistem banke se automatski zbraja na kraju tabele, dok je ukupni iznos budžeta banke potrebno upisati u odgovarajuća polja za red „Ukupni budžet banke“.

(7) Obrazac BA 48.02 Budžet FinTech (BIS2) sadrži podatke o FinTech aktivnostima koje je banka pokrenula ili namjerava pokrenuti u narednoj poslovnoj godini, te planiranom/realizovanom budžetu za navedene aktivnosti. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji se odnose na planirani i realizovani budžet i aktivnosti u godini za koju se dostavlja izvještaj, kao i podatke o postojećim i planiranim FinTech aktivnostima u narednoj poslovnoj godini.

(8) Sadržaj obrasca:

a) Kolona Naziv - predstavlja naziv FinTech aktivnosti,

b) Kolona Vrsta FinTech-a - predstavlja vrstu FinTech aktivnosti, gdje je potrebno izabrati jednu od ponuđenih vrsta, odnosno upisati vrstu aktivnosti u slučaju da se ne nalazi u ponuđenoj listi,

c) Kolona Naziv pružaoca usluge/dobavljača - sadrži podatak o nazivu pružaoca usluge/dobavljača FinTech aktivnosti,

d) Kolona Vrsta odnosa sa pružaocem usluge - sadrži podatak o vrsti usluge koju banka ima sa pružaocem usluga po pitanju navedene FinTech aktivnosti, te je istu potrebno izabrati iz ponuđene liste,

e) Kolona Poslovni proces koji FinTech podržava - sadrži podatak o procesu koji je podržan navedenom FinTech aktivnošću, te je potrebno navesti naziv jednog ili više poslovnih procesa,

f) Kolona Status - sadrži podatak o statusu na dan slanja izvještaja koji može biti: potpuno implementirano, testna faza, razvojna faza, u planu i bez iskustva,

g) Kolona Datum početka pružanja usluge u produkciji – sadrži podatak o datumu kada je banka krenula s pružanjem usluge u produkciji,

h) Kolona Budžet u - sadrži podatak o budžetu za navedenu FinTech aktivnosti za godinu za koju se godišnji izvještaj popunjava (izvještajnu godinu), a sastoji se od dvije podkolone u koje se za svaku od stavki unosi iznos planiranog budžeta i iznos realizovanog budžeta; iznos se unosi u KM valuti,

i) Kolona Planirano u 1. godini (KM) - sadrži podatak o planiranom budžetu za navedenu FinTech aktivnosti za narednu godinu; iznos se unosi u KM valuti,

j) Kolona Kratak opis - predstavlja kratak opis navedene aktivnosti.

(9) Godine koje se nalaze u kolonama pod h) i i) se automatski popunjavaju, nakon što se unese izvještajna godina u zaglavlju obrasca.

Član 10.
Izvještaj Značajne promjene u informacionom sistemu banke

(1) Izvještaj Značajne promjene u informacionom sistemu banke sadrži podatke o značajnim izmjenama u okviru informacionog sistema banke.

(2) Izvještaj se sastoji od jednog obrasca i to: BA 49.00 Značajne promjene u informacionom sistemu banke (PIS).

(3) Obrazac iz stava (2) ovog člana sadrži podatke o značajnim promjenama u okviru informacionog sistema banke (na primjer: software-ske aplikacije, hardware-ske, mreža i

drugo), bez obzira da li su iste planirane ili ne. Obrazac se dostavlja na kvartalnom nivou i sadrži sve izmjene koje su se desile (započete, u toku, završene), a u okviru kvartala za koji se izvještava.

(4) Sadržaj obrasca:
   a) Kolona Dio informacionog sistema - sadrži podatke o nazivu dijela informacionog sistema na koji se odnosi izmjena (na primjer, ključna bankarska aplikacija, elektronsko bankarstvo, operativni sistem, aplikacije za podršku, hardware, mreža i slično),
   b) Kolona Opis izmjene - sadrži kratak opis izmjene,
   c) Kolona Hitnost izmjene - sadrži podatak da li je izmjena bila hitna ili planirana,
   d) Kolona Način promjene - sadrži podatak o tome da li je izmjena izvršena interno od strane uposlenika banke ili eksterno od strane pružaoca usluga,
   e) Kolona Status - sadrži podatak o statusu izmjene (završena, u toku ili u pripremi odnosno da li je otkazana).

(5) Obrazac 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 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 obrazaca:
   a) BA 50.01 Kategorizacija incidenata (INC1),
   b) BA 50.02 Broj incidenata/zastoja po poslovnim procesima (INC2),
   c) BA 50.03 Broj prema vrstama incidenata (INC3),
   d) BA 50.04 Cyber incidenti (INC4) i
   e) BA 50.05 Elektronsko bankarstvo i kartično poslovanje – moguće zloupotrebe (INC5).

(3) Obrazac BA 50.01 Kategorizacija incidenata (INC1) definiše nivoe incidenata. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji se odnose na nivo incidenta 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 ocjena u prethodno navedene ocjene od I do IV, te u slučaju više od 4 nivoa, izvještava o incidentima iz najviša 4 nivoa. U okviru izvještaja potrebno je navesti naziv svake od kategorija I-IV, kao i definisano očekivano vrijeme rješavanja incidenta.

(4) BA 50.02 Broj incidenata/zastoja po poslovnim procesima (INC2) sadrži pregled incidenata po definisanim poslovnim procesima. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke o incidentima koji su se desili u kvartalu za koji se izvještaj dostavlja.

(5) Sadržaj obrasca:
   a) Kolona IT segment – predstavlja IT segmente za koje je moguće da se desi incident/zastoj. U slučaju da se desio incident/zastoj u IT segmentu koji nije naveden, potrebno je upisati podatak pod opcijom „druge poslovne aplikacije“, te u koloni II navesti naziv poslovnog procesa,
   b) Kolona Poslovni proces – predstavlja poslovne procese koji su navedeni za IT segment „ključna bankarska aplikacija“, gdje je iz liste padajućeg menija potrebno izabrati poslovni proces na koji je incident uticao zastojem,
   c) Kolona Kritični/ključni poslovni proces i IT segment – potrebno označiti da li je poslovni proces/IT segment za koji se desio zastoj kritični/ključni poslovni proces u banci (DA ili NE),
   d) Kolona Eksternalizacija – sadrži podatak o tome da li je IT podrška odnosno sam poslovni proces/IT segment eksternalizovan, izborom jedne od ponuđenih opcija (materijalno značajna, nije materijalno značajna, nije eksternalizacija),

e) Kolone Broj incidenata po kategorijama incidenta – od I do IV, sadrže podatak o tome koliko incidenata se desilo za navedeni poslovni proces/IT segment, u skladu sa kategorizacijom incidenata,
f) Kolona Ukupno – predstavlja ukupan broj incidenata za sve četiri prethodne kategorije, koji je zabilježen za odgovarajući poslovni proces/IT segment; polje se računa automatski,
g) Kolona Broj problema/zastoja koji nisu kategorisani kao incidenti - predstavlja podatak o broju prekida koji su se desili, a nisu kategorisani kao incidenti koji pripadaju jednoj od 4 navedene kategorije,
h) Kolona Ukupno vrijeme prekida rada procesa – predstavlja ukupno vrijeme prekida obavljanja određenog poslovnog procesa/IT segmenta uslijed zabilježenih incidenata, te se prikazuje u minutama,
i) Kolona Broj afektiranih transakcija – potrebno upisati broj transakcija u okviru navedenog poslovnog procesa/IT segmenta na koje su navedeni incidenti imali uticaj, na primjer, broj transakcija koje se nisu izvršile, broj transakcija koje su bile u zastoju, broj pogrešnih transakcija i slično,
j) Kolona Iznos afektiranih transakcija (KM) – potrebno upisati ukupni novčani iznos za broj afektiranih transakcija koje su upisane u koloni pod i); iznos se unosi u KM valuti,
k) Kolona Broj afektiranih klijenata – potrebno upisati broj klijenata na koje je zastoj/prekid uticao,
l) Kolona Broj afektiranih poslovnih jedinica – potrebno upisati broj poslovnih jedinica na koje je zastoj/prekid uticao,
m) Kolona Uticaj na reputacioni rizik – podatak o tome da li su zastoji/prekidi imali uticaja na reputacioni rizik banke (DA ili NE),
n) Kolona Broj incidenata koji su imali uticaja na reputacioni rizik – ako je odgovor u koloni pod m) DA, onda je potrebno popuniti broj incidenata koji je imao uticaj na reputacioni rizik,
o) Kolona Broj rješenih incidenata – podatak o broju incidenata koji su riješeni od strane uposlenika banke i broj incidenata koji su riješeni eksterno od strane pružaoca usluga, za svaki od navedenih procesa,
p) Kolona Ukupni iznos gubitka prouzrokovan incidentom (KM) – predstavlja podatak o finansijskom gubitku koji je prouzrokovan incidentom uslijed nedostupnosti/sporosti sistema odnosno poslovnog procesa; iznos se unosi u KM valuti,
q) Kolona Napomena/opis – sadrži napomenu u slučaju potrebe za dodatnim informacijama od strane banke.

(6) Obrazac BA 50.03 Broj prema vrstama incidenata (INC3) sadrži broj incidenata prema definisanim vrstama incidenata. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji su opisani u nastavku.

(7) Sadržaj obrasca:
a) Kolona Operativni incidenti – predstavlja operativne incidente po kategorijama koje su dalje razrađene u pod kategorije,
b) Kolone Broj incidenata kategorije – od I do IV, sadrže podatak o tome koji broj incidenata se desio za navedeni operativni incident, gdje je prema kategorizaciji incidenta potrebno popuniti odgovarajuću kolonu,
c) Kolona Ukupno – predstavlja ukupan broj incidenata za sve četiri kategorije, koji je zabilježen za odgovarajući poslovni proces, računa se automatski,
d) Kolona Broj incidenata kod pružaoca usluga - predstavlja broj operativnih incidenata koji su se desili kod pružaoca usluga, a koji su imali uticaj na cjelokupni informacioni sistem banke,
e) Kolona Broj događaja koji nisu klasifikovani kao incidenti - predstavlja podatak o broju događaja koji se desio, a nisu kategorisani kao incidenti,

f) Kolona Finansijski gubitak uslijed incidenta (KM) – sadrži podatak o finansijskom gubitku koji su navedeni incidenti uzrokovali,
g) Kolona Vremenski period trajanja incidenta – sadrži podatak o tome koliko dugo vremenski su navedeni incidenti trajali, izraženo u minutama,
h) Kolona Broj pogođenih klijenata – potrebno upisati broj klijenata na koje su navedeni incidenti uticali,
i) Kolona Uticaj na kritični/ključni proces – potrebno označiti da li su incidenti koji su se desili, uticali na rad kritičnog/ključnog poslovnog procesa (DA ili NE) i
j) Kolona Napomena/opis – u slučaju uticaja na kritični/ključni proces, navesti nazive svih procesa na koje su navedeni incidenti imali uticaj.

(8) Obrazac BA 50.04 Cyber incidenti (INC4) sadrži broj cyber incidenata prema definisanim vrstama incidenata. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji su opisani u nastavku.

(9) Sadržaj obrasca:
a) Kolona Kategorija – predstavlja kategorije sigurnosnih incidenata za koje je potrebno popuniti podatke,
b) Kolona Vrsta napada/prijetnji – sadrži listu napada/prijetnji od kojih je potrebno izabrati jednu,
c) Kolona Broj detektovanih pokušaja – potrebno upisati broj pokušaja koji je detektovan za navedenu vrstu i kategoriju napada; u slučaju velikog broja detektovanih pokušaja, nije neophodno da banka upiše tačan broj, dovoljno je okvirno,
d) Kolona Broj realizovanih napada u okviru sistema banke – sadrži podatak o broju napada koji su realizovani u okviru banke i imali su uticaj na cjelokupni informacioni sistem,
e) Kolona Broj realizovanih napada u okviru pružaoca usluga – sadrži podatak o broju napada koji su realizovani u okviru pružaoca usluga i imali su uticaj na cjelokupni informacioni sistem banke,
f) Kolona Vrijeme nedostupnosti sistema – podatak o vremenu trajanja nedostupnosti sistema izazvanog napadima, prikazan u minutama,
g) Kolona Finansijski gubitak uslijed incidenta (KM) – predstavlja podatak o finansijskom gubitku izazvanom napadima; iznos se unosi u KM valuti,
h) Kolona Broj afektiranih klijenata – potrebno upisati broj klijenata na koje su navedeni napadi imali uticaj i
i) Kolona Napomena/opis – sadrži dodatni podatak ako banka ima potrebnu da navede.

(10) Obrazac BA 50.05 Elektronsko bankarstvo i kartično poslovanje – moguće zloupotrebe (INC5) sadrži incidente koji se odnose na moguće zloupotrebe sistema elektronskog bankarstva i kartičnog poslovanja. Ovdje je potrebno naglasiti da se radi o zlonamjernim transakcijama uslijed slabosti informacionog sistema, kao npr. posljedica hakerskih napada i slično. Obrazac se dostavlja na kvartalnom nivou i sadrži podatke koji su opisani u nastavku.

(11) Sadržaj obrasca:
a) Kolona Vrsta događaja – predstavlja vrste događaja za koje je potrebno popuniti podatke, gdje se prikazani statusi događaja koji se odnose na zloupotrebe otkrivene od strane banke ili prijavljene od strane korisnika; status otvoren - označava transakcije koje još nisu provedene, a označene su kao potencijalne zloupotrebe sistema; status transakcija obavljena – označava transakcije za koje je utvrđeno da su bile zloupotrebe sistema, a transakcije su provedene; status odbijen - označava transakcije za koje su pravovremeno uočene zloupotrebe te transakcija nije provedena do kraja, odnosno spriječeno je izvršenje transakcije; status neriješeno – označava transakcije za koje je uočeno da su bile zloupotrebe ali imaju neriješen status odnosno analiza transakcije je još u toku; status neusaglašen – označava transakcije za koje postoji neusaglašen stav banke i korisnika o zloupotrebi sistema,

b) Kolona Broj transakcija u elektronskom bankarstvu – sadrži broj transakcija koje su se za određene vrste događaja iz kolone I desile u elektronskom bankarstvu,
c) Kolona Iznos (KM) – predstavlja iznos za odgovarajuću vrstu događaja koja se desila u elektronskom bankarstvu; iznos se unosi u KM valuti,
d) Kolona Broj transakcija u kartičnom poslovanju – sadrži broj transakcija koje su se za određene vrste događaja iz kolone I desile u kartičnom poslovanju,
e) Kolona Iznos (KM)– predstavlja iznos za odgovarajuću vrstu događaja koja se desila u kartičnom poslovanju; iznos se unosi u KM valuti.

Član 12.

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 dva obrasca:
a) BA 51.01 Obim elektronskog bankarstva (EB1) i
b) VA 51.02 Sredstva autentifikacije i autorizacije u sistemu elektronskog bankarstva (EB2).
(3) Obrazac BA 51.01 Obim elektronskog bankarstva (EB1) 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, gdje se iznosi unosi u KM valuti. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.
(4) Sadržaj obrasca:
a) Kolona predstavlja vrste prometa, kao i učešće prometa elektronskog i mobilnog bankarstva u ukupnom platnom prometu na nivou banke,
b) Kolonu Broj klijenata - predstavlja broj klijenata na dan izvještavanja za pravna lica,
c) Kolona Realizovane transakcije UPP - se sastoji od dvije podkolone: realizovane transakcije UPP – kolona 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 (KM) koja sadrži podatak o realizovanim iznosima transakcijama za pravna lica u domaćem platnom prometu za period kalendarske godine za koju se izvještava,
d) Kolona Realizovane transakcije IPP - se sastoji od dvije podkolone: realizovane transakcije IPP – kolona 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 (KM) koja sadrži podatak o realizovanim iznosima transakcijama za pravna lica u ino platnom prometu za period kalendarske godine za koju se izvještava.
e) Kolone pod d) sa svojim podkolonama se ponavljaju za podatke o fizičkim licima, dok se u podkolonama kolone ukupno vrši automatsko računanje iz kolona pravnih i fizičkih lica.
(5) Obrazac BA 51.02 Sredstva autentifikacije i autorizacije u sistemu elektronskog bankarstva (EB2) sadrže podatke o načinima autentifikacije i autorizacije koje banka koristi u sistemu elektronskog odnosno mobilnog bankarstva, za fizička i pravna lica. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.
(6) Sadržaj obrasca:
a) Kolona Naziv sistema - sadrži podatak o nazivu sistema elektronskog ili mobilnog bankarstva koje banka pruža svojim klijentima,
b) Kolona Naziv pružaoca usluga u slučaju eksternalizacije - sadrži naziv pružaoca usluga sistema elektronskog ili mobilnog bankarstva,
c) Kolona Vrsta elektronskog bankarstva - sadrži podatak o vrsti elektronskog bankarstva (na primjer: elektronsko bankarstvo za fizička lica, elektronsko bankarstvo za pravna lica, mobilno bankarstvo za fizička lica i slično),
d) Kolona Vrsta klijenta - sadrži podatak da li je klijent pravno lice (PL) ili fizičko lice (FL),

e) Kolona Način autentifikacije - se sastoji od četiri podkolone: Element autentifikacije broj 1 koji sadrži predefinisane elemente autentifikacije (na primjer: pametna kartica + PIN, USB certifikat + PIN, jednokratna lozinka OTP i slično), te Broj klijenata (fizička i pravna lica) u koje je potrebno unijeti podatak o broju fizičkih odnosno pravnih lica na dan izvještavanja, zatim Element autentifikacije broj 2 i njegov broj klijenata,
f) Kolona Način autorizacije - se sastoji od dvije podkolone: element autorizacije koji se bira iz ponuđene liste i broj klijenata koji koristi taj element autorizacije.

Član 13.
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 dva obrasca:
   a) BA 52.01 Obim kartičnog poslovanja (KP1) i
   b) BA 52.02 Broj POS i ATM uređaja (KP2).
(3) Obrazac BA 52.01 Obim kartičnog poslovanja (KP1) sadrži podatke o obimu (broju i iznosu transakcija) kartičnog poslovanja za fizička i pravna lica, gdje se iznos unosi u KM valuti. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.
(4) Sadržaj obrasca:
   a) Kolona Brend/vrsta kartice - predstavlja brend i vrstu kartice koji se koristi u banci,
   b) Kolona Pravna lica - se sastoji od dvije podkolone: broj kartica - koja sadrži podatak o broju kartica za pravna lica na dan izvještavanja i iznos transakcija (KM) - koja sadrži podatak o ukupnom iznosu transakcija za pravna lica za period kalendarske godine za koju se izvještava,
   c) Kolona Fizička lica - se sastoji od dvije podkolone: broj kartica - koja sadrži podatak o broju kartica za fizička lica na dan izvještavanja i iznos transakcija (KM) - koja sadrži podatak o ukupnom iznosu transakcija za fizička lica za period kalendarske godine za koju se izvještava.
(5) Obrazac BA 52.02 Broj POS i ATM uređaja (KP2) sadrži podatke o broju POS i ATM uređaja u banci i izvan banke. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.
(6) Sadržaj obrasca:
   a) Kolona Vrsta uređaja - sadrži vrste uređaja za koje se izvještava,
   b) Kolona Broj uređaja u banci - sadrži podatak o broju uređaja u banci na dan izvještavanja,
   c) Kolona Broj uređaja izvan banke - sadrži podatak o broju uređaja izvan banke na dan izvještavanja,
   d) Kolona Ukupno – podatak u koloni se automatski računa.

Član 14.
Izvještaj Upotreba novih tehnologija

(1) Izvještaj Upotreba novih tehnologija sadrži podatke o novim FinTech tehnologijama koje banka koristi u svojim poslovnim procesima.
(2) Izvještaj se sastoji od jednog obrasca i to: Obrazac BA 53.01 Obim korištenja novih tehnologija – FinTech (OFT).
(3) Obrazac iz stava (2) ovog člana sadrži podatke o vrstama novih tehnologija, poslovnim procesima koje podržavaju te broju i iznosu transakcija ostvarenom u toku izvještajne godine. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.
(4) Sadržaj obrasca:
   a) Kolona Naziv - predstavlja naziv nove tehnologije,
   b) Kolona Vrsta nove tehnologije - potrebno iz liste izabrati vrstu nove tehnologije,
   c) Kolona Kratak opis - sadrži opis nove tehnologije,

d) Kolona Poslovni proces koji podržava - sadrži podatak o poslovnom procesu koji je podržan novom tehnologijom,
e) Kolona Broj transakcija - predstavlja broj transakcija koji je u izvještajnoj godini obavljen sa navedenom novom tehnologijom, ako je primjenjivo,
f) Kolona Iznos transakcija (KM) - predstavlja novčani iznos obavljenih transakcija u izvještajnoj godini, ako je primjenjivo; iznos se unosi u KM valuti.

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 obrasca:
a) BA 54.01 BCM - Načini testiranja (BCM1),
b) BA 54.02 BCM - Scenariji za testiranje (BCM 2),
c) BA 54.03 BCM - Testirani poslovni procesi (BCM3) i
d) BA 54.04 BCM - Ostali podaci o oporavku informacionog sistema (BCM4).
(3) Obrazac BA 54.01 BCM - Načini testiranja (BCM1) sadrži podatke o načinima testiranja, uključenosti centrale banke u testiranje, kao i o broju uključenih poslovnih jedinica. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.
(4) Sadržaj obrasca:
a) Kolona Predmet - sadrži podatke koji se odnose na način testiranja plana kontinuiteta poslovanja,
b) Kolona Odabrati/upisati odgovor – za svaki od podataka iz kolone I sadrži listu ponuđenih odgovora, izuzev za podatak koji zahtjeva broj.
(5) Obrazac BA 54.02 BCM - Scenariji za testiranje (BCM2) sadrži podatke o scenarijima testiranja funkcionalnosti rezervnog informatičkog centra. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.
(6) Sadržaj obrasca:
a) Kolona Scenarij - sadrži scenarije testiranja,
b) Kolona DA/NE - je potrebno unijeti podatak da li je navedena vrsta scenarija bila uključena u predmetno testiranje i
c) Kolona Datum zadnjeg testiranja navedenog scenarija- predstavlja podatak gdje je za svaki od scenarija iz kolone pod a) (bez obzira da li je scenarij bio uključen u zadnje testiranje) potrebno upisati datum zadnjeg testiranja.
(7) Obrazac BA 54.03 BCM - Testirani poslovni procesi (BCM3) 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 i RPO parametrima. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji su opisani u nastavku.
(8) Sadržaj obrasca:
a) Kolona Poslovni proces i IKT sistem koji ih podržava - sadrži podatke o najčešćim poslovnim procesima unutar banke,
b) Kolona DA/NE - sadrži podatak da li je navedeni poslovni proces bio uključen u predmetno testiranje,
c) Kolona Kritičan/ključan - sadrži podataka o tome da li je poslovni proces koji je naveden u koloni I definisan kao kritičan/ključan proces, gdje je na isti potrebno odgovoriti sa DA ili NE,
d) Kolona Definisani RTO - predstavlja podatak o prihvatljivom vremenu neraspoloživosti poslovnog procesa banke koji je definisan Analizom uticaja na poslovanje,
e) Kolona Definisani RPO - predstavlja podatak o prihvatljivom gubitku podataka u slučaju prekida operacija koji je definisan Analizom uticaja na poslovanje,

f) Kolona Ostvareni RTO - predstavlja podatak o RTO vremenu koji je za navedeni poslovni proces ostvaren u toku testiranja.

(9) Obrazac BA 54.04 BCM - Ostali podaci o oporavku informacionog sistema (BCM4) sadrži ostale potrebne podatke o oporavku informacionog sistema. Obrazac se dostavlja na godišnjem nivou i sadrži podatke koji se odnose na: obuhvaćenost poslovnih procesa prilikom testa, korištenost resursa sa primarnog informatičkog centra prilikom testiranja, lokaciju primarnog/rezervnog/lokalnog informatičkog centra, vrstu rezervnog informatičkog centra, učestalost testiranja sa kopija podataka i učestalost osvježavanja podataka na rezervnom informatičkom centru

(10) Sadržaj obrasca:
a) Kolona Predmet - sadrži podatke o kojima je potrebno izvještavati Agenciju,
b) Kolona Odabrati/upisati - za pitanja pod rednim brojevima 1-4 sadrži predefinisane odgovore koje je potrebno odabrati,
c) Kolona Objašnjenje - sadrži objašnjenje u slučaju da banka ima potrebu isto upisati.

III ROKOVI ZA IZVJEŠTAVANJE

Član 16.
Rokovi izvještavanja

(1) Banka je dužna da godišnje (kalendarski), a najkasnije do 05. marta naredne godine za prethodnu godinu, dostavlja Agenciji sljedeće izvještajne obrasce:
a) Obrazac BA 42.01 - Opšti podaci o organizacionoj strukturi (OP1),
b) Obrazac BA 42.02 - Opšti podaci o odgovornim osobama (OP2),
c) Obrazac BA 42.05 - Opšti podaci o internoj reviziji informacionog sistema (OP5),
d) Obrazac BA 43.01 - Resursi IT - infrastruktura (RIT1),
e) Obrazac BA 43.02 - Resursi IT - serveri (RIT2),
f) Obrazac BA 43.03 - Resursi IT - mrežni uređaji (RIT3),
g) Obrazac BA 43.04 - Resursi IT - radne stanice (RIT4),
h) Obrazac BA 43.05 - Resursi IT - bankomati (RIT5),
i) Obrazac BA 43.06 - Resursi IT - podrška (RIT6),
j) Obrazac BA 43.07 - Resursi IT - udaljeni pristup (RIT7),
k) Obrazac BA 44.00 - Strateški i operativni ciljevi (SOP),
l) Obrazac BA 48.01 - Budžet informacionog sistema (BIS1),
m) Obrazac BA 48.02 - Budžet FinTech (BIS2),
n) Obrazac BA 50.01 - Kategorizacija incidenata (INC1),
o) Obrazac BA 51.01 - Obim elektronskog bankarstva (EB1),
p) Obrazac BA 51.02 - Sredstva autentifikacije i autorizacije u sistemu elektronskog bankarstva (EB2),
q) Obrazac BA 52.01 - Obim kartičnog poslovanja (KP1),
r) Obrazac BA 52.02 - Broj POS i ATM uređaja (KP2),
s) Obrazac BA 53.01 - Obim korištenja novih tehnologija (OFT),
t) Obrazac BA 54.01 - BCM - Način testiranja (BCM1),
u) Obrazac BA 54.02 - BCM - Scenariji testiranja (BCM2),
v) Obrazac BA 54.03 - BCM - Testirani poslovni procesi (BCM3) i
w) Obrazac BA 54.04 - BCM - Ostali podaci o oporavku informacionog sistema (BCM4).

(2) Banka je dužna da kvartalno (kalendarski), a najkasnije do kraja narednog mjeseca po isteku kvartala, dostavlja Agenciji sljedeće izvještajne obrasce:
a) Obrazac BA 42.03 - Opšti podaci o fluktuaciji kadrova (OP3),
b) Obrazac BA 42.04 - Opšti podaci o vanjskim IT saradnicima (OP4),
c) Obrazac BA 45.00 - Plan tretiranja rizika informacionog sistema (RIS),

d) Obrazac BA 46.00 - Rezultati penetracionog testiranja/testova ranjivosti (PEN),
e) Obrazac BA 47.01 - Pregled planiranih i provedenih revizija informacionog sistema (ITR1),
f) Obrazac BA 47.02 - Pregled preporuka/naloga revizije informacionog sistema (ITR2),
g) Obrazac BA 49.00 - Značajne promjene u informacionom sistemu banke (PIS),
h) Obrazac BA 50.02 - Broj incidenata/zastoja po poslovnim procesima (INC2),
i) Obrazac BA 50.03 - Broj prema vrstama incidenata (INC3),
j) Obrazac BA 50.04 - Cyber incidenti (INC4),
k) Obrazac BA 50.05 - Elektronsko bankarstvo i kartično poslovanje - moguće zloupotrebe (INC5).

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

(4) 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 (na primjer, član Uprave, rukovodilac organizacione jedinice za upravljanje informacionim sistemom u banci, voditelj za sigurnost informacionog sistema, interni revizor i slično).

IV ZAVRŠNE ODREDBE

Član 17.
Prestanak važenja uputstva

Danom primjene ovog Uputstva prestaje da važi Uputstvo za izvještavanje o upravljanju informacionim sistemom broj: 01-4923/17 od 22.12.2017. godine.

Član 18.
Stupanje na snagu

Ovo Uputstvo stupa na snagu danom donošenja i objavljuje se na službenoj web stranici Agencije, a primjenjuje se počev od izvještavanja sa finansijskim datumom 31.12.2020. godine.

Broj: 01-176/21
Sarajevo, 18.01.2021. godine

DIREKTOR, s.r.

Jasmin Mahmuzić