Odgovori na komentare i sugestije na prednacrt Odluke o upravljanju informacionim sistemom u banci

GENERALNI KOMENTAR AGENCIJA ZA BANKARSTVO FBIH

Uzimajući u obzir da se najveći broj upita iz javne rasprave odnosio na funkciju upravljanja IKT rizicima, kao i na aktivnosti prve i druge linije odbrane u okviru "3 linije odbrane", u okviru konačne Odluke, načinjene su određene izmjene u tom dijelu, te su u nastavku data pojašnjenja.

Odluka se fokusira na uspostavljanje principa "3 linije odbrane", te je konačni cilj odluke jačanje kapaciteta u sve 3 linije odbrane, sa posebnom pažnjom na 2. liniju, koja je detaljnije definisana ovom Odlukom.
Banke su dužne, uzimajući u obzir princip proporcionalnosti naveden u čl 13. Odluke, donijeti odluku o načinu uspostavljanja navedene 3 linije odbrane i njihovoj organizaciji, vodeći računa o nespojivosti funkcija i odgovorajućoj segregaciji.
Funkcija upravljanja IKT rizicima, koja je definisana ovom Odlukom, predstavlja drugu liniju odbrane, u gore navedenom konceptu.
Članovima 4. (2) i 12. (3) je definisana organizaciona pozicija i zadaci funkcije upravljanja IKT rizicima. Funkcija upravljanja IKT rizicima može organizaciono biti smještena unutar jedinstvene kontrolne funkcije upravljanja rizicima, ali nije obavezno, te funkcija upravljanja IKT rizicima može biti i samostalna organizacijska jedinica. U slučaju izmještanja izvan kontrolne funkcije upravljanja rizicima, neophodna je svakodnevna saradnja između navedene dvije funkcije.
Prilikom uspostavljanja druge linije - funkcije upravljanja IKT rizicima, potrebno je osigurati sljedeće:
- direktnu liniju izvještavanja funkcije upravljanja IKT rizicima prema Upravi banke i njenu neovisnost, u smislu da funkcija upravljanja IKT rizicima nije u nadležnosti člana Uprave koji je ujedno nadležan za prvu liniju odbrane, kao i organizacijsku jedinicu za upravljanje IKT sistemom,
- osigurati neovisnost funkcije upravljanja IKT rizicima od funkcija zaduženih za IKT upravljanje, razvoj, promjene i operacije (uključujući operativnu sigurnost).

Uloga voditelja sigurnosti (CISO) nije definisana eksplicitno ovom odlukom, što ne znači da ne može da i dalje postoji u banci. Funkcija upravljanja IKT rizicima nije ograničena u smislu obavljanja kontrolnih i savjetodavnih aktivnosti voditelja sigurnosti (npr. definisanje ili predlaganje politike sigurnosti i nadziranje postupanja po istoj), ali ne smije učestvovati u definisanju operativnih akata sigurnosti te dizajnu i implementaciji kontrolnih mjera.
Dizajn i implementacija kontrolnih mjera su isključivo u nadležnosti prve linije odbrane. Također, u okviru prve linije odbrane je i svakodnevni pregled zapisa informacionog sistema, u smislu, otkrivanja eventualnih sigurnosnih incidenata, nadzora aktivnosti korisnika, uključujući i IKT korisnike i sl.
Što se tiče organizacione pozicije prve linije odbrane, ona može organizaciono biti smještena u okviru organizacione jedinice upravljanja IKT sistemom ili kao samostalna organizaciona jedinica. Pri tome je potrebno voditi računa o adekvatnom razdvajanju dužnosti i odgovornosti, radi minimiziranja rizika, adekvatne segregacije i osiguravanja efikasnog upravljanja.

OBLAST	ČLAN	OPIS	STAV	TAČKA		KOMENTARI	
	Član 3.	Interni akti	(1)		Banka je dužna propisati i primijeniti interne akte, u vidu strategija, politika, metodologija, procedura i radnih uputa, kojima se uređuje upravljanje IKT sistemom, uključujući upotrebu, praćenje i nadzor IKT sistema.		
	Član 3.	Interni akti	(2)		Interni akti iz stava (1), kao minimum, trebaju biti: a) usklađeni sa propisima, standardima i pravilima struke, te međusobno, b) redovno pregledani i ažurirani i c) potpuni, detaljni i primjenjivi.		
	Član 3.	Interni akti	(3)		Potrebno je osigurati da su svi korisnici IKT sistema upoznati sa sadržajem internih akata vezanim uz IKT sistem, u skladu sa potrebama svakog korisnika.		
	Član 3.	Interni akti	(4)		Ugovori, nalazi revizije, izvještaji koje razmatraju organi banke, uputstva i ostali dokumenti trebaju biti sačinjeni odnosno prevedeni na jedan od jezika u zvaničnoj upotrebi u Federaciji Bosne i Hercegovine.		
	Član 4.	Odgovornosti nadzornog odbora			Nadzorni odbor banke dužan je, kao minimum, da:		
	Član 4.	Odgovornosti nadzornog odbora		a)	uspostavi, održava i unapređuje efikasan proces upravljanja IKT sistemom, u cilju implementacije sigurnog, pouzdanog i efikasnog IKT sistema u banci, te osigurava da uprava banke osigura uslove za njegovo provođenje,		
	Član 4.	Odgovornosti nadzornog odbora		b)	uspostavi, održava i unapređuje proces upravljanja IKT rizikom, kao dio jedinstvenog procesa upravljanja rizicima banke, te osigurava da uprava banke osigura uslove za njegovo provođenje		

Član 4.	Odgovornosti nadzornog odbora		c)	odlučuje o adekvatnoj organizacionoj strukturi banke sa jasnom i preciznom podjelom nadležnosti, dužnosti i odgovornosti, a kako bi osigurala efikasno i sigurno upravljanje IKT sistemom i IKT rizicima, uključujući upravljanje sigurnošću IKT sistema, upravljanje rizicima trećih strana pružaoca IKT usluga, upravljanje IKT incidentima, upravljanje kontinuitetom poslovanja i internu reviziju IKT sistema, te efikasnu i pravovremenu komunikaciju, saradnju i koordinaciju među navedenim funkcijama,	**Komentar:** 1. Uzimajući u obzir navedenu odredbu i odredbu Člana 4 tačka e), ukoliko organizacija upravljanja sigurnošću IKT sistema i organizacija upravljanja IKT sistemom, u svom radu i izvještajnoj liniji, budući da su odvojeni odjeli, nezavisno odgovaraju istom članu Uprave, koji je između ostalog zadužen i za Upravljanje IKT rizicima, mogu li se navedene odredbe smatrati ispunjenim, uz navedeno tumačenje? Ukoliko je tumačenje pogrešno, molimo Vas za ispravno tumačenje. Potrebno je razjasniti ovu odredbu i vezu člana (5) s obzirom da se može tumačiti dvojako. 2. Da li će se postojeća forma izvještaja mijenjati i biti definsana uputstvima? 3. Molimo pojašnjenje šta se očekuje da bude obuhvaćeno Politikom o korištenju IKT usluga trećih strana (tačka g, stav vii)?	**Komentar:** 1. Upravljanje sigurnošću IKT sistema je sastavni dio upravljanja IKT rizicima, uzimajući u obzir da je sigurnost IKT jedan od rizika IKT sistema. Organizacija upravljanja IKT sistemom, u svom radu i izvještajnoj liniji, treba da je odvojeni odjel i da imaj nezavisne linije izvještavanja prema Upravi banke, u odnosu na upravljanje IKT rizicima, u okviru kojeg se nalazi i upravljanje IKT sigurnosću. Organizacija upravljanja IKT sistemom treba da odgovara prema članu Uprave zaduženom za IT, dok upravljanje IKT rizicima (bez obzira gdje se organizaciono nalazi) treba da odgovara npr prema članu uprave odgovornom za upravljanje rizicima. Član Uprave odgovoran za upravljanje IKT sistemom, ne može da bude istovremeno odgovoran i za upravljanje IKT rizicima. 2. Da, izvještavanje o IKT i IKT rizicima, u regulatorne i statističke svrhe, će biti potrebno izmijeniti shodno izmjenama u Odluci, te će biti propaćeno odgovarajućim uputstvom. 3. Sadržaj navedene politike će biti propisan dodatnim uputstvima.
Član 4.	Odgovornosti nadzornog odbora		d)	u okviru organizacione strukture banke, utvrđuje jasne uloge i odgovornosti, stručne kvalifikacije i potrebne kompetencije, osiguravajući da su broj i potrebne vještine uposlenika banke adekvatni za pružanje podrške efikasnom i sigurnom funkcionisanju IKT sistema i upravljanju IKT rizicima na kontinuiranoj osnovi,		
Član 4.	Odgovornosti nadzornog odbora		e)	osigurava da organizacija upravljanja sigurnošću IKT sistema bude nezavisna od organizacije upravljanja IKT sistemom u svom radu i izvještajnoj liniji,		
Član 4.	Odgovornosti nadzornog odbora		f)	donosi i periodično preispituje odgovarajući budžet za ispunjavanje potreba banke za osiguravanje efikasnog, sigurnog i pouzdanog IKT sistema, te adekvatnog nivoa digitalne operativne otpornosti, u pogledu svih vrsta resursa, uključujući i relevantne programe za podizanje svijesti o sigurnosti IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti, te sticanja znanja i vještina u području IKT i IKT sigurnosti.		

Član 4.	Odgovornosti nadzornog odbora		g)	usvaja: i. Strategiju IKT sistema, ii. Strategiju kontinuiteta poslovanja, iii. Politiku za upravljanje IKT rizicima, iv. Politiku informacione sigurnosti, v. Politiku upravljanja IKT incidentima, vi. Politiku za testiranje digitalne operativne otpornosti i vii. Politiku o korištenju IKT usluga trećih strana, te osigura uslove za njihovo provođenje, nadzire njihovo provođenje i periodično ih revidira, a najmanje jednom godišnje analizira i prilagođava promjenama, uzimajući u obzir poslovni model banke, kompleksnost IKT sistema i sklonost ka preuzimanju rizika i		
Član 4.	Odgovornosti nadzornog odbora		h)	propiše sadržaj i periodičnost izvještavanja nadzornog odbora u vezi sa: i. upravljanjem IKT sistemom, uključujući izvještavanje o realizaciji operativnih planova, te najmanje o značajnim IKT incidentima, kao i odgovorima, oporavku i korektivnim mjerama, ii. upravljanjem IKT rizicima, uključujući izvještaj o stepenu digitalne operativne otpornosti i iii. ugovorima sklopljenim sa trećim stranama pružaocima IKT usluga, svim relevantnim planiranim materijalnim promjenama u vezi sa njima te potencijalnom uticaju tih promjena na prioritetne ili važne funkcije koje su podložne tim ugovorima, uključujući sažetak analize rizika za procjenu uticaja tih promjena.		
Član 5.	Odgovornosti uprave banke	(1)		Uprava banke je dužna, kao minimum, da:		
Član 5.	Odgovornosti uprave banke	(1)	a)	priprema prijedloge strategija i politika iz člana 4. tačka g) ove odluke za usvajanje nadzornom odboru, osigura provođenje istih na svim nivoima odlučivanja i u poslovnim procesima, te izvještava nadzorni odbor o njihovom provođenju,	**Komentar:** 1. Da li funkcija upravljanja sigurnošću IKT sistema obuhvata sve oblasti predviđene ISO 27001? Uključujući BCM, Crisis Management, tehničku i	**Komentar:** 1. Odgovornosti funkcije upravljanja IKT rizicima, uključujući i upravljanje sigurnošću IKT sistema su

Član 5.	Odgovornosti uprave banke	(1)	b)	donosi i provodi procedure upravljanja IKT sistemom i IKT rizicima, u skladu sa poslovnim ciljevima i poslovnom strategijom banke, a koje osiguravaju održavanje standarda dostupnosti, autentičnosti, integriteta, povjerljivosti i sljedivosti podataka, definisanih Strategijom IKT sistema,	fizičku zaštitu? Da li se pod pojmom sigurnost IKT sistema tretira i fizička i logička sigurnost? 2. Ukoliko imamo politiku, strategiju i operativne planove, da li je neophodan i dokument za nazivom "Okvir"? Šta bi u ovom slučaju bilo prihvatljivo kao "Okvir"? 3. Koji su kriteriji odnosno nivoi na osnovu kojih se primjenjuje procjena redovnosti za proispitivnaje rizika? 4. da li će upustvima biti definisan zahtjev za adekvatan broj resursa za sprovođenje odluke? Na osnovu čega je potrebno odrediti dovoljan broj zaposlenika za podršku operativnim potrebama. 5. Na šta se odnosi odredba stava (h) "i rizicima povezanim sa trećim stranama pružaocima IKT usluga,..."? 6. Šta se podrazumijeva pod nositeljima ključnih funkcija? 7. Ukoliko imamo politike i procedure za upravljanje projektima, unutar kojih se dodjeljuju odgovarajuće uloge ovisno o cilju projekta, da li je neophodno zasebno dokumentovati metodologiju za upravljanje IKT Projektima? Ako se vratimo na definiciju IKT Projekta, gotovo da možemo ustvarditi da je svaki Projekt u stvari i IKT projekt. 8.da li član uprave mora da ima formalno obrazovanje i iskustvo u oblasti IKT rizikom samo može biti nadležan za isto? Da li ovim povećavamo potrebe za dodatnim kompetencijama Članova uprave?Šta se podrazumijeva kontinuirane edukacije I posebne obuke? 9. Pojasniti princip proporcionalnosti detaljno. Da li je moguće definisati pragove radi izbjegavanja koncentracije radnih zadataka na mali broj uposelnika? Da li ovo znači da po default-u CISO nije taj koji će biti kontrolna funkcija upravljanja IKT rizicima, odnosno da li se ovdje uvodi nova funkcija za upravljanje Ikt rizicima, za koje CISO neće biti odgovoaran? Da li se zbog pojma sigurnost IKS sistema podrazumijeva da I fizička sigurnost odgovara članu uprave za upravljanje rizicima? Primjer - Nisu sve Banke definisale	propisane članom 6. ove odluke. Ova odluka se ne referira na oblasti ISO 27001. Oblasti BCM, Crisis Management, tehnička i fizička zaštita ne moraju nužno biti odgovornost ove funkcije, ali svakako ova funkcija treba biti uključena u rad BCM, Crisis Management i tehničke i fizičke zaštitu. Analiza i upravljanje rizicima u okviru tehničke i fizičke zaštite u onom dijelu u kojem se odnose na informaciono-komunikacioni sistem banke jesu odgovornosti ove funkcije. Definicija sigurnosti IKT sistema je data u definicijama i uključuje fizičku sigurnost u onoj mjeri u kojoj to može utiče na IKT sistem. 2. U članu 12. koji definiše upostavu okvira za upravljanje IKT rizicima, izraz "okvir" se ne odnosi na pojedinačni, specifični interni akt, nego na skup internih akata, kojima se kao jednom cjelinom, definiše način upravljanja rizicima IKT-a. 3. Kriteriji za procjenu redovnosti procjene IKT rizika uključuju veličinu banke, poslovni model banke, kompleksnost i veličinu IKT sistema, upotrebu savremenih tehnologija u okviru IKT sistema, prirodu i kretanje rizika kojima je IKT sistem banke izložen i slično. 4. Agencija će u okviru nadzora cijeniti adekvatnost u stručnosti i broju resursa kojima banka raspolaže u organizacionim jedinicima upravljanja IKT i upravljanja IKT rizicima. Banka, u skladu sa svojom veličinom, poslovnim modelom, kompleksnošću i veličinom informacionog sistema, vrstama tehnologija koje koristi treba da osigura neometano, kontinuirano obavljanje poslovnih procesa i zadataka, koji ovise od gore navedenih organizacionih jedinica, imajući u vidu da sve ključne odgovornosti trebaju biti pokrivene i adekvatnim rezervnim osobama/uposlenicima. 5. Odredba pojašnjava da se u okviru upravljanja IKT rizicima trebaju uzeti u obzir i rizici povezani sa trećim stranama pružaocima IKT usluga, a što je predmetom sekcije IX Odluke. 6. Šta se podrazumjeva pod nosiocima ključnih funkcija je definisano u skladu sa Zakon o bankama tačka 2. a) a) i u okviru Odluci o sistemu internog upravljanja . 7. . Banka treba imati definisane postupke upravljanja projektom, uključujući faze projekta, odgovornosti, način upravljanja rizicima projekta, izvještavanje i slično. Odluka propisuje da banka treba usvojiti metodologiju upravljanja projektom, na nivou Uprave banke. Ukoliko su svi navedeni elementi metodologije propisani i politikom i procedurama, koje su usvojene na nivou Uprave banke, banka ne treba propisivati zasebno i dokument metodologije. Navedeni elementi će biti detaljnije propisani i Uputstvom. 8. Banka je dužna osigurati da članovi organa banke imaju odgovarajuće pojedinačno i kolektivno
Član 5.	Odgovornosti uprave banke	(1)	c)	uspostavi i osigura adekvatan okvir za upravljanje IKT rizicima, a koji je potrebno najmanje jednom godišnje analizirati i prilagoditi promjenama,		
Član 5.	Odgovornosti uprave banke	(1)	d)	na osnovu procjene ukupnog profila rizičnosti banke, te obima i složenosti njenih poslovnih operacija, redovno preispituje rizike koji su utvrđeni u vezi sa ugovornim aranžmanima o upotrebi IKT usluga kojima se podržavaju prioritetne (važne) funkcije		
Član 5.	Odgovornosti uprave banke	(1)	e)	prati izvršenje operativnih planova provođenja Strategije IKT sistema, kao i bitne izmjene,		
Član 5.	Odgovornosti uprave banke	(1)	f)	osigura da su sve uloge i odgovornosti vezane uz upravljanje IKT sistemom adekvatno uspostavljene, jasno definirane i dodijeljene, vodeći računa o adekvatnoj segregaciji dužnosti,		
Član 5.	Odgovornosti uprave banke	(1)	g)	osigura potrebne i adekvatne resurse za upravljanje IKT sistemom i IKT rizicima, uključujući i IKT rizike povezane sa trećim stranama pružaocima IKT usluga, uključujući dovoljan broj i stručnu osposobljenost zaposlenika za pružanje podrške operativnim potrebama u procesu upravljanja IKT sistemom i upravljanju IKT rizicima, kao i za provođenje Strategije IKT sistema, te dovoljna finansijska sredstva za osiguravanje navedenog,		
Član 5.	Odgovornosti uprave banke	(1)	h)	uspostavi i implementira odgovarajući sistem izvještavanja o upravljanju IKT sistemom, IKT rizicima i rizicima povezanim sa trećim stranama pružaocima IKT usluga,		
Član 5.	Odgovornosti uprave banke	(1)	i)	uspostavi funkciju za praćenje aranžmana o upotrebi IKT usluga sklopljenih sa trećim stranama pružaocima IKT usluga ili imenuju člana višeg rukovodstva koji će biti odgovoran za nadzor nad povezanom izloženosti rizicima i relevantnom dokumentacijom,		
Član 5.	Odgovornosti uprave banke	(1)	j)	osigura da svi članovi osoblja, uključujući i nositelje ključnih funkcija, prođu odgovarajuće osposobljavanje o IKT rizicima, uključujući i o informacionoj sigurnosti, na godišnjoj osnovi ili češće, ako je to potrebno i		

ODGOVORNOSTI	Član 5.	Odgovornosti uprave banke	(1)	k)	donosi sljedeće procedure i interne akte: i. Operativne planove provođenja Strategije IKT sistema, ii. Procedure za upravljanje IKT rizicima, iii. Procedure za testiranje digitalne operativne otpornosti, iv. Plan kontinuiteta poslovanja u području IKT sistema i planove odgovora i oporavka IKT sistema, te Analizu uticaja na poslovanje (eng. BIA), v. Procedure upravljanja IKT incidentima, vi. Procedure upravljanja sigurnosnim i zaštitnim (regulatornim) kopijama, vii. Procedure upravljanja pristupom IKT sistemu, viii. Procedure za upravljanje ažuriranjima software-a, ix. Procedure za upravljanje zaštitom od malicioznog software-a, x. Procedure upravljanja IKT imovinom, xi. Metodologiju upravljanja IKT projektima, xii. Procedure nabave, razvoja i održavanja IKT sistema, xiii. Procedure upravljanja IKT promjenama, xiv. Procedure upravljanja zapisima IKT sistema, xv. Plan i program za uspostavu i podizanje svijesti o sigurnosti informacionog sistema, xvi. Plan edukacije uposlenika i xvii. Planove komunikacije u krizi. i ostale interne akte koji se odnose na specifične dijelove upravljanja IKT sistemom.	[illegible] funkcije CSO - chief security officer koji pokriva informacijsku (logičku) I fizičku sigurnost. 10. Napraviti pojašnjenje u vezi predispozicija za lice zaduženo za provođenje komunikacijskih planova za IKT incidente. 11. Molimo pojašnjenje tijela za potrebe koordinacije aktivnosti vezanih uz IKT sistem (stav (5) predmetnog člana) 12. Napraviti pojašnjenje stav (4) vezano ua odgovornosti članova UB. Potrebno naglasiti da funkcija IKT sigurnosti i IKT rizika mogu odgovarati članu uprave zaduženom za rizike ali isto tako i članu uprave zaduženom za kontrolne funckije (Predsjednik UB). Primjer dopunjenog teksta stav (4): Lice zaduženo za sigurnost IKT sistema odgovara članu uprave zaduženom za upravljanje rizicima ili članu uprave koji je odgovoran za kontrolnu funkciju upravljanja IKT rizicima, ukoliko je drugo imenovano. Izvor: ODLUKA O SISTEMU INTERNOG UPRAVLJANJA U BANCI, Član 33. Kontrolna funkcija banke 13. Iz stava 2. ovog člana, proizilazi da Banka može imati jednog člana Uprave koji je nadležan za upravljanje IKT sistemom i IKT rizikom, dok iz stava 4, proizilazi da lice zaduženo za sigurnost sistema može da odgavara članu UB koji je nadležan za upravljanje rizicima IKT sistema. U smislu navedenih formulacija se može tumačiti da funkcija upravljanja IKT istemom i lice/funkcija upravljanja IKT sigurnošću može biti dodijeljena jednom članu Uprave koji je ujedno nadležan i za IKT rizike. Molimo potvrdu ili precizniju formulaciju, posebno uzimajući u obzir član 4 stav e. 14. Da li se kao posebno tijelo za potrebe koordinacije aktivnosti vezanih uz IKT sistem (stav 6) može smatrati Odbor za upravljanje informacionim sistremom koji je bio propisan i prethodnom odlukom?	[illegible] znanje, sposobnosti, vještine i iskustva kako bi u potpunosti i srazmjerno svojim odgovornostima razumjeli i pratili poslovanje banke, glavne rizike i sistem upravljanja u banci, te organizaciju banke, odnosno grupe, uključujući potencijalne sukobe interesa. Član uprave zadužen za IKT rizike treba da ima iskustvo i razumijevanje u oblasti IKT rizika, kako bi mogao da razumije i procijeni IKT rizik koji banka preuzima. Pod kontinuiranom edukacijom i posebnim obukama se smatra edukacija u vezi sa IKT rizicima, a u cilju razumijevanja istih. Navedeno je definisano i u članu 82. Odluke o sistemu internog upravljanja. 9. Princip proporcionalnosti je detaljno definisan u okviru člana 13. odluke. Ovom odlukom se samo detaljnije propisuju elementi upravljanja IKT rizikom, kao II linijom odbrane. CISO funkcija kao takva nije više definisana Odlukom, određeni prijašnji zadaci te funkcije mogu biti u okviru funkcije upravljanja IKT rizicima, bez obzira organizaciono gdje se ona nalazila, dok se operativni zadaci trebaju dodijeliti I liniji odbrane. Pogled na aktivnosti je dat u uvodu. Šta je uključeno u pojam sigurnosti IKT sistema je već ranije pojašnjeno. 10. U banci najmanje jedna osoba treba biti zadužena za provođenje komunikacijskih planova za IKT incidente, a poštujući odredbe član 20. ove odluke. 11. Banka može, u skladu sa procjenom navedenom u stavu, formirati posebno tijelo za potrebe upravljanja i koordinacije aktivnostima vezanim uz IKT sistem, uključujući upravljanje prioritetima razvoja, projekata, sigurnosti IKT i slično. 12.Dodatnim članom 4. stav (2) napravljeno je pojašnjenje navedenog. 13. Navedeno je pojašnjeno u prethodnom stavu. Suština jeste da organizacija upravljanja IKT i organizacija upravljanja IKT rizicima, uključujući i sigurnost IKT, odgovaraju različitim članovima Uprave. 14. Da, može.
	Član 5.	Odgovornosti uprave banke	(2)		Član/članovi uprave banke odgovorni za upravljanje IKT sistemom i IKT rizikom dužni su posjedovati adekvatan nivo znanja i vještina da razumiju i procijene IKT rizik i njegov uticaj na poslovanje banke, kao i kontinuirano se educirati i pratiti posebne obuke, razmjerno veličini IKT rizika kojim se upravlja.			
	Član 5.	Odgovornosti uprave banke	(3)		Uprava banke je dužna uspostaviti funkcije upravljanja sigurnošću IKT sistema, što uključuje imenovanje lica zaduženog za sigurnost IKT sistema, te definisati ovlaštenja, odgovornosti i obim rada. Uprava banke je dužna srazmjerno veličini, vrsti, obimu i složenosti IKT sistema, kao i prirodi, obimu i složenosti svojih usluga, aktivnosti i poslovanja, procijeniti potrebni broj zaposlenika u funkcijama upravljanja sigurnošću IKT sistema.			
	Član 5.	Odgovornosti uprave banke	(4)		Uzimajući u obzir princip proporcionalnosti naveden u čl. 13 ove odluke, funkcija upravljanja sigurnošću IKT sistema može biti dodijeljena kontrolnoj funkciji upravljanja IKT rizicima. Lice zaduženo za sigurnost IKT sistema odgovara članu uprave zaduženom za upravljanje rizicima ili upravljanje rizicima IKT sistema, ukoliko je drugo imenovano.			
	Član 5.	Odgovornosti uprave banke	(5)		Uprava banke je dužna imenovati najmanje jedno lice zaduženo za provođenje komunikacijskih planova za IKT incidente koje u tu svrhu ispunjava funkciju komunikacije s javnošću i medijima.			

Član 5.	Odgovornosti uprave banke	(6)		Uprava banke je dužna razmotriti potrebu formiranja posebnog tijela za potrebe koordinacije aktivnosti vezanih uz IKT sistem, uzimajući u obzir veličinu banke, prirodi, obim i složenosti svojih usluga, aktivnosti i poslovanja, unutrašnju organizaciju, te veličinu i kompleksnost informacionog sistema.		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(1)		Lice zaduženo za sigurnost IKT sistema (CISO) treba biti kompetentno lice sa odgovarajućim stručnim kvalifikacijama, specijalističkim znanjima i iskustvom iz oblasti upravljanja IKT sigurnosti, te posjedovati relevantne međunarodno priznate certifikate iz oblasti IKT sigurnosti.		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)		CISO treba, kao minimum, da nadzire i koordinira aktivnosti vezane uz sigurnost IKT sistema, a što uključuje minimalno sljedeće:	**Komentar:** 1. Da li CISO može biti odgovoran za upravljenje IKT rizicima ili mora postojati odvojena funkcija? 2. Ko je vlasnik politike IS? 3. Jasno specificirati šta je sistemska a šta stalna obuka. 4. Koje interne kontrole provodi CISO funkcija? 5. Šta se podrazumijeva pod stavom (2) b. nadzor jer može doći do preklapanja odgovornosti za različite linije odbrane? 6. Pojasniti ko je vlasnik incident management procesa 7. razmotriti objedinjavanje stava (2) l. i stava (3) jer su iste odredbe 8. da li je predviđeno proširivanje kontrolnih funkcija predviđenih Zakonom o bankama ili se samo proširuje odgovornost postojećih kontrolnih funkcija sa odgvornosti nadzora (član 12. stav (4)). Molimo pojašnjenje budući da izmjena kontrolnih funkcija implicira izmjenu Zakona o bankama.	Komentar: 1. Treba postojati funkcija upravljanja IKT rizicima. Navedenu funkciju, u nedostatku drugih adekvatnih resursa, može preuzeti dosadašnji CISO, vodeći računa o adekvatnom broju uposlenika zaduženih za upravljanje IKT rizicima, s tim da dio dužnosti koje se odnose na operativni dnevni nadzor zapisa, treba delegirati prvoj linije odbrane. 2. Vlasnik politike IS je na nivou funkcije upravljanja IKT rizicima. Politika sigurnosti IKT sistema treba imati jasnu vezu sa procjenom rizika informaciono komunikacionog sistema. Operativni akti vezani uz primjenu načela definisanih u Politici sigurnost su u nadležnosti prve linije. 3. Sistemska obuka predstavlja organizovanu i planiranu obuku koja se provodi prema unaprijed definisanim pravilima i procedurama. Obuka je usmjerena na razvijanje specifičnih veština i znanja koja su potrebna za obavljanje određenog posla ili funkcije, te se fokusira na obuku koja je potrebna da bi zaposleni mogli da obavljaju određeni zadatak ili funkciju. Kontinuirana obuka podrazumjeva stalni proces usavršavanja i edukacije zaposlenih tokom čitave njihove karijere, s ciljem stalnog poboljšanja njihovih vještina i znanja. Ova obuka ima za cilj da zaposlenima omogući da se stalno razvijaju, prate nove tehnologije i trendove i unaprede svoje kompetencije. 4. Funkcija upravljanja IKT rizikom je nadležna da koordinira i nadgleda provođenje internih kontrola koje su definisane ovom odlukom, a koje se odnose se na upravljanje rizicima informaciono komunikacionog sistema. 5. Pod nadzorom i analizom IKT sistema, a u cilju otkrivanja sigurnosnih prijetnji i ranjivosti, se smatraju aktivnosti nadzora zapisa IKT sistema, u cilju utvrđivanja potencijalnih sigurnosnih opasnosti, kao i u cilju utvrđivanja poštivanja propisanih mjera, te analize arhitekture IKT sistema i praćenje pojave novih sigurnosnih prijetnji, u cilju definisanja novih odnosno dodatnih zaštitnih mjera.Ovdje se ne misli na dnevno nadgledanje zapisa, koje bi bilo zadatak prve linije odbrane. 6. Vlasnik incident management procesa, u slučaju IKT incidenata, je organizacija upravljanja IKT
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	a)	koordinira i sprovodi interne kontrole usklađene sa ovom odlukom,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	b)	vrši nadzor i analizu IKT sistema, u cilju otkrivanja sigurnosnih prijetnji i ranjivosti,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	c)	učestvuje u aktivnostima identifikacije i procjene IKT rizika i pružanju prijedloga mjera ovladavanja IKT rizicima, iz članova 15. – 19. ove odluke,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	d)	učestvuje u izradi Politike informacione sigurnosti, iz člana 17. ove odluke, te daje prijedloge za njeno unapređenje, u skladu sa razvojem IKT sistema i IKT rizika u banci,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	e)	prati promjene IKT sistema i analizira uticaj promjena IKT sistema na postojeće kontrole IKT sigurnosti, daje prijedlog uvođenja novih kontrola sigurnosti IKT sistema, uključujući i razvoj novih funkcionalnosti i IKT projekte,		

Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	f)	osigurava, prati i koordinira aktivnosti iz okvira za testiranje informacione sigurnosti,	9. jasnije definisati uloge i odgovornosti funkcija CISO, upravljanja IKT rizicima i sigurnosti. 10. Da li će korz uputstva bit jasne i detaljne smjernice u pogledu obaveza CISO funkcije, a vezano za članove 38, 39 I 40, pogotovo prilikom CI/CD procesa u razvoju? 11. Lice zaduženo za sigurnost IKT sistema" zaista ne odgovara opšteprihvaćenom terminu i nazivu (CISO) koji se uobičajeno koristi u ovom kontekstu. U međunarodnim okvirima i raspravama, jasno je o kakvoj izvršnoj, upravljačkoj C-funkciji se radi i to isto bi trebalo biti adekvatno prevedeno, navedeno i prihvaćeno u domaćim okvirima.	sistemom - odnosno prva linija. Odgovornost prijave incidenta je na vlasniku procesa kod kojeg je uočen incident, što može biti poslovna strana, IKT organizacija, ali i upravljanje IKT rizicima. Rukovođenje rješavanjem problema, u slučaju da je u pitanju IKT sistem, vrši organizacija upravljanja IKT sistemom. 7. razmotriti objedinjavanje stava (2) l. i stava (3) jer su iste odredbe. - PRIHVAĆEN KOMENTAR, TAČKA L) SE BRIŠE. 8. Odgovor na ovo pitanje je dat u uvodu komentara. 9. Funkcija upravljanja IKT rizicima je odgovorna za postupke definisane okvirom za upravljanje IKT rizikom, uključujući identifikaciju rizika, procjenu rizika, ovladavanje rizicima, praćenje efikasnosti, nadzor i izvještavanje o IKT rizicima. Funkcija CISO, iz prethodno važeće odluke, se više ne definiše zasebno. 10. Navedeno neće biti predmetom detaljnijeg definisanja kroz uputstva. Funkcija upravljanje IKT rizicima treba da bude pravovremeno uključena u sve promjene, razvoj i projekte IKT sistema, u cilju osiguravanja definisanog nivoa sigurnosti IKT sistema. 11. Odgovor na ovo pitanje je dat u uvodu.
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	g)	osigurava adekvatne i pravovremene aktivnosti razmjene informacija o IKT incidentima i cyber prijetnjama, definisane članom 51. ove odluke,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	h)	učestvuje u procjeni IKT rizika i pružanju mjera ovladavanja IKT rizicima u slučaju angažovanja trećih strana pružaoca IKT usluga,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	i)	prati sigurnosne rizike koji proizilaze iz korištenja usluga trećih strana pružaoca IKT usluga,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	j)	osigurava, prati i koordinira aktivnosti vezane uz realizaciju programa podizanja svijesti o sigurnosti IKT sistema,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	k)	učestvuje u radu odbora i radnih grupa koji su formirani za potrebe upravljanja sigurnošću IKT sistema i		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(2)	l)	izvještava redovno upravu banke o aktivnostima vezanim uz stanje sigurnosti IKT sistema, a najmanje na kvartalnoj osnovi.		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(3)		CISO je dužan da redovno izvještava upravu banke o stanju i aktivnostima vezanim uz sigurnost IKT sistema, a minimalno na kvartalnom nivou.		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(4)		CISO je dužan:		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(4)	a)	svoju profesionalnu kompetentnost održavati putem sistemske i stalne obuke, te pravovremeno se educirati o rizicima IKT sistema i tehnologija koje se koriste u banci,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(4)	b)	poznavati relevantne međunarodne standarde i smjernice koje se odnose na uspostavu i nadzor sigurnosti IKT sistema,		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(4)	c)	biti u toku sa najnovijim praksama upravljanja sigurnosnim IKT incidentima, kako bi bilo u mogućnosti efikasno odgovoriti na trenutne ili nove oblike cyber napada i		
Član 6.	Lice zaduženo za sigurnost IKT sistema (CISO)	(4)	d)	pratiti relevantna tehnološka dostignuća kako bi bolje razumijela mogući uticaj koji bi uvođenje novih tehnologija moglo imati na zahtjeve u pogledu IKT sigurnosti.		
Član 7.	Interna IKT revizija	(1)		Banka je dužna provoditi internu reviziju IKT sistema i sistema upravljanja IKT rizicima, u skladu sa zahtjevima propisanim Odlukom o sistemu internog upravljanja u banci, a na osnovu definisanog programa rada interne revizije.	**Komentar:** 1. . Da li ovo znači da se interna revizija primarno treba oslanjati na okvir za upravljanje IKT rizicima u nadležnosti funkcije upravljanja i kontrole IKT rizika, a ne na vlastitu procjenu kako je u skladu sa standardima interene revizije?	**Komentar:** 1. Interna revizija informacionog sistema je dužna razviti svoju metodologiju procjene IKT rizika za potrebe obavljanja interne revizije, ali je dužna u okviru procjene uzeti u obzir i aktuelnu procjenu rizika informacionog sistema, te oblasti koje su označene sa višim stepenom rizika adekvatno procijeniti u okviru svoje metodologije, te im u skladu sa tim, posvetiti više pažnje.
Član 7.	Interna IKT revizija	(2)		Banka je dužna planirati i provoditi internu reviziju IKT sistema u skladu sa metodologijom procjene IKT rizika, imajući u vidu da u određenim vremenskim intervalima budu redovno detaljno pregledani (obuhvaćeni) svi elementi okvira za upravljanje IKT rizicima i svi IKT procesi, a naročito oni koji podupiru prioritetne (važne) funkcije, te kontrole kojima se osigurava visoka digitalna otpornost banke, a proporcionalno IKT rizicima banke.		
Član 7.	Interna IKT revizija	(3)		Lica koja obavljaju internu reviziju IKT sistema banke trebaju posjedovati adekvatna stručna znanja i vještine neophodna za obavljanje revizije IKT sistema i upravljanja IKT rizicima, a uzimajući u obzir veličinu i kompleksnost IKT sistema u banci.		

	Član 7.	Interna IKT revizija	(4)		Funkcija interne revizije je dužna na adekvatan način dokumentovati informacije na osnovu kojih je donesena ocjena adekvatnosti i efikasnosti kontrola u okviru oblasti koja je predmetom revizije, uključujući i podatke o revidiranim internim aktima, IKT procesima i testiranim uzorcima.		
	Član 7.	Interna IKT revizija	(5)		Banka je dužna propisati postupke za upravljanje kašnjenjem u izvršenju naloženih mjera.		
	Član 8.	Eksterna revizija IKT sistema	(1)		Banka je dužna obavljati eksternu reviziju IKT sistema na godišnjem nivou, u skladu sa propisima Agencije koji regulišu oblast eksterne revizije u bankama, ukoliko odredbama ove Odluke nije drugačije definisano.	**Komentar:** 1. prethodna odluka je podrazumijevala 30.5. kao rok izvršenja. S obzirom da se izvještaji trebaju usvajati od strane više upravljačkih tijela, smatramo da je period za realizaciju revizije i nadzora te izrade I usvajanja kratak, Postoji li mogućnost korekcije ovog roka?	**Komentar:** 1. Da, predviđa se promjena ovog vremenskog roka. Eksterna revizija informacionog sistema nije vezana uz kalendarsku godinu, te smatramo da je efikasnije razdvojiti eksternu reviziju informacionog sistema od eksterne finansijske revizije, te je obavljati u ranijem vremenskom periodu. Banka može eksternu reviziju informacionog sistema obaviti i krajem kalendarske godine ili početkom naredne.
	Član 8.	Eksterna revizija IKT sistema	(2)		Ako Agencija utvrdi da eksterna revizija IKT sistema nije obavljena ili da revizorski izvještaj nije sastavljen u skladu sa zakonom, podzakonskim aktima donesenim na osnovu zakona, propisa kojim se uređuje računovodstvo i revizija i pravilima revizorske struke ili ako obavljenom supervizijom poslovanja banke ili na drugi način utvrdi da revizorska ocjena nije zasnovana na istinitim i objektivnim činjenicama, može odbiti revizorski izvještaj i zahtijevati od banke da reviziju		
	Član 8.	Eksterna revizija IKT sistema	(3)		Društvo za reviziju banke i ovlašteni revizor koji obavlja reviziju banke ne može biti lice čiji izvještaj o obavljenoj reviziji IKT sistema za prethodnu poslovnu godinu Agencija nije prihvatila.		
	Član 8.	Eksterna revizija IKT sistema	(4)		Izvještaj o obavljenoj reviziji IKT sistema je poseban izvještaj, te je banka dužna dostaviti Agenciji navedeni izvještaj najkasnije do 31.03. tekuće godine.		
	Član 8.	Eksterna revizija IKT sistema	(5)		Banka je dužna da reviziju IKT sistema obavlja na godišnjem nivou.		
	Član 8.	Eksterna revizija IKT sistema	(6)		Agencija zadržava pravo nalaganja mjera propisanih Zakonom o bankama i propisima Agencije koji regulišu eksternu reviziju u bankama.		
	Član 9.	Strategija IKT sistema	(1)		Banka je dužna:		
	Član 9.	Strategija IKT sistema	(1)	a)	razviti i nadzirati provođenje strategije IKT sistema,		
	Član 9.	Strategija IKT sistema	(1)	b)	definisati operativne planove koji podržavaju provođenje strategije IKT sistema i		
	Član 9.	Strategija IKT sistema	(1)	c)	uspostaviti postupke praćenja i mjerenja efikasnosti provođenja strategije IKT sistema.		
	Član 9.	Strategija IKT sistema	(2)		Strategija IKT sistema iz stava (1) ovog člana, treba da:		
	Član 9.	Strategija IKT sistema	(2)	a)	definiše povezanost i usklađenost strateških ciljeva IKT sistema sa poslovnim ciljevima banke,		

	Član 9.	Strategija IKT sistema	(2)	b)	definiše dugoročne i kratkoročne inicijative unapređenja IKT sistema banke, koje sadrže način na koji bi se IKT sistem banke trebao razvijati radi efikasnog pružanja podrške i sudjelovanja u realizaciji poslovne strategije banke, uključujući razvoj organizacione strukture, promjene IKT sistema, uključujući i IKT arhitekturu, te ključne ovisnosti o trećim stranama,	**Komentar:** 1. Potrebno dodatno pojašnjenje pojma definisanog tačkom (2) stav c) - izložiti pristup upravljanju IKT incidentima. 2. Da li je moguće odvojiti IT i sigurnosnu strategiju, obzirom na zahtjev da ove funkcije budu potpuno odvojene u izvještajnoj liniji? 3. Mišljenja smo da je Strategija IKT sistema krovni dokument (visokog nivoa), i da navedene odredbe se isuviše detaljno bave pristupima IKT incidentima, IKT rizicima i tolerancijom na interupcije sistema. Mišljenja smo da navedeni detalji trebaju biti dio drugih akata (upustava, metodologija i procedura) i da na ovom nivou ne bi trebali biti dio Strategije kao dokumenta visokog nivoa. Na ovaj način bismo teme koju su već definisane nižim aktima (uputstvima i procedurama) ponovo razradili u Strategiji, što smatramo potencijalno suvišnim u aktu ovog nivoa. Molimo da se razmotri izmjena članova c), d) i f). 4. Molimo da se preformulise tacka h) budući da nije logično da se strategijom definiše strategija. Banke mogu u okviru strategija IKT sistema definisati strateške smjernice ovladavanja prepoznatim IKT rizicima povezanim sa trećim stranama. Ukoliko shvatanje nije adekvatno molimo pojašnjenje.	**Komentar:** 1. U okviru strategije potrebno je pojasniti pristup banke upravljanju IKT incidentima, uključujući ciljeve, pristup i odgovornosti vezane uz upravljanje IKT incidentima. 2. Banka može navedeno odvojiti u 2 dokumenta. 3. U okviru samog dokumenta Strategije potrebno je dati suštinski pristup navedenim oblastima sa ključnim odredbama, npr definisati prihvatljivi nivo IKT rizika i tolerancije, a ne detaljno opisivati postupke koje će banka provoditi u cilju osiguravanja istih, što bi bilo predmetom procedura i drugih nižih internih akata. Svakako je potrebno izbjeći ponavljanje istog u više različitih internih akata različitih nivoa. U dokumentu Strategija je potrebno dati suštinski pristup i ciljeve, koji će se dalje razrađivati kroz niže interne akte (politike i procedure, metodologije), a vodeći računa o činjenici da se navedeni dokument usvaja od strane Nadzornog odbora. 4. SUGESTIJA SE PRIHVATA.
	Član 9.	Strategija IKT sistema	(2)	c)	izloži pristup upravljanju IKT incidentima		
	Član 9.	Strategija IKT sistema	(2)	d)	sadrži opis planova komunikacije u slučaju IKT incidenata,		
	Član 9.	Strategija IKT sistema	(2)	e)	definiše kako se okvirom za upravljanje IKT rizicima podupire poslovna strategija banke i njeni ciljevi		
	Član 9.	Strategija IKT sistema	(2)	f)	utvrdi toleranciju na IKT rizik, u skladu sa sklonošću preuzimanja rizika banke, te analizirati uticaj tolerancije prilikom poremećaja u radu IKT sistema,		
	Član 9.	Strategija IKT sistema	(2)	g)	definiše jasne ciljeve u području informacione sigurnosti, uključujući dostupnost, povjerljivost, integritet i sljedivost podataka i IKT sistema, kao i ključne pokazatelje uspješnosti i ključne parametre rizika i		
	Član 9.	Strategija IKT sistema	(2)	h)	definiše strategiju banke vezanu za IKT rizik povezan sa trećim stranama pružaocima IKT usluga.		
	Član 9.	Strategija IKT sistema	(3)		Banka je dužna strategiju IKT sistema periodično ažurirati, a posebno prilikom izmjene poslovne strategije banke i značajnih promjena u strategiji za upravljanje IKT rizicima, a kako bi se osigurala kontinuirana usklađenost između poslovnih ciljeva i ciljeva IKT sistema, kao i odgovarajućih planova i aktivnosti.		
	Član 10.	Operativni planovi	(1)		Operativni planovi iz člana 9. stav (1) tačka b) ove odluke treba da:		
UP	Član 10.	Operativni planovi	(1)	a)	detaljnije definišu aktivnosti koje će poduzeti kako bi se postigao cilj strategije iz člana 9. stav (2) ove odluke,		

RAVLJANJE IKT SISTEMOM	Član 10.	Operativni planovi	(1)	b)	sadrže kao minimum sljedeće elemente: opis aktivnosti i projekata IKT sistema, uključujući i implementaciju mjera koje proizilaze iz procjene IKT rizika, planirane ugovore sa trećim stranama pružaocima IKT usluga, ljudske resurse, budžet, vremenske rokove i odgovorna lica i		
	Član 10.	Operativni planovi	(1)	c)	budu predmetom redovnog praćenja i preispitivanja, a kako bi se osigurala njihova relevantnost i adekvatnost.		
	Član 10.	Operativni planovi	(2)		Uprava banke treba biti jasno, detaljno i pravovremeno obaviještena o realizaciji i statusu aktivnosti definisanih operativnim planovima, a najmanje na kvartalnom nivou.		
	Član 11.	IKT sistemi	(1)		Banka je dužna uspostaviti, implementirati, nadzirati, održavati, redovno revidirati i poboljšavati proces upravljanja IKT sistemom.		
	Član 11.	IKT sistemi	(2)		Banka je dužna upotrebljavati i održavati ažurnim IKT sisteme i alate koji su:		
	Član 11.	IKT sistemi	(2)	a)	primjereni veličini poslovnih funkcija banke koje podržava, a u skladu sa principom proporcionalnosti, uzimajući u obzir svoju veličinu i ukupni profil rizičnosti, kao i prirodu, obim i složenost usluga, aktivnosti i poslovanja banke,		
	Član 11.	IKT sistemi	(2)	b)	pouzdani,		
	Član 11.	IKT sistemi	(2)	c)	opremljeni dovoljnim kapacitetima za: i. tačnu i pouzdanu obradu podataka neophodnih za obavljanje aktivnosti i pravovremeno pružanje usluga banke, ii. periode visoke opterećenosti sistema, iii. uvođenje novih tehnologija i	**Komentar:** 1. da li će upustva definisati princip proporcionalnosti i pragove? Ako neće bankama će biti potrebne jedinstvene smjernice zbog jednoznačnosti pristupa.	**Komentar:** 1. Agencija neće definisati pragove.
	Član 11.	IKT sistemi	(2)	d)	tehnološki otporni kako bi se na adekvatan način nosili sa dodatnim potrebama za obradom informacija u stresnim okolnostima na tržištu ili drugim nepovoljnim situacijama.		

	Član 11.	IKT sistemi	(3)		Pored internih akata iz člana 3. ove odluke, banka je dužna pribavljati i pohranjivati i drugu dokumentaciju (tehničku, funkcionalnu, korisničku i drugu) i informacije koje se odnose na IKT sistem i njegove specifične dijelove. Navedena dokumentacija treba biti tačna, potpuna i ažurna.		
	Član 12.	Uspostava okvira za upravljanje IKT rizicima	(1)		Banka je dužna da, kao dio sveukupnog okvira i mehanizama interne kontrole i procesa upravljanja rizicima, uspostavi pouzdan, sveobuhvatan i dokumentovan okvir za upravljanje IKT rizicima.		
	Član 12.	Uspostava okvira za upravljanje IKT rizicima	(2)		Okvir za upravljanje IKT rizicima banke treba biti u potpunosti integrisan i usklađen sa sveukupnim okvirom upravljanja rizicima banke, a u skladu sa Odlukom o sistemu internog upravljanja u banci („Službene novine FBiH“, br. 39/21).	**Komentar:** 1. Da li će odredbe stava (3) biti opisane uputstvima? 2. Šta podrazumijeva digitalna operativna otpornost - da li će isto biti detaljno pojašnjenjo upustvima. Kada Banka može očekivati distribuciju upustava za predmetna područja. 3. Detaljnije pojasniti pojam kontrolne f-je upravljanja rizicima za nadzor IKT rizika. 4. U članu 12. Stav (4) je naznačeno da je Banka dužna da odgovornost za kontrolu i nadzor nad IKT rizicima dodijeli kontrolnoj funkciji upravljanja	Komentar:

Član 12.	Uspostava okvira za upravljanje IKT rizicima	(3)		Ispunjavanje uslova iz stava (1) ovog člana omogućava banci efikasno upravljanje IKT rizikom i donošenje adekvatnih odluka o preuzimanju IKT rizika, te osigurava provođenje adekvatnih mjera za upravljanje tim rizikom, uključujući i osiguranje visokog nivoa digitalne operativne otpornosti, a u cilju brzog, efikasnog i sveobuhvatnog odgovara na IKT rizik.	rizicima. Dakle, po našem shvatanju, ovo je kao što imamo kreditne rizike koji provode svoje aktivnosti, a kontrolu i nadzor nad kreditnim rizicima radi kontrolna funkcija. Ono što jeste zbunjujuće jest član 5. Stav(4) koji kaže da funckija upravljanja sigurnošću može biti dodijeljena kontrolnoj funkciji upravljanja IKT rizicima, te bi rekli da se to kosi sa gore navedenim.Molimo da se jasno i precizno definiše pozicija i odgovornosti CISO funkcije, upravljanja IKT rizicima kao i veza sa kontrolnim funkcijama koje su definisane Zakonom o bankama. Svaka promjena kontrolnih funkcija implicira i promjenu Zakona o bankama. 5. 6. Naglašavamo da prema Zakonu o bankama i Odluci o sistemu internog upravljanja u banci IKT sigurnost nije predviđena ili propisana kao posebna kontrolna funkcija. Dodatno, za IKT sigurnost je nadležna cjelokupna Uprava Banke, i lice zaduženo za IKT treba da u tom slučaju odgovara Upravi, a ne pojedinačnom članu Uprave Banke. Posebno cijenimo da se ta odgovornost ne može ograničiti na jednog člana Uprave Banke. Postavlja se pitanje kako postupiti u slučaju kada je odgovornost za upravljanje rizicima podijeljena na više članova Uprave Banke? 7. Sa navedenim u vezi predlažemo formulaciju prema kojoj funkcija sigurnosti IKT sistema može biti smještena u jednoj od neovisnih kontrolnih funkcija (osim u Internoj Reviziji) ili postojati kao samostalna neovisna funkcija (samostalna org.jedinica) , sve u zavisnosti od veličine I organizacije banke, sa tim da direktno odgovara i ima liniju komunikacije prema Upravi Banke i Nadzornom odboru. Na taj način se može osigurati da je IKT sigurnost neovisna u raportiranju i komunikaciji prema UB i NO , koji su u osnovi kao kolektivni organ i najodgovorniji za upravljanje cyber i IKT rizikom.	1. Uputstvima će biti detaljnije definisane, između ostaloga, obavezne kontrole koje je potrebno implementirati. Osim obaveznih kontrola, banka je dužna, u skladu sa procjenom IKT rizika, definisati potrebne kontrole. 2. Definicija digitalne operativne otpornosti je data u definicijama Odluke. Agencija će se potruditi da uputstva izadju što ranije, ali svakako se banke u ovom momentu za potrebe pripreme mogu osloniti i na uputstva koja su izdata od strane EU (RTS), koja su propratni akti uz DORA odluku. 3. Odgovornosti f-je upravljanja IKT rizicima su detaljnije pojašnjenje u okviru članova 12. - 22. ove Odluke. 4. Namjera ove odluke nije promjena kontrolnih funkcija. Odlukom o sistemu internog upravljanja su definisana zaduženja kontrolne funkcije upravljanja rizicima, uključujući i IKT rizike. Ovom odlukom se detaljnije pojašnjava okvir upravljanja IKT rizicima. 5., 6. i 7. U uvodnom dijelu je pojašnjenja funkcija upravljanja IKT rizicima i njena uloga.
Član 12.	Uspostava okvira za upravljanje IKT rizicima	(4)		U skladu sa članom 36. stav 1. tačka a) Odluke o sistemu internog upravljanja, banka je dužna odgovornost za kontrolu i nadzor nad IKT rizicima dodijeliti kontrolnoj funkciji upravljanja rizicima.		
Član 13.	Princip proporcionalnosti			Okvir za upravljanje IKT rizicima, kao i pravila utvrđena u ovoj Odluci, banka je dužna primijeniti u skladu sa načelom proporcionalnosti, uzimajući u obzir svoju veličinu i ukupni profil rizičnosti te prirodu, obim i složenost svojih usluga, aktivnosti i poslovanja, unutrašnju organizaciju, te veličinu i kompleksnost IKT sistema.	**Komentar:** 1. da li će upustva definisati princip proporcionalnosti i pragove? Ako neće bankama će biti potrebne jedinstvene smjernice zbog jednoznačnosti pristupa.	**Komentar:** 1. Odgovor je dat ranije kroz prethodna pitanja.
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(1)		Okvir za upravljanje IKT rizicima, treba da obuhvati najmanje strategije, politike, metodologije, programe, procedure i planove, te IKT kontrole koje su potrebne za propisnu i primjerenu zaštitu sve informacione i IKT imovine, u cilju svođenja uticaja IKT rizika na najmanju moguću mjeru, a u skladu sa ciljevima definisanim strategijom.		
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(2)		U okviru Politike za upravljanje IKT rizicima i procedura za upravljanje IKT rizicima, banka je dužna uključiti i sljedeće:		

Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(2)	a)	postupke za redovno i pravovremeno identifikovanje i mjerenje, odnosno procjenu IKT rizika kojima je banka izložena ili bi mogla biti izložena,		
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(2)	b)	postupke za uspostavu mjera za ublažavanje IKT rizika, te pravila za primjenu tih mjera,		
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(2)	c)	postupke praćenja efikasnosti uspostavljenih mjera, a na bazi broja prijavljenih IKT incidenata, te, ako je to potrebno, poduzimanje radnji za ispravljanje mjera,	**Komentar:** 1. da li proces upravljanja IKT rizicima može biti dio procesa upravljanja sigurnošću? 2. da li će uputstvima biti objašnjena metrika iz stava (2) tacka f)?	**Komentar:** 1. U okviru procesa upravljanja IKT rizicima potrebno je uključiti i upravljanje IKT sigurnošću, kao jednim od IKT rizika. 2. Uputstvima će se dati smjernice za kriterije i klasifikaciju IKT incidenata.
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(2)	d)	postupke za kontrolu rizika, uključujući i postupke provođenja testiranja digitalne operativne otpornosti,		
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(2)	e)	postupke za izvještavanje organa banke o IKT rizicima,		
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(2)	f)	postupke praćenja nivoa digitalne operativne otpornosti sa jasnim prikazom aktuelne situacije u pogledu digitalne operativne otpornosti na bazi broja prijavljenih značajnih IKT incidenata i efikasnosti preventivnih kontrola i		
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(2)	g)	postupke za utvrđivanje i procjenjivanje postojanja IKT rizika koji proizilaze iz bilo kakvih većih promjena u IKT sistemu ili uslugama, IKT procesima i/ili nakon svakog značajnijeg operativnog ili IKT incidenta.		
Član 14.	Sadržaj okvira za upravljanje IKT rizicima	(3)		Banka je dužna adekvatno dokumentovati proces upravljanja IKT rizicima.		
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(1)		Banka je dužna kontinuirano identifikovati IKT rizike.		
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(2)		U okviru identifikacije IKT rizika, banka je dužna:		
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(2)	a)	identifikovati i dokumentovati svoje poslovne funkcije, uloge i podržavajuće procese,		
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(2)	b)	identifikovati i uspostaviti mapiranje informacione i IKT imovine kojom se pruža podrška identifikovanim poslovnim funkcijama i podržavajućim procesima iz tačke a) ovog stava, kao što su IKT sistemi, uposlenici, izvođači i treće strane, te njihove međusobne povezanosti, te dokumentovati i redovno ažurirati,	**Komentar:** 1. molimo pojašenjenje stava (5). Da li funkcija upravljanja IKT rizicima može preispitivati adekvatnost klasifikacije informacione i IKT imovine koja je izvršena od vlasnika iste? 2. kome pripada odgovornost za klasifikaciju informacione imovine? i da li je infomaciona imovina podaci koji se čuvaju u sistemu. 3. Šta se podrazumijeva pod "klasifikovati identifikovane poslovne funkcije"? U odnosu na šta se klasifikuju, da li postoji neka kategorizacija ili skala za klasifikaciju?	**Komentar:** 1. Stavom se definiše da je banka dužna preispitati adekvatnost prethodno urađene klasifikacije informacione i IKT imovine.U slučaju da se analizom odnosno procjenom rizika utvrde neki novi rizici odnosno promijeni nivo rizika, potrebno je preispitati adekvatnost ranije klasifikovane informacione i IKT imovine, u dogovoru sa vlasnikom navedene imovine. 2. Odgovornost za klasifikaciju imovine je na vlasniku imovine. Definicija informacione imovine je uključena u član 2 sa definicijama. 3. Stav (4) definiše da je potrebno "klasifikovati identifikovane poslovne funkcije". Dakle, identifikovane poslovne funkcije je potrebno procijeniti u pogledu povjerljivosti, integriteta i dostupnosti i klasifikovati. 4. Banka je dužna identifikovati međusobne ovisnosti pružaoca usluge, utvrđujući njihove međusobne povezanosti, u smislu podizvođača ili neke druge ovisnosti jednog pružaoca usluga o
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(2)	c)	identifikovati i dokumentovati sve procese ovisne o trećim stranama pružaocima IKT usluga i identifikovati međusobne ovisnosti pružaoca usluga.		
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(3)		U okviru mapiranja iz stava (2) tačka b) ovog člana, banka je dužna mapirati svu IKT imovinu, uključujući i onu na udaljenim lokacijama, mrežne resurse i hardware-sku opremu, te mapirati i konfiguracije IKT imovine, te veze između različite IKT imovine i njihove međuovisnosti.		

Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(4)		Banka je dužna klasifikovati identifikovane poslovne funkcije, podržavajuće procese i informacionu i IKT imovinu iz stava (2) ovog člana, uzimajući u obzir zahtjeve u pogledu povjerljivosti, integriteta i dostupnosti.	4. Molimo pojašnjenje na šta se misli pod "... identifikovati međusobne ovisnosti pružaoca usluge"?	međusobne povezanosti, u smislu podizvođača ili neke druge ovisnosti jednog pružaoca usluga o drugome. Cilj ove odredbe je utvrditi i procijeniti adekvatno rizik ovisnosti o svakom pružaocu usluga ponaosob. Ukoliko pružalac usluga A je na neki način povezan sa pružaocem usluga B, te oba pružaoca usluga pružaju usluge banci, u slučaju problema u poslovanju pružaoca usluga B, jasno je da će se to odraziti i na poslovanje pružaoca usluga A i njegove usluge prema banci. Zbog toga je potrebno unaprijed identifikovati ključne veze između pružaoca usluga banke.
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(5)		Prilikom procjene rizika, banka je dužna preispitati adekvatnost klasifikacije informacione i IKT imovine.		
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(6)		Banka je dužna odrediti jasnu odgovornost za informacionu i IKT imovinu.		
Član 15.	Identifikovanje rizika (funkcija, procesa i imovine)	(7)		Banka je dužna osigurati relevantnu evidenciju za potrebe stava (1) i (2) ovog člana, te ih održavati ažurnom, a naročito nakon svake značajne izmjene.		
Član 16.	Procjena rizika	(1)		Banka je dužna redovno mjeriti, odnosno procjenjivati IKT rizike koje je identifikovala.	**Komentar:** 1. molimo pojašnjenje stava (5) budući da nije jasno na koje druge finansijske institucije se misli, da li se navedeno odnosi na bankarsku grupu?	**Komentar:** 1. Misli se na sve finansijske subjekte sa kojima je banka na neki način povezana, prima usluge od njih ili im pruža.
Član 16.	Procjena rizika	(2)		U okviru procjene IKT rizika, banka je dužna identifikovati IKT rizike koji utiču na klasifikovane poslovne funkcije, podržavajuće procese i informacionu imovinu, iz člana 15. ove odluke.		
Član 16.	Procjena rizika	(3)		Banka je dužna provoditi i dokumentovati procjenu IKT rizika na godišnjoj osnovi ili češće, a obavezno u slučaju važnije promjene u IKT sistemu, postupcima ili procedurama koji utiču na poslovne funkcije, podržavajuće procese ili IKT imovinu.		
Član 16.	Procjena rizika	(4)		Banka je dužna najmanje jedanput godišnje provoditi posebnu procjenu IKT rizika za sve zastarjele IKT sisteme, a obavezno prije i nakon povezivanja tehnologija, aplikacija ili sistema.		
Član 16.	Procjena rizika	(5)		Banka je dužna osigurati kontinuiranu identifikaciju svih izvora IKT rizika, posebno izloženost riziku drugih finansijskih subjekata i od drugih finansijskih subjekata, te procjenjivati prijetnje, uključujući i cyber prijetnje, i ranjivosti IKT sistema koje su relevantne za poslovne funkcije, podržavajuće procese i informacionu i IKT imovinu banke. Banka je dužna redovno, a najmanje jednom godišnje, preispitivati scenarije rizika koji utiču na njih, uključujući cyber rizike.		
Član 17.	Ovladavanje rizicima	(1)		Banka je dužna jasno i precizno odrediti i primjenjivati kriterije za odlučivanje i postupke za ovladavanje IKT rizicima, uzimajući u obzir rizični profil banke, odnosno sklonost banke ka preuzimanju IKT rizika, određenu strategijom rizika.		
Član 17.	Ovladavanje rizicima	(2)		Na osnovu procjene IKT rizika iz člana 16. ove odluke, banka je dužna identifikovati i implementirati potrebne kontrole za ovladavanje IKT rizicima, uključujući i potrebne promjene u postojećim poslovnim procesima, kontrolnim mjerama, IKT sistemu i IKT uslugama, osigurati svođenje IKT rizika na prihvatljivi nivo rizika , te zaštititi informacionu i IKT imovinu u skladu sa njezinom klasifikacijom.		
Član 17.	Ovladavanje rizicima	(3)		Banka je dužna uzeti u obzir vrijeme potrebno za provođenje identifikovanih kontrola iz stava (2) ovog člana, kao i vrijeme potrebno za poduzimanje odgovarajućih privremenih kontrola za smanjenje IKT rizika, a kako bi ti rizici ostali unutar ograničenja sklonosti preuzimanju IKT rizika banke.		
Član 17.	Ovladavanje rizicima	(4)		Kontrolama iz stava (2) ovog člana, banka je dužna:		
Član 17.	Ovladavanje rizicima	(4)	a)	osigurati sigurnost sredstava za prenos podataka,		

UPRAVLJANJE IKT RIZICIMA	Član 17.	Ovladavanje rizicima	(4)	b)	na najmanju moguću mjeru svesti rizik od oštećenja ili gubitka podataka, neovlaštenog pristupa i tehničkih nedostataka koji mogu narušiti poslovanje,	**Komentar:** 1. potrebno detaljnije pojasniti stav (3) ovog člana 2. pojasniti na šta se odnosi odredba iz stava (4) tačka a) 3. Da li znači da je funkcija upravljanja ikt rizicima odgovorna za kreiranje politike sigurnosti informacionog sistema I koja će biti iznad CISO funkcije? Na koji način Odluka tretira fizičku sigurnost informacionog sistema? 4. Da li je priprema i ažuriranje Politike informacione sigurnosti u nadležnosti Lica zaduženog za sigurnost IKT sistema (CISO) kako je definisano članom 6 ili nadležnost kontrolne funkcije upravljanja rizicima?	**Komentar:** 1. Ukoliko banka procjenom rizika identifikuje određeni rizik koji je potrebno tretirati, ali vrijeme potrebno za implementaciju definisanih trajnih mjera zahtijeva duži vremenski period, banka je dužna navedeno uzeti u obzir i implementirati privremene mitigacione mjere u međuvremenu, kako ne bi bila izložena navedenom riziku, dok se ne završi implementacija prethodno definisanih trajnih mjera. 2. Odredba iz stava (4) tačka a) se odnosi na kontrole zaštite podataka u prenosu, npr korištenjem enkripcijskih mjera. Navedeno će biti predmetom detaljnijeg definisanja kroz Uputstva. 3. Na ovo pitanje je dat odgovor kroz prethodna pitanja. Fizička sigurnost informacionog sistema je dio rizika ikt sistema. 4. Na ovo pitanje je ranije dat odgovor.
	Član 17.	Ovladavanje rizicima	(4)	c)	spriječiti umanjenje dostupnosti, narušavanje autentičnosti i integriteta, kršenje povjerljivosti i gubitka podataka i		
	Član 17.	Ovladavanje rizicima	(4)	d)	osigurati da su podaci zaštićeni od rizika koji proizilaze iz upravljanja podacima, uključujući propuste u administraciji, rizike vezane uz obradu podataka i ljudske greške.		
	Član 17.	Ovladavanje rizicima	(5)		U sklopu okvira za upravljanje IKT rizicima, Banka je dužna:		
	Član 17.	Ovladavanje rizicima	(5)	a)	propisati, provoditi i redovno ažurirati politiku informacione sigurnosti, kojom se definišu pravila za zaštitu dostupnosti, autentičnosti, integriteta i povjerljivosti podataka, informacione i IKT imovine, kako bi se postigli ciljevi u području informacione sigurnosti,		
	Član 17.	Ovladavanje rizicima	(5)	b)	primjenom pristupa koji se zasniva na procjeni rizika, uspostaviti pouzdanu strukturu za upravljanje mrežom i infrastrukturom pomoću odgovarajućih tehnika, metoda i protokola, koji mogu uključivati automatizovane mehanizme za izolaciju zahvaćene informacione i IKT imovine u slučaju cyber napada (mogućnost trenutnog prekida ili segmentiranja kako bi se u najvećoj mogućoj mjeri spriječila zaraza),		
	Član 17.	Ovladavanje rizicima	(5)	c)	propisati i provoditi procedure, postupke i kontrole kojima se ograničava fizički ili logički pristup informacionoj i IKT imovini samo na ono što je nužno za legitimne i odobrene funkcije i aktivnosti, te u tu svrhu implementirati postupke i kontrole koji se odnose na prava pristupa i osiguravaju dobro upravljanje njima,		
	Član 17.	Ovladavanje rizicima	(5)	d)	propisati i provoditi procedure, postupke i kontrole za pouzdane mehanizme autentifikacije, na osnovu relevantnih standarda i namjenskih kontrolnih sistema, te mjere za zaštitu kriptografskih ključeva, kojima se podaci, u mirovanju i prijenosu, šifriraju, a na osnovu rezultata klasifikacije podataka i procjene IKT rizika,		
	Član 17.	Ovladavanje rizicima	(5)	e)	propisati i provoditi procedure za upravljanje promjenama IKT-a, a u skladu sa članom 40. ove odluke		
	Član 17.	Ovladavanje rizicima	(5)	f)	propisati i provoditi odgovarajuće i sveobuhvatne dokumentovane postupke za upravljanje ažuriranjima software-a, kao i upravljanje zaštitom od malicioznog koda,		
	Član 17.	Ovladavanje rizicima	(5)	g)	propisati i provoditi procedure upravljanja IKT imovinom, a u skladu sa članom 37. ove odluke,		
	Član 17.	Ovladavanje rizicima	(5)	h)	propisati i provoditi odgovarajuće procedure izrade i upravljanja sigurnosnim kopijama, a u skladu sa članom 35. ove Odluke,		
	Član 17.	Ovladavanje rizicima	(5)	i)	propisati i provoditi odgovarajuće planove kontinuiteta poslovanja iz oblasti IKT sistema, te planove odgovora i oporavka, a u skladu sa članom 32. ove Odluke i		
	Član 17.	Ovladavanje rizicima	(5)	j)	propisati i provoditi odgovarajuće programe i planove osposobljavanje i podizanja svijesti o informacionoj sigurnosti, u skladu sa članom 21. ove Odluke.		
	Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(1)		Banka je dužna uspostaviti sistem redovnog praćenja, nadzora i izvještavanja o IKT rizicima.		
	Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(2)		U okviru redovnog praćenja IKT rizika, Banka je dužna uspostaviti kontrole za kontinuiran nadzor IKT sistema i pravovremeno otkrivanje neobičnih aktivnosti, u skladu sa članom 41. ove Odluke, a što uključuje i probleme sa performansama IKT sistema i IKT incidente, te identifikaciju mogućih važnih jedinstvenih tačaka prekida.		

Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(3)		Banka je dužna kontrole iz stava (2) ovog člana osigurati na višestrukim nivoima, definisati pragove upozorenja i kriterije za aktiviranje i pokretanje procesa odgovora na IKT incidente, uključujući mehanizme za automatsko upozoravanje relevantnog osoblja zaduženog za odgovor na IKT incidente.	**Komentar:** 1. Da li će stav (5) biti pojašnjen dodatno uputstvima? Ako ne molimo pojašenjnje. 2. Na koji način će se definisati metrika za dovoljno adekvatnih resursa? 3. Da li je stav (7) tačke a) i b) odgovornost funkcije prve ii druge linije odbrane? molimo pojašnjenje. 4. Čija je nadležnost kreiranje izvještaja predviđenih stavom (8)? koja vrsta izvještaja? da li će isti biti popisani dodacima odluke?	**Komentar:** 1. Banka je dužna provjeravati efikasnost uspostavljenih kontrola u svrhu umanjivanja identifikovanih rizika. Npr, kao odbranu od malicioznog software banka je definisala kroz tretman rizika upotrebu antivirusnog rješenja. Banka je dužna kontrolisati da li je navedeno rješenje funkcionalno i umanjuje navedeni rizik u skladu sa ciljem njegove implementacije. 2. Ranije je dat odgovor na pitanje vezano uz adekvatnost i broj resursa. Navedeno ovisi o principima proporcionalnosti datim u članu 13., te obavezi banke da osigura adekvatan kontinuitet kvalitetnog funkcionisanja svojih poslovnih procesa. 3. Navedeno pod a) je odgovornost prve linije odbrane, dok je pod b) odgovornost druge linije odbrane. 4. Nadležnost kreiranja izvještaja o adekvatnosti upravljanja IKT rizicima je u nadležnosti funkcije upravljanja IKT rizicima. Banka je dužna sama propisati način izvještavanja, uključujući potrebne elemente koji su definisani ovim članom.
Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(4)		Banka je dužna osigurati adekvatno razdvajanje dužnosti uposlenika u procesu nadzora i procesima koji su predmet nadzora.		
Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(5)		Pri obavljanju kontrole IKT rizika, banka je dužna provjeravati uspostavljene kontrole za ovladavanje IKT rizicima, te vršiti ocjenu njihove efektivnosti i efikasnosti, uključujući i kontrole testiranja digitalne operativne otpornosti definisane članom 23. – 27. ove odluke.		
Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(6)		Banka je dužna kontinuirano pratiti i utvrđivati utiču li promjene u postojećem operativnom okruženju na implementirane kontrole, te da li je potrebno uvođenje dodatnih kontrola radi smanjivanja povezanih IKT rizika. Navedene promjene trebaju biti sastavnim dijelom formalnog procesa upravljanja promjenama.		
Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(7)		Banka je dužna osigurati dovoljno adekvatnih resursa, uključujući i osposobljene uposlenike za:		
Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(7)	a)	praćenje aktivnosti korisnika, nastanka neobičnih pojava u IKT sistemu i IKT incidenata, a naročito cyber napada i		
Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(7)	b)	prikupljanje informacija o ranjivostima, cyber prijetnjama i IKT incidentima, a osobito cyber napadima, te za analizu njihovog vjerovatnog uticaja na digitalnu operativnu otpornost banke.		
Član 18.	Praćenje, nadzor i izvještavanje o IKT rizicima	(8)		Banka je dužna uključiti izvještavanje o IKT rizicima, u okviru izvještavanja o rizicima, te u okviru izvještaja dati jasan prikaz aktuelne situacije u pogledu digitalne operativne otpornosti, i to na bazi broja prijavljenih značajnih IKT incidenata i efikasnosti preventivnih kontrola.		
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(1)		Banka je dužna osigurati i dokumentovati proces preispitivanja okvira za upravljanje IKT rizicima, najmanje jednom godišnje, kao i	**Komentar:**	**Komentar:**
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(1)	a)	nakon značajnih IKT incidenata, cyber napada, iskustava iz testova (npr penetracioni testovi, TLPT, testovi kontinuiteta poslovanja IKT-a, planovi za odgovor i oporavak i sl.), uputa iz revizija i drugo,		
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(1)	b)	bez odgađanja u slučaju identifikacije značajnih slabosti i nedostataka u okviru kritičnih (vitalnih) IKT sistema i		
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(1)	c)	obavezno nakon svake značajne promjene u IKT sistemu, procesima ili procedurama koje utiču na poslovne funkcije koje se podržavaju IKT sistemom, te IKT imovinu,		
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(1)		te ga kontinuirano poboljšavati na osnovu „naučenih lekcija" tokom njegovog provođenja i praćenja.		

Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(2)		Banka je dužna lekcije stečene iz testiranja digitalne operativne otpornosti, te iz stvarnih IKT incidenata, posebno cyber napada, kao i problema pri aktivaciji planova kontinuiteta poslovanja IKT-a, te planova odgovora i oporavka u području IKT-a, zajedno sa relevantnim informacijama razmijenjenim sa partnerskim finansijskim subjektima i procjenama prilikom revizije i supervizije, adekvatno i kontinuirano uključiti u proces procjene IKT rizika. Na osnovu navedenog, banka je dužna provoditi odgovarajuća preispitivanja relevantnih komponenti okvira za upravljanje IKT rizikom i njihove adekvatnosti.	**Komentar:** 1. U čijoj nadležnosti bi bilo provođenje odredbi stava (4)? Molimo pojašnjenje. 2. U odnosu na stav 1 - da li je potrebno ažurirati svaki put strategiju, politike, procedure u svim navedenim slučajevima i šta se u stvari podrazumijeva pod 'osigurati i dokumentovati proces preispitivanja okvira za upravljanje IKT rizicima'?	1. Oboje je prvenstveno zadatak druge linije odbrane - funkcije upravljanja IKT rizicima. 2. Banka je dužna osigurati pisani trag o izvršenom procesu preispitivanja okvira za upravljanja IKT rizicima, nakon pojave događaja definisanih ovim stavom. U slučaju da se preispitivanjem zaključi da je potrebno implementirati novu kontrolnu mjeru, kontrolu, promijeniti odnosno poboljšati određeni proces i slično, potrebno je izmijeniti interni akt kojim se definiše predmetno. U suprotnom, potrebno je imati dokument kojim se pokazuje da je izvršena analiza te da je izveden zaključak da nove kontrolne mjere nisu potrebne, odnosno da su implementirane mjere dovoljne.
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(3)		Banka je dužna pratiti razvoj IKT rizika tokom vremena, analizirati učestalost, vrste, veličinu i razvoj IKT incidenata, a naročito cyber napada i njihovih obrazaca, a u svrhu razumijevanja nivoa izloženosti IKT riziku i unapređenja cyber zrelosti i spremnosti banke.		
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(4)		Banka je dužna propisati, provoditi i na adekvatan način dokumentovati:		
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(4)	a)	redovno praćenje relevantnih novih tehnologija kako bi bolje razumjela mogući uticaj tih tehnologija na zahtjeve u pogledu IKT sigurnosti i digitalne operativne otpornosti. i		
Član 19.	Preispitivanje i poboljšavanje okvira upravljanja IKT rizicima	(4)	b)	redovno praćenje najnovijih praksi upravljanja IKT rizikom, kako bi bila u mogućnosti efikasno odgovoriti na trenutne ili nove oblike cyber napada.		
Član 20.	Komunikacija	(1)		U sklopu okvira za upravljanje IKT rizicima, banka je dužna definisati planove komunikacije u krizi, kojima će se uspostaviti jasni postupci za upravljanje internom i eksternom komunikacijom u slučaju aktiviranja planova kontinuiteta IKT-a ili planova odgovora i oporavka IKT sistema, uključujući i značajne IKT incidente.	**Komentar:** 1. Molimo pojašnjenje termina značajni IKT incidenti? Da li će upustvima biti definisani detalji vezani za klasifikaciju incidenata i unificiranje? 2. U odnosu na stav (4), molimo pojašnejnje na kakvu evidenciju aktivnosti prije poremećaja u radu se misli, s obzirom da prije poremećaja imamo redovne operativne aktivnosti.	**Komentar:** 1. Da, upustvima će biti definisani detalji vezani za klasifikaciju incidenata i unificiranje. 2. Banka je dužna osigurati adekvatne kontinuirane zapise o procesima i aktivnostima, a koji mogu poslužiti za analizu uzroka određenog poremećaja, te adekvatnih dokaza u eventualnom sudskom procesu.
Član 20.	Komunikacija	(2)		U okviru planova komunikacije u krizi, banka je dužna uzeti u obzir različite potrebe komunikacije za interne uposlenike i eksterne učesnike, kao i razlike u potrebama uposlenika uključenih u upravljanje IKT incidentom, posebno osoblja nadležnog za odgovor i oporavak, od osoblja koje je potrebno samo informisati.		
Član 20.	Komunikacija	(3)		Banka je dužna osigurati odgovornu objavu barem značajnih IKT incidenata ili ranjivosti, klijentima, javnosti i partnerskim finansijskim subjektima, ovisno o IKT incidentu.		
Član 20.	Komunikacija	(4)		U slučaju aktivacije planova kontinuiteta IKT-a ili planova odgovora i oporavka IKT-a, uključujući i značajne IKT incidente, banka je dužna voditi evidenciju aktivnosti prije i nakon poremećaja u radu, koja treba biti lako dostupna.		
Član 21.	Osposobljavanje i podizanje nivoa svijesti o sigurnosti IKT sistema	(1)		Banka je dužna uspostaviti i provoditi program za osposobljavanje, uključujući program podizanja svijesti o sigurnosti IKT sistema i digitalnoj operativnoj otpornosti, za sve svoje uposlenike, a kako bi osigurala da su pravovremeno osposobljeni za izvršavanje dužnosti i odgovornosti u skladu sa politikom informacione sigurnosti i postupcima u cilju smanjenja ljudskih pogrešaka, krađa, prevara, zloupotreba ili gubitaka.	**Komentar:**	**Komentar:** 1. Banka je dužna educirati svoje pružaoce IKT usluga u onoj mjeri u kojoj je to potrebno radi

Član 21.	Osposobljavanje i podizanje nivoa svijesti o sigurnosti IKT sistema	(2)		Programom osposobljavanja trebaju biti pravovremeno obuhvaćeni svi zaposlenici, uključujući i više rukovodeće osoblje, a nivo njihove složenosti treba biti srazmjeran nadležnostima njihovih funkcija i odgovornosti. Banka je dužna, prema potrebi, u programe osposobljavanja, uključiti i treće strane pružaoce IKT usluga.	1. Stavom (2) ovog člana definisano je da se u programe osposobljavanja, uključe i treće strane pružaoci IKT usluga. Na koji način i u kojem opsegu, kako to definisati, kako će Banka edukovati pružaoce IKT usluga? Da li se ovdje misli na awareness ili stručne edukacije ili šta već?	1. Banka je dužna educirati svoje pružaoce IKT usluga u onoj mjeri u kojoj je to potrebno radi osiguranja sigurnosti svog IKT sistema. Banka je dužna procijeniti rizik koji postoji prilikom angažovanja trećih strana pružaoca IKT usluga, te u skladu sa tom procjenom, primijeniti adekvatne mjere zaštite svog IKT sistema i svojih poslovnih procesa. Te mjere uključuju i edukaciju kadra pružaoca IKT usluga, u onoj mjeri u kojoj je to potrebno.
Član 21.	Osposobljavanje i podizanje nivoa svijesti o sigurnosti IKT sistema	(3)		Banka je dužna osigurati da se programom osposobljavanja obezbijedi osposobljavanje uposlenika redovno, a najmanje jednom godišnje, vodeći posebno računa o pravovremenom osposobljavanju u pogledu prepoznatih IKT prijetnji.		
Član 22.	Edukacija	(1)		Banka je dužna da osigura stručno osposobljavanje i kontinuiranu edukaciju zaposlenika u organizacionoj jedinici IKT-a i upravljanja sigurnošću IKT sistema, kao i internog revizora IKT sistema, a kako bi osigurala da su navedeni uposlenici pravovremeno i adekvatno osposobljeni za obavljanje svojih funkcija, uzimajući u obzir razvoj IKT i IKT rizika, te veličinu i kompleksnost IKT sistema u banci.	**Komentar:** 1. vezano za odredbu stava (1) molimo pojašnejnje da li su uključeni u edkuaciju i zaposlenici funkcije upravljanja IKT rizicima? 2. Zašto su izuzeti uposlenici kontrolne funkcije upravljanja rizicima koji su u skladu sa članom 12, stav 4 odgovorni za kontrolu i nadzor nad IKT rizicima 3. Odgovornost za izbor i organizaciju edukacije, koju instancu je potrebno izvještavati na kvartalnom nivou? Da li je to prečesto? Da li se ovdje misli na uključenost HR-a u sprovođenje Odluke? 4. Član 9 Stav (2), c), d), i f) - Definicija kontinuirano ispitivanja efikasnosti planova nije jasna. Naime, jasno nam je da Banka treba kreirati planove edukacije, budežtirati edukacije, provesti ih, ali na koji način validirati efikasnost plana edukacije i šta to podrazumijeva?	**Komentar:** 1. da, zaposlenici funkcije upravljanja IKT rizicima su također uključeni u navedeni član. 2. odgovor je dat u prethodnom pitanju. 3. HR treba biti uključen u planiranje, provođenje i izvještavanje o realizovanoj edukaciji. Kvartalno izvještavanje je prema Upravi banke. 4. Za edukaciju stručnih kadrova, naročito u oblasti IKT, sigurnosti IKT, IKT revizije i upravljanja IKT rizicima potrebno je planirati niz adekvatnih edukacija u cilju osposobljavanja navedenih uposlenika u planiranom vremenskom periodu. Tokom navedenog perioda, odnosno na njegovom isteku potrebno je validirati da li su navedeni uposlenici stekli potrebna znanja i da li su osposobljeni za obavljanje svojih radnih zadataka, a što je bilo cilj edukacije, te da li je u tom smislu navedena edukacija bila kvalitetna i dovoljna. U okviru Uputstava će dalje biti razrađen navedeni član, također.
Član 22.	Edukacija	(2)		Banka je dužna izraditi detaljni godišnji plan edukacije uposlenika, definisati vremenske rokove, dokumentovati njegovu realizaciju, te kvartalno izvještavati o realizaciji plana.		
Član 22.	Edukacija	(3)		Banka je dužna kontinuirano ispitivati efikasnost svojih planova edukacije i, ako je potrebno, ažurirati ih, kako bi osigurala da su obuke adekvatne i primjerene veličini i kompleksnosti IKT sistema, IKT rizicima, kao i da prate razvoj novih IKT i IKT rizika, uključujući i cyber rizike.		

	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(1)		U okviru za upravljanje IKT rizicima, Banka je dužna definisati, provoditi i redovno ažurirati Politiku za testiranje digitalne operativne otpornosti i procedure za testiranje digitalne operativne otpornosti, a u svrhu procjene pouzdanosti i efikasnosti implementiranih kontrola i spremnosti na postupanje prilikom IKT incidenata.		
	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(2)		Politika i procedure za testiranje digitalne operativne otpornosti iz stava (1) ovog člana trebaju uključiti niz procjena, testova, metodologija, postupaka i alata koji se primjenjuju u skladu sa članom 23.- 27. ove odluke.		
	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(3)		Politikom i procedurama za testiranje digitalne operativne otpornosti banka je dužna primijeniti pristup zasnovan na procjeni rizika, a uzimajući u obzir razvoj IKT rizika, sve konkretne rizike kojima je banka izložena ili bi mogla biti izložena, kritičnost informacione i IKT imovine i usluga, kao i ostale faktore koje banka smatra odgovarajućim. Programom testiranja potrebno je uzeti u obzir i prijetnje i ranjivosti utvrđene praćenjem prijetnji te postupcima procjene IKT rizika.		
	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(4)		Banka je dužna osigurati da testiranja provode neovisne interne ili vanjske osobe s dovoljno znanja, vještina i stručnosti u testiranju mjera sigurnosti IKT sistema, osiguravajući izbjegavanje sukoba interesa u fazama dizajna i provođenja testa, te osiguravajući dovoljna sredstva u tu svrhu.		
	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(5)		Banka je dužna uspostaviti postupke za prioritizaciju, klasifikaciju i otklanjanje svih slabosti i nedostataka otkrivenih izvođenjem testova iz stava (2) ovog člana, te metodologiju interne provjere kako bi se utvrdilo da su sve identifikovane slabosti i nedostaci u potpunosti otklonjeni. U slučaju prioritetnih (važnih) IKT sistema, Banka je dužna bez odgađanja otkloniti identifikovane slabosti i nedostatke.	**Komentar:** 1. da li se u okviru stava (1) misli na proširenje zahtjeva postojećih DR procedura i planova i testiranja? 2. Da li će biti dodatnih pojašnjenja kroz uputstva?	**Komentar:** 1. Politika za testiranje digitalne operativne otpornosti spada u testove provjere efikasnosti kontrolnih mjera, te obuhvata npr penetracione i vulnerability testove, kao i scenarije ransomware napada, dok DR centar spada u postupke odgovora. 2. Da, TLPT testovi će biti dalje pojašnjeni kroz uputstva.
	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(6)		Banka je dužna osigurati obavljanje primjerenih testova IKT sistema, pri čemu:		
	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(6)	a)	za sve IKT sisteme i aplikacije kojima se podupiru prioritetne (važne) funkcije banke se testiranje provodi barem jedanput godišnje,		
	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(6)	b)	za IKT sisteme koji nisu kritični, proporcionalno rizicima, testiranje se provodi barem jedanput svake tri godine,		

	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(6)	c)	prije svake izmjene postojeće ili dodavanja nove komponente IKT sistema i usluga, u slučaju da se radi o podržavanju prioritetnih (važnih) funkcija, kao i u slučaju značajnih izmjena IKT procesa i infrastrukture, uključujući promjene provedene zbog IKT incidenata, i		
	Član 23.	Testiranje digitalne operativne otpornosti (digital operational resilience testing)	(6)	d)	u slučaju implementacije novih ili znatno izmijenjenih aplikacija dostupnih putem interneta.		
	Član 24.	Sadržaj testiranja informacione sigurnosti (digital operational resilience testing)			Politikom i procedurama za testiranje digitalne operativne otpornosti iz člana 23. ove odluke, treba da obuhvataju izvođenje odgovarajućih testova, kao što su procjene i skeniranja ranjivosti, analize javno dostupnih izvora, procjene mrežne sigurnosti, analize odstupanja, preispitivanja fizičke sigurnosti, upitnici i software-ska rješenja za skeniranje, preispitivanja izvornog koda ako je to izvedivo, testiranja na osnovu scenarija, testiranje kompatibilnosti, testiranje performansi, integralno testiranje (eng. end-to-end testing) i penetracijsko testiranje. Testiranja na osnovu scenarija trebaju obuhvatiti i scenarije relevantnih i poznatih potencijalnih napada , a na osnovu uočenih sigurnosnih prijetnji.	**Komentar:** 1.da li se ovdje misli na proširenje zahtjeva postojećih DR procedura i planova i testiranja? Da li će biti dodatnih pojašnjenja kroz uputstva?	**Komentar:** 1. TLPT testovi će biti predmetom posebnih uputstava. DR planovi se ubrajaju u planove oporavka, što je pojašnjeno u ranijim odgovorima.
TESTIRANJE DIG	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(1)		Banka je dužna provoditi napredno testiranje sigurnosti IKT sistema u obliku penetracijskog testiranja vođenim prijetnjama (TLPT) najmanje jednom u 3 godine. Uzimajući u obzir rizik banke i operativne okolnosti, Agencija može, kada je to potrebno, tražiti od banke da smanji ili poveća ovu učestalost.		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(2)		TLPT-jem iz stava (1) ovog člana je potrebno obuhvatiti više ili sve prioritetne (važne) funkcije banke. TLPT je potrebno provoditi na produkcijskom sistemu koji podržava te funkcije.		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(3)		Banka je dužna identifikovati sve relevantne IKT sisteme, procese i tehnologije, kojima se podržavaju prioritetne (važne) funkcije, kao i IKT usluge, uključujući i one koje su eksternalizovane/ugovorene sa IKT pružaocima usluga, a kojima se podržavaju prioritetne (važne) funkcije.		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(4)		Banka je dužna procijeniti koje prioritetne (važne) funkcije će biti obuhvaćene TLPT-om, te rezultat procjene dostaviti Agenciji.		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(5)		Ako su treće strane pružaoci IKT usluga obuhvaćeni TLPT-om, banka je dužna poduzeti sve potrebne i zaštitne mjere kako bi osigurala učešće takvih trećih strana pružaoca IKT pružaoca usluga u TLPT-u. Banka u svakom trenutku zadržava potpunu odgovornost za osiguravanje usklađenosti sa ovom odlukom.		

DIGITALNE OPERATIVNE OTPORNOSTI	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(6)		Ne dovodeći u pitanje stav (2) i (3), u slučaju kada se opravdano može očekivati da će sudjelovanje treće strane pružaoca IKT usluga iz stava (5) ovog člana, negativno uticati na kvalitet ili sigurnost usluga odnosno povjerljivost podataka povezanih sa takvim uslugama, a koji se odnose na klijente treće strane pružaoca IKT usluga koji nisu obuhvaćeni primjenom ove odluke, banka se može pismeno dogovoriti sa trećom stranom pružaocem IKT usluga da treća strana pružalac IKT usluga direktno angažuje eksterne provoditelje testiranja. U tom slučaju, TLPT se provodi pod vodstvom jedne imenovane banke, udruženog TLPT-a, u kojem učestvuje nekoliko banaka (eng. pooled testing) kojima treća strana pružalac IKT usluga pruža iste usluge.	**Komentar:** 1. Vezano za stav (11), molimo pojašnjenje na koju se potvrdu misli, s obzirom da stav (9) ne tretira pitanje nikakve potvrde. Da li se misli na stav 10: "...planove za ispravljanje nedostataka i dokumentaciju kojom se potvrđuje da je TLPT proveden u skladu sa zahtjevima."	**Komentar:** 1. Ovaj stav se odnosi isključivo na slučaj da banka učestvuje u grupnom testiranju u okviru svoje bankarske grupe, te je u navedeno testiranje uključeno drugo nadležno tijelo, izvan BiH. Ovaj član se ne odnosi na grupna testiranja koja se obavljaju u okviru BiH gdje je Agencija nadležno tijelo.
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(7)		Udruženim TLPT-jem iz stava (6) ovog člana potrebno je obuhvatiti relevantan obim IKT usluga koje podržavaju prioritetne (važne) funkcije koje su banke ugovorile sa trećom stranom pružaocem IKT usluga. Broj banaka koje učestvuju u udruženom TLPT-ju treba biti srazmjeran složenosti i vrsti uključenih usluga.		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(8)		Udruženi TLPT smatra se TLPT-jem koji provode banke koje učestvuju u udruženom TLPT-ju i na njega se primjenjuju odredbe ove odluke.		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(9)		Banka je dužna, u saradnji sa trećim stranama pružaocima IKT usluga i drugim uključenim stranama, uključujući provoditelje testiranja, ali isključujući Agenciju, primjenjivati efektivne (adekvatne) kontrole upravljanja rizicima kako bi ublažila rizike od mogućeg uticaja na podatke, od oštećenja imovine i od poremećaja u radu prioritetnih (važnih) funkcija, usluga ili operacija u samoj banci, njenim partnerima ili finansijskom sektoru.		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(10)		Banka je dužna, na kraju testiranja, nakon što su usaglašeni izvještaji i planovi za ispravljanje nedostataka, dostaviti Agenciji sažetak relevantnih nalaza, planove za ispravljanje nedostataka i dokumentaciju kojom se potvrđuje da je TLPT proveden u skladu sa zahtjevima.		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(11)		U slučaju da banka učestvuje u grupnom testiranju, pritkom čega drugo nadležno tijelo izvan zemlje izdaje potvrdu iz stava (9), banka je dužna Agenciji dostaviti potvrdu, sažetak relevantnih nalaza i planove za ispravljanje		
	Član 25.	Napredno testiranje sigurnosti IKT sistema (TLPT)	(12)		Ne dovodeći u pitanje takvu potvrdu, banka u svakom slučaju ostaje potpuno odgovorna za uticaje/posljedice testiranja iz stava (5).		
	Član 26.	Provoditelji testiranja TLPT	(1)		Banka je dužna angažovati provoditelje testiranja za potrebe obavljanja TLPT, a u skladu sa članom 27. ove odluke. U slučaju kada banka angažuje interne provoditelje testiranja za potrebe obavljanja TLPT-a, dužna je angažovati eksterne provoditelje testiranja za svaki treći test.		
	Član 26.	Provoditelji testiranja TLPT	(2)		Agencija će odrediti banke koje su dužne obavljati TLPT, kao i banke koje mogu koristiti interne provoditelje testiranja, na osnovu principa proporcionalnosti, a uzimajući u obzir sljedeće:	**Komentar:** 1. Da li će Banke dobiti definisanu metriku proporcionalnosti?	**Komentar:** 1. Agencija će objaviti listu banaka koje će biti dužne obavljati navedena TLPT testiranja.
	Član 26.	Provoditelji testiranja TLPT	(2)	a)	faktore povezane sa uticajem, posebno mjeru u kojoj usluge i aktivnosti koje banka pruža imaju na finansijski sektor u cjelini,		
	Član 26.	Provoditelji testiranja TLPT	(2)	b)	moguće probleme u pogledu finansijske stabilnosti, što uključuje sistemsku prirodu banke na nivou finansijskog sistema i		
	Član 26.	Provoditelji testiranja TLPT	(2)	c)	specifični profil IKT rizičnosti i nivo IKT zrelosti banke ili korištenih tehnoloških karakteristika.		

	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(1)		Banke su dužne angažovati provoditelje testiranja za izvođenje TLPT-a koji:		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(1)	a)	koji imaju zadovoljavajući nivo stručnosti i adekvatno iskustvo i reference, te su među najadekvatnijim i najuglednijim provoditeljima testiranja,		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(1)	b)	posjeduju tehničke i organizacijske sposobnosti i posebno stručno znanje u području saznanja o prijetnjama, penetracionom testiranju i testiranju „red tima“ (eng. red team),		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(1)	c)	su akreditovani u oblasti obavljanja penetracijskih testiranja međunarodno priznatim akreditacijama te se pridržavaju formalnih kodeksa ponašanja ili etičkih okvira,		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(1)	d)	pružaju nezavisno uvjerenje ili revizorski izvještaj u vezi sa adekvatnim upravljanjem rizicima povezanim sa provođenjem TLPT-a, uključujući odgovarajuću zaštitu povjerljivih informacija banke i pravnu zaštitu s obzirom na poslovne rizike banke i		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(1)	e)	su propisno i u potpunosti pokriveni odgovarajućim osiguranjem od profesionalne odgovornosti, uključujući i rizike od protupravnog i nemarnog postupanja.	**Komentar:** 1. da li će proces odobrenja Agencije za angažovanje internih provoditelja testiranja biti regulisan uputstvom i da li će biti predviđen rok za odgovor?	**Komentar:** 1. Navedeno će biti predmetom daljih uputstava.
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(2)		U slučaju anažovanja internih provoditelja testiranja, banka je dužna osigurati da, pored uslova iz stava (1) ovog člana, budu ispunjeni i sljedeći uslovi:		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(2)	a)	angažovanje internih provoditelja testiranja je odobreno od strane Agencije,		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(2)	b)	Agencija je potvrdila da banka ima dovoljno adekvatnih resursa, te da je osigurala izbjegavanje sukoba interesa prilikom dizajniranja i provođenja testa i		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(2)	c)	pružatelj informacija o prijetnjama nije dio banke.		
	Član 27.	Zahtjevi za provoditelje testiranja u vezi sa provođenjem TLPT	(3)		Banka je dužna osigurati da se ugovorom sklopljenim sa eksternim provoditeljima testiranja osigura adekvatno upravljanje rezultatima TLPT-a i da niti jedna obrada podataka s tim u vezi, uključujući proizvodnju, izradu, smještaj, obradu, izvještavanje, obavještavanje ili uništavanje, ne stvara rizike po banku.		

	Član 28.	Kontinuitet poslovanja u području IKT sistema	(1)		U sklopu okvira za upravljanje IKT rizicima, banka je dužna donijeti Strategiju upravljanja kontinuitetom poslovanja koja treba da sadrži ciljeve upravljanja kontinuitetom poslovanja sa jasnim kvantitativnim i kvalitativnim zahtjevima koji se odnose na dostupnost poslovnih funkcija i podržavajućih procesa banke, a vodeći računa o veličini i ukupnom profilu banke, kao i prirodi, obimu i složenosti svojih usluga, aktivnosti i poslovanja.		
	Član 28.	Kontinuitet poslovanja u području IKT sistema	(2)		Na osnovu Strategije upravljanja kontinuitetom poslovanja iz stava (1) ove odluke, banka je dužna donijeti Plan kontinuiteta poslovanja u području IKT sistema (Plan kontinuiteta IKT-a) koji je sastavni dio plana kontinuiteta poslovanja banke uzimajući u obzir identifikovane poslovne funkcije, procese i resurse IKT sistema iz člana 15. ove odluke.		
	Član 29.	Analiza uticaja na poslovanje	(1)		Banka je dužna provoditi analizu uticaja na poslovanje (eng. BIA) analiziranjem svoje izloženosti znatnijim prekidima poslovanja i procjenom njihovih potencijalnih efekata (uključujući na povjerljivost, integritet i dostupnost), kvantitativno i kvalitativno, upotrebom internih i/ili eksternih podataka i analizom scenarija.		
	Član 29.	Analiza uticaja na poslovanje	(2)		Analizom uticaja na poslovanje potrebno je uzeti u obzir kritičnost utvrđenih i mapiranih poslovnih funkcija, podržavajućih procesa, trećih strana i informacione imovine, kao i njihove međusobne zavisnosti, a u skladu sa članom		
	Član 29.	Analiza uticaja na poslovanje	(3)		U okviru analize uticaja na poslovanje potrebno je kao minimum:		
	Član 29.	Analiza uticaja na poslovanje	(3)	a)	navesti prioritetne (važne) funkcije i podržavajuće procese, a u skladu sa članom 15. stav (1) ove odluke,		
	Član 29.	Analiza uticaja na poslovanje	(3)	b)	navesti IKT imovinu potrebnu za odvijanje pojedinačnih poslovnih funkcija, kao i njihove međusobne zavisnosti i povezanosti, a u skladu sa članom 15. stav (2) ove odluke,		
	Član 29.	Analiza uticaja na poslovanje	(3)	c)	odrediti, kao minimum, RTO, RPO i SDO za svaku pojedinačnu poslovnu aktivnost, imajući u vidu eksternalizaciju i zavisnost od trećih strana.		
	Član 29.	Analiza uticaja na poslovanje	(4)		Pri utvrđivanju parametara RTO, RPO i MTD, banka je dužna uzeti u obzir i mogući opšti uticaj na cjelokupno finansijsko tržište. Navedenim parametrima banka je dužna osigurati da se u ekstremnim scenarijima postigne dogovoreni nivo usluga., a u skladu sa strategijom IKT- i ciljevima informacione sigurnosti.		
	Član 29.	Analiza uticaja na poslovanje	(5)		Banka je dužna osigurati da su IKT resursi i IKT usluge uspostavljeni i usklađeni sa analizom uticaja na poslovanje, a posebno u pogledu adekvatnog osiguranja redundantnosti ključnih (važnih) IKT komponenti, a kako bi se spriječili prekidi		
	Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(1)		Na osnovu analize uticaja na poslovanje banka je dužna donijeti Plan kontinuiteta IKT-a.		
	Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(2)		Planom kontinuiteta IKT-a banka je dužna osigurati:		
	Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(2)	a)	kontinuitet prioritetnih (važnih) funkcija banke u okviru definisanih RTO i RPO parametara,		
	Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(2)	b)	brze, adekvatne i efikasne odgovore na sve IKT incidente i njihovo rješavanje, na način kojim se ograničava šteta, a daje prioritet nastavku poslovanja i mjerama oporavka,		

Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(2)	c)	aktivaciju, bez odlaganja, ciljanih planova kojima se omogućavaju kontrole, procesi i tehnologije za suzbijanje širenja IKT incidenta i sprječavanja dalje štete, a koje su prilagođene svakoj vrsti IKT incidenta, kao i prilagođene postupke odgovora i oporavka uspostavljenih u skladu sa članom 31. ove odluke,		
Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(2)	d)	procjenu preliminarnog uticaja, štete i gubitka i		
Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(2)	e)	definisanje komunikacijskih mjera i mjera za upravljanje kriznim situacijama kojima se osigurava prenos ažurnih informacija svim relevantnim članovima banke i eksternim zainteresovanim stranama, a u skladu sa članom 20. ove odluke, i izvještavanje Agencije u skladu sa članom 44. ove odluke.		
Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(3)		Planom kontinuiteta IKT-a banka je dužna podržati ciljeve za zaštitu, i ako je potrebno, ponovnu uspostavu povjerljivosti, integriteta i dostupnosti poslovnih procesa, podržavajućih procesa i IKT imovine.		
Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(4)		U okviru Plana kontinuiteta IKT-a banka je dužna razmotriti niz različitih scenarija kojima bi mogla biti izložena, uključujući ekstremne, ali moguće scenarije, te procijeniti njihov potencijalni uticaj. Na osnovu tih scenarija banka je dužna opisati način osiguravanja kontinuiteta IKT sistema i usluga, kao i informacionu sigurnost banke.		
Član 30.	Plan kontinuiteta IKT-a i planovi odgovora i oporavka IKT sistema	(5)		Pri procesu planiranja kontinuiteta poslovanja u području IKT-a banka je dužna definisati procese, uloge i odgovornosti, a kako bi osigurala da su eksternalizovani dijelovi IKT sistema i servisi adekvatno pokriveni planovima kontinuiteta poslovanja. Banka je dužna uzeti u obzir zavisnost o uslugama trećih strana.		
Član 31.	Planovi odgovora i oporavka IKT sistema	(1)		Na osnovu analize uticaja na poslovanje iz člana 29. ove odluke i plana kontinuiteta IKT-a, iz člana 30. ove odluke, banka je dužna da definiše i usvoji planove odgovora i oporavka IKT sistema.		
Član 31.	Planovi odgovora i oporavka IKT sistema	(2)		Planovima odgovora i oporavka IKT sistema je potrebno definisati uslove za aktiviranje planova, kao i mjere koje je potrebno poduzeti kako bi se osigurala dostupnost, kontinuitet i oporavak minimalno prioritetnih (važnih) funkcija odnosno ključnih (važnih) IKT sistema i usluga. Planovi za oporavak IKT sistema trebaju biti usmjereni prema postizanju ciljeva oporavka poslovanja banke.		
Član 31.	Planovi odgovora i oporavka IKT sistema	(3)		Banka je dužna da u slučaju nastanka okolnosti koje zahtijevaju primjenu plana odgovora i oporavka IKT sistema odmah po saznanju o navedenom obavijesti Agenciju sa svim relevantnim činjenicama i okolnostima koje se na to odnose.		
Član 31.	Planovi odgovora i oporavka IKT sistema	(4)		Banka je dužna ažurirati planove kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema barem jedanput godišnje, a na osnovu rezultata testiranja, saznanja o aktuelnim prijetnjama, kao i iskustvima stečenim iz prethodnih događaja, kao i nalaza/preporuka revizija, te obavezno prilikom promjene ciljeva oporavka, poslovnih funkcija, podržavajućih procesa ili IKT imovine.		
Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(1)		Banka je dužna testirati planove kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema:		

UPRAVLJANJE KONTINUITETOM POSLOVANJA	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(1)	a)	kojima se podržavaju sve funkcije, najmanje jednom godišnje i	**Komentar:** **1. DA li se stavom (1) tacka a) smatra da Banka u slučaju scenarija nedostupnosti primarnog data centra, na rezervnom centru mora imati sve funkcije (kritične, važne i ostale)?** **Plan kontinuiteta IKT-a bi trebao da sadrži više aktivnosti/scenarija/odgovora. Na koji način vršiti testiranje (u cijelosti ili prema definisanim/izabranim scenarijima)?** 2. Da li je stav (3) vezan za članove 20 i 30 koji tretiraju oblast komuniciranja? da li se misli na scenarije nastanka krize? 3. u Članu 32. Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema, stav(1), navedeno je da je Banka dužna testirati planove kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema: a) kojima se podržavaju sve funkcije, najmanje jednom godišnje. U članu 33. (i drugim članovima) Rezervni informatički centar, navedeno je da je Banka je dužna osigurati rezervni informatički centar koji osigurava kontinuitet prioritetnih (važnih) funkcija. Pitanje je dakle da li se testiranje planova mora vršiti za sve funkcije ili se misli na kritične, prioritetne funkcije kako je navedeno u više članova Odluke?	Komentar: 1. Ne, stav (1) a) znači da je banka dužna testirati planove kontinuiteta IKT kojima se podržavaju sve funkcije, što nužno ne znači da banka na DR treba imati podršku za nastavak poslovanja funkcija koje nisu vitalne. Planovi kontinuiteta IKT se mogu odnositi i na nastavak poslovanja na primarnoj lokaciji. Testiranje plana kontinuiteta bi se trebalo izvoditi po scenarijima, vodeći računa o tome da se svake godine uraditi jedan ili više testova, a svi scenariji testiraju u periodu 3 godine (npr), odnosno obavezno po načinjenim značajnim izmjenama u okviru IKT sistema ili poslovnih procesa koji imaju uticaja na njih, u slučaju fluktuacije osoblja i drugih značajnijih izmjena. 2. Da. 3. odgovor je dat u prethodnim pitanjima
	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(1)	b)	u slučaju svih bitnih promjena u IKT sistemima koji podržavaju prioritetne (važne) funkcije.		
	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(2)		Banka je dužna testirati i odgovarajuće planove kontinuiteta IKT-a, u slučaju da su prioritetne (važne) funkcije eksternalizovane ili ugovorene sa trećim stranama pružaocima IKT usluga.		
	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(3)		Banka je dužna testirati planove komunikacije u krizi.		
	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(4)		U okviru testiranja iz stava (1) banka je dužna obavezno uključiti scenarije cyber napada i prebacivanja sa primarne IKT infrastrukture na redundantne kapacitete, sigurnosne kopije i rezervni informatički centar.		
	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(5)		Banka je dužna:		
	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(5)	a)	dokumentovati rezultate testiranja, sa svim popratnim detaljima i dokazima o testiranju,		
	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(5)	b)	analizirati i otkloniti sve utvrđene nedostatke koji proizlaze iz testiranja, te o njima izvijestiti upravljačke organe banke i		
	Član 32.	Testiranje plana kontinuiteta IKT-a, planova odgovora i oporavka IKT sistema	(5)	c)	preispitati planove kontinuiteta IKT-a i planove odgovora i oporavka IKT sistema, uzimajući u obzir rezultate testova iz stava (1), kao i preporuke iz revizijskih ili supervizijskih pregleda.		

Član 33.	Rezervni informatički centar	(1)		Banka je dužna osigurati rezervni informatički centar koji:	**Komentar:** 1. da li se u stavu (1) tacka a) tretira i fizička i logička dostupnost? Ako je na logičku, kako odnosna odredba korespondira sa definicijom RPO, RDO i SDO za rezervni informatički centar, čime su predviđeni vremena i razine oporavka? 2. molimo za dodatno pojašnjenje stava (1) tačka d). Ako imate strech mrezu za obezbjedjenje full failover modela da li to znaci da ovaj clan nije zadovoljen? Šta se podrazumijeva pod logički odvojenim informatičkim centrom?	**Komentar:** 1. Stav 1 tačka a) tretira isključivo fizičku odvojenost. 2. tačka d) je prebačena u zahtjev koji se odnosi na sisteme za upravljanja rezervnim kopijama podataka te je prilagođena.
Član 33.	Rezervni informatički centar	(1)	a)	je lociran na odgovarajućoj geografskoj udaljenosti od lokacije primarnog informatičkog centra, uzimajući u obzir rizik da pojedinačni scenario, incident ili katastrofa ne mogu istovremeno uticati na primarni i rezervni informatički centar i sistеme oporavka,		
Član 33.	Rezervni informatički centar	(1)	b)	osigurava kontinuitet prioritetnih (važnih) funkcija na isti način kao i primarni informatički centar ili pruža nivo usluga neophodnih da banka obavlja svoje prioritetne (važne) funkcije u okviru definisanih ciljeva oporavka (RTO, RPO i		
Član 33.	Rezervni informatički centar	(1)	c)	je odmah dostupan zaposlenicima banke kako bi se osigurao kontinuitet prioritetnih (važnih) funkcija u slučaju nedostupnosti primarnog informatičkog centra i		
Član 33.	Rezervni informatički centar	(1)	d)	je logički odvojen od primarnog informatičkog centra, zaštićen od neovlaštenog pristupa ili oštećenja u području IKT sistema.		
Član 33.	Rezervni informatički centar	(2)		Efektivna funkcionalnost rezervnog informatičkog centra treba biti potvrđena najmanje jednom godišnje, kao i poslije implementiranih značajnih promjena u IKT sistemu banke. Banka je dužna, 30 dana prije planiranog testiranja funkcionalnosti rezervnog informatičkog centra, obavijestiti Agenciju.		
Član 33.	Rezervni informatički centar	(3)		Rezultate testiranja iz stava (2) ovoga člana potrebno je detaljno dokumentovati i osigurati da je izvještaj o rezultatima testiranja usvojen od strane uprave banke.		
Član 34.	Eksternalizacija IKT sistema izvan države	(1)		U slučaju eksternalizacije cjelokupnog ili dijela IKT sistema izvan teritorije Bosne i Hercegovine, banka je dužna:	**Komentar:** 1. na koji način tretirati cloud usluge? 2. koje je razlika u pojmovima lokalni informatički centar i primarni informatički centar? 3. Da li Banka ima ingerenciju samostalno analizirati i definisati vrstu podataka koje je potrebno osigurati u lokalnom informatičkom centru odnosno zemlji, bez obzira na kritičnost servisa kojem podaci pripadaju? 4. Da li je neophodno da Banka za slučaj eksternalizacije u Cloudu, za koje je osiguran adekvatan biznis continuity samom uslugom (npr. AWS ili Googlew Cloud), mora osiguravati i lokalne kopije podataka?	**Komentar:** 1. Cloud usluge je potrebno tretirati na isti način kao i sve ostale eksternalizovane usluge. Ukoliko usluge koje su eksternalizovane u cloud su potrebne za pružanje/podršku prioritetnim funkcijama, potrebno ih je osigurati na teritoriji BiH na način npr korištenjem hibridnog rješenja ili slično, vodeći računa o adekvatnoj kvaliteti obavljanja poslovnog procesa u navedenom slučaju. 2. primarni informatički centar je centar gdje je smješteno produkciono okruženje banke, te u slučaju da je navedeno izvan BiH, banka je dužna imati lokalni informatički centar. Kod banaka kod kojih je produkciono okruženje unutar BiH primarni i lokalni centar bi trebali predstavljati istu lokaciju. 3. Banka je dužna osigurati sve podatke neophodne za nesmetano odvijanje svih poslovnih procesa definisanih ovih članom. 4.Da, u slučaju da su potrebni navedeni podaci u skladu sa tačkom h).
Član 34.	Eksternalizacija IKT sistema izvan države	(1)	a)	definisati prioritetne (važne) funkcije banke sa stanovišta kontinuiteta poslovanja i odvijanja istih u zemlji, uzimajući u obzir analizu uticaja na poslovanje, kao i važeće zakonske propise,		
Član 34.	Eksternalizacija IKT sistema izvan države	(1)	b)	definisati odgovarajuće RTO, RPO i SDO parametre za funkcije definisane tačkom a) ovog stava, osiguravajući adekvatne nivoe usluge,		
Član 34.	Eksternalizacija IKT sistema izvan države	(1)	c)	definisati ključne resurse IKT sistema banke koji podržavaju prioritetne (važne) definisane poslovne procese iz tačke a) ovog stava, uzimajući pri tome u obzir i podržavajuće resurse, te napredak i primjenu IKT u poslovnim procesima banke,		
Član 34.	Eksternalizacija IKT sistema izvan države	(1)	d)	definisati plan kontinuiteta IKT-a i planove oporavka IKT sistema u zemlji,		
Član 34.	Eksternalizacija IKT sistema izvan države	(1)	e)	osigurati lokalni informatički centar na teritoriji Bosne i Hercegovine kako bi osigurala kontinuitet prioritetnih (važnih) funkcija u zemlji na isti način kao i u okviru primarnog informatičkog centra odnosno pružanje nivoa usluga neophodnih da banka obavlja svoje prioritetne (važne) funkcije u okviru definisanih ciljeva oporavka (RTO, RPO i SDO),		
Član 34.	Eksternalizacija IKT sistema izvan države	(1)	f)	provoditi testiranje funkcionalnosti lokalnog informatičkog centra najmanje na godišnjem nivou, te osigurati da je izvještaj o rezultatima testiranja usvojen od strane uprave banke,		
Član 34.	Eksternalizacija IKT sistema izvan države	(1)	g)	osigurati osposobljenost zaposlenika banke za izvođenje navedenih aktivnosti,		

Član 34.	Eksternalizacija IKT sistema izvan države	(1)	h)	analizirati i definisati vrstu podataka koje je potrebno osigurati u lokalnom informatičkom centru odnosno zemlji, kako bi se zadovoljile poslovne potrebe banke, uzimajući u obzir tačku a) i e) ovog stava, kao i važeći zakonski propisi i		
Član 34.	Eksternalizacija IKT sistema izvan države	(1)	i)	osigurati ažurnost podataka definisanih tačkom h) u lokalnom informatičkom centru na dnevnoj osnovi.		
Član 34.	Eksternalizacija IKT sistema izvan države	(2)		Banka je dužna, 30 dana prije planiranog testiranja funkcionalnosti lokalnog informatičkog centra, obavijestiti Agenciju.		
Član 35.	Sigurnosne kopije podataka i sistema	(1)		Banka je dužna uspostaviti proces upravljanja sigurnosnim kopijama (eng. backup) koji uključuje procedure izrade, smještaja, testiranja kopija podataka i sistema, te ponovne uspostave i oporavka, kao i adekvatan transport i predaju kopija, a kako bi se osigurala raspoloživost podataka i sistema u slučaju potrebe, te omogućio adekvatan oporavak odnosno ponovna uspostava prioritetnih (važnih) procesa u zahtijevanom vremenu i raspoloživosti.		
Član 35.	Sigurnosne kopije podataka i sistema	(2)		U okviru procesa upravljanja sigurnosnim kopijama, banka je dužna propisati za sve resurse IKT sistema:		
Član 35.	Sigurnosne kopije podataka i sistema	(2)	a)	vrstu,		
Član 35.	Sigurnosne kopije podataka i sistema	(2)	b)	način izrade,		
Član 35.	Sigurnosne kopije podataka i sistema	(2)	c)	obim,		
Član 35.	Sigurnosne kopije podataka i sistema	(2)	d)	frekvenciju izrade,		
Član 35.	Sigurnosne kopije podataka i sistema	(2)	e)	frekvenciju odlaganja na udaljenu lokaciju,		
Član 35.	Sigurnosne kopije podataka i sistema	(2)	f)	te period čuvanja sigurnosnih kopija.		
Član 35.	Sigurnosne kopije podataka i sistema	(2)		Obim i frekvenciju izrade sigurnosnih kopija, banka je dužna definisati u skladu sa zahtjevima analize uticaja na poslovanje i planovima za odgovor i oporavak IKT sistema, te procjenjivati u skladu s provedenom procjenom IKT rizika.		
Član 35.	Sigurnosne kopije podataka i sistema	(3)		Banka je dužna sigurnosne kopije osigurati na jednoj ili više sekundarnih lokacija, od kojih najmanje jedna mora biti dovoljno udaljena od primarne lokacije, na kojoj se nalaze izvorni podaci, na način da nisu izložene istim rizicima. Sigurnosne kopije trebaju biti ažurne i adekvatno zaštićene od odgovarajućih rizika (cyber napadi, rizici prilikom prijenosa i drugo).		
Član 36.	Zaštitne (regulatorne) kopije podataka			Banka je dužna osigurati zaštitne (regulatorne) kopije podataka:	**Komentar:** 1. Koji set podataka treba biti osiguran za sprovedbu kontrola od strane agencije u slučaju rane intervencije odnosno za restrukturu? 2. Koje podatke treba obezbijediti, ko im smije pristupiit, koliko ažurni ti podaci moraju bit, koja je frekvencija obezbjeđivanja?	
Član 36.	Zaštitne (regulatorne) kopije podataka		a)	koje sadrže minimalni set podataka neophodan za nastavak poslovanja banke i pružanje prioritetnih (važnih) funkcija i usluga, kao i sprovedbu kontrola od strane Agencije u slučaju rane intervencije ili restrukture,		**Komentar:** 1. Podaci koji se odnose na izvještajne podatke i podatke koji su neophodni za nesmetan i brz postupak provođenja restrukture sukladno propisima koji regulišu tu oblast. Ukoliko se ukaže

	Član 36.	Zaštitne (regulatorne) kopije podataka		b)	u lako dostupnom formatu kojem je moguće pristupiti/pročitati koristeći standardne, uobičajene, sveprisutne dostupne alate, neovisno od izvornih sistema u kojima su podaci nastali,	podaci moraju biti, koja je frekvencija obezbjeđivanja? 3. Koji je to potrebni format? i u kojoj formi treba biti dostupan na centralnoj lokaciji Banke? Molimo za dodatno pojašnjenje definicije formata koji se koristi za dostavljanje back-up-a, tj precizirano tumačenje 'lako dostupnog formata kojem je moguće pristupiti koristeći standardne/uobičajene alate.' Važno je napomenuti da alati koji se koriste za kreiranje rezervnih kopija (back-up) imaju vlastite enkripcije.	potreba, navedeno će biti pobliže definisano pratećim aktom za provođenje ove odluke. 2. Ažurnost i frekvencija će biti definisani dalje Uputstvom. 3. Navedeno će biti detaljnije definisano Uputstvom.
	Član 36.	Zaštitne (regulatorne) kopije podataka		c)	ažurne u skladu sa zahtjevima Agencije i		
	Član 36.	Zaštitne (regulatorne) kopije podataka		d)	dostupne na centralnoj lokaciji banke.		
UPRAVLJANJE IKT OPER	Član 37.	IKT operacije	(1)		Banka je dužna upravljati svojim IKT operacijama na osnovu dokumentovanih, usvojenih i implementiranih procesa i procedura. Tim dokumentima potrebno je definisati kako banka upotrebljava, prati i kontroliše svoje IKT sisteme i usluge. Navedene procedure trebaju biti potpune, ažurne i međusobno usklađene.		
	Član 37.	IKT operacije	(2)		Banka je dužna osigurati da je izvršavanje IKT operacija usklađeno sa zahtjevima poslovanja banke, uključujući i zahtjevima informacione sigurnosti.		
	Član 37.	IKT operacije	(3)		Banka je dužna održavati i unapređivati efikasnost svojih IKT operacija, naročito svođenja pogrešaka koje proizlaze iz izvršavanja ručnih zadataka na najmanju moguću mjeru.		
	Član 37.	IKT operacije	(4)		Banka je dužna evidentirati, pratiti i čuvati zapise za kritične IKT operacije kako bi se omogućilo otkrivanje, analiza i ispravljanje pogrešaka.		
	Član 37.	IKT operacije	(5)		Banka je dužna:		
	Član 37.	IKT operacije	(5)	a)	definisati i provoditi procedure upravljanja IKT imovinom, tokom cijelog njenog životnog ciklusa, od nabavke ili razvoja do povlačenja iz upotrebe, u cilju osiguranja dostupnosti, autentičnosti, integriteta i povjerljivosti podataka i		
	Član 37.	IKT operacije	(5)	b)	provoditi postupke planiranja te praćenja performansi i kapaciteta kako bi pravovremeno spriječila, otkrila i odgovorila na značajne probleme u radu IKT sistema i nedostatke kapaciteta IKT sistema.		
	Član 38.	Upravljanje projektima	(1)		Banka je dužna uspostaviti proces upravljanja projektima kojim su definisane uloge i odgovornosti potrebne za efikasnu podršku provođenju strategije IKT sistema.	**Komentar:** 1. Koje podatke treba obezbijediti, ko im smije pristupiit, koliko ažurni ti podaci moraju bit, koja je frekvencija obezbjeđivanja? 2. Da li će u okviru uputstava biti neke posebne smjernice za minimalne set dokumentacije neophodne u okviru upravljanja projektima, posebno kada je u pitanju agile pristup? 3. U kojoj mjeri se očekuje uključenost funkcije upravljanja sigurnošću kod upravljanja projektima pogotovo kada je u pitanju agile pristup. Da li se očekuju formalno propisani sigurnosni zahtjevi bez obzira na metodologiju upravljanja?	**Komentar:** 1. Pitanje se vjerovatno odnosi na prethodni član, te je gore i dat odgovor. 2. Minimalni set dokumentacije neće biti propisan uputstvima.Uputstvo će dalje definisati sadržaj politike upravljanja projektima. Agile pristup također podrazumijeva izradu relevatne pisane dokumentacije. Banka treba osigurati adekvatnu i potpunu dokumentaciju u okviru projekta kako bi dokazala da na adekvatan način upravljanja projektom, njegovim rizicima, kao i vezanim rizicima uz informacioni sistem, te da prati definisanu projektnu metodologiju. 3. Funkcija upravljanja IKT rizicima - druga linija treba dati svoje mišljenje o procjeni sigurnosti novih proizvoda/izmjena na informacionom sistemu te preporuke za sigurnosne kontrole. Navedeno je potrebno dati na početku projekta, kao i pregledati na kraju projekta, odnosno nakon eventualnih izmjena u toku projekta, te je zahtjeve sigurnosti potrebno osigurati u pisanoj formi.
	Član 38.	Upravljanje projektima	(2)		Banka je dužna na odgovarajući način pratiti i smanjivati rizike koji proizlaze iz IKT projekata, a uzimajući u obzir i rizike koji mogu proizaći iz međusobne zavisnosti različitih projekata i zavisnosti višestrukih projekata o istim resursima i/ili stručnostima. Banka je dužna uključiti projektni rizik u okvir upravljanja IKT rizicima.		
	Član 38.	Upravljanje projektima	(3)		Banka je dužna propisati i usvojiti metodologiju upravljanja projektima.		
	Član 38.	Upravljanje projektima	(4)		Metodologijom upravljanja projektima, banka je dužna osigurati da zahtjeve informacione sigurnosti analizira i odobrava funkcija upravljanja sigurnošću IKT sistema.		
	Član 38.	Upravljanje projektima	(5)		U zavisnosti od važnosti i veličine IKT projekta, te uticaju na prioritetne (važne) funkcije, banka je dužna redovno, kao i dodatno po potrebi, izvještavati upravu banke o uspostavi i napretku IKT projekta, te povezanim rizicima.		
	Član 39.	Nabava i razvoj IKT sistema	(1)		Banka je dužna definisati i provoditi procedure kojima se propisuje način nabave, razvoja i održavanja IKT sistema.		
	Član 39.	Nabava i razvoj IKT sistema	(2)		Banka je dužna osigurati da se prije svake kupovine ili razvoja IKT sistema jasno i na odgovarajućem nivou upravljanja definišu i odobre funkcionalni i nefunkcionalni zahtjevi, uključujući zahtjeve u pogledu informacione sigurnosti.		

ACIJAMA	Član 39.	Nabava i razvoj IKT sistema	(3)		Banka je dužna uspostaviti kontrole za ovladavanje rizikom od nenamjernih promjena ili namjerne manipulacije IKT sistemom tokom razvoja i uvođenja u produkcijsko okruženje.	**Komentar:** 1. Potrebno je definisati koji je to zadovoljavajući nivo upravljanja i šta znači odobrenje, da li je prihvatljivo u formi zapisnika odgovarajućih odbora ili se očekuje formalna, potpisna odluka nekog tijela? Na koji način se očekuje ispunjenje ovih preduslova u agilnim i CI/CD pristupima razvoju, gdje funkcionalnosti često nisu poznate unaprijed. Da li je prihvatljivo dokumentovanje kroz alate u vidu epic-a, user story-ja bez formalnih odobrenja pojedinačnih funkcionalnosti?	**Komentar:** 1. Odobrenje funkcionalnih i nefunkcionalnih zahtjeva u okviru projekta je dio upravljanja razvojem sistema i treba biti odobreno od strane organa upravljanja, u okviru preglednog, jasnog, potpunog pisanog dokumenta. Funkcionalnosti sistema u velikoj mjeri trebaju biti poznate unaprijed, sa svojim ciljevima razvoja pojedinog modula/funkcionalnosti, te je potrebno definisati parametre kojima se mjeri napredak razvoja. Dokumentovanje kroz epic-e može biti prihvatljivo, pod uslovom da ispunjava ključne zahtjeve vezane za trag (audit trail), odgovornosti i kontrolu kvalitete. Potrebno je da postoji jasan, detaljan zapis: svaka promjena ima istoriju i odgovorno lice (accountability), postoji dokumentacija ishoda (outputa) i sve to se može na jasan i detaljan način prezentirati.
	Član 39.	Nabava i razvoj IKT sistema	(4)		Banka je dužna:		
	Član 39.	Nabava i razvoj IKT sistema	(4)	a)	osigurati odvojena IKT okruženja kako bi osigurala adekvatnu segregaciju dužnosti i ublažila efekat neprovjerenih promjena u produkcionim okruženjima,		
	Član 39.	Nabava i razvoj IKT sistema	(4)	b)	odvojiti produkciona okruženja od razvojnih, testnih i drugih neprodukcionih okruženja,		
	Član 39.	Nabava i razvoj IKT sistema	(4)	c)	zaštititi integritet i povjerljivost produkcijskih podataka u neprodukcionim okruženjima, te pristup produkcijskim podacima ograničiti na ovlaštene korisnike i		
	Član 39.	Nabava i razvoj IKT sistema	(4)	d)	zaštititi integritet izvornog koda interno razvijenih IKT sistema.		
	Član 39.	Nabava i razvoj IKT sistema	(5)		Banka je dužna detaljno dokumentovati razvoj, implementaciju, rad i konfiguraciju IKT sistema.		
	Član 39.	Nabava i razvoj IKT sistema	(6)		U skladu s procjenom rizika, banka je dužna primjenjivati postupke nabave i razvoja IKT sistema i na IKT sisteme koje razvijaju ili kojima upravljaju krajnji korisnici poslovne funkcije izvan IKT organizacije. Banka je dužna voditi registar ovakvih sistema.		
	Član 40.	Upravljanje IKT promjenama	(1)		Banka je dužna definisati i provoditi procedure upravljanja IKT promjenama kako bi se izbjeglo da promjene dovedu do neočekivanog i neželjenog ponašanja IKT sistema, odnosno naruše njegovu sigurnost ili funkcionalnost.		
	Član 40.	Upravljanje IKT promjenama	(2)		Procedurama iz stava (1) ovog člana, banka treba osigurati da se sve promjene IKT sistema evidentiraju, testiraju, procjenjuju, odobravaju, provode i provjeravaju na kontrolisan način.		
	Član 40.	Upravljanje IKT promjenama	(3)		Procedurama upravljanja IKT promjenama, banka je dužna obuhvatiti i sljedeće:		
	Član 40.	Upravljanje IKT promjenama	(3)	a)	tzv. hitne promjene		
	Član 40.	Upravljanje IKT promjenama	(3)	b)	povratak na staro stanje (prije promjene) i		
	Član 40.	Upravljanje IKT promjenama	(3)	c)	upravljanje sigurnosnim i funkcionalnim ispravkama (eng. patch).		
	Član 40.	Upravljanje IKT promjenama	(4)		Banka je dužna da utvrdi početne verzije software-skih komponenata IKT sistema, te evidentira i dokumentuje sve promjene komponenata IKT sistema onim slijedom kako su nastajale, zajedno sa vremenom nastanka promjene.		
	Član 41.	Upravljanje IKT incidentima i problemima	(1)		Banka je dužna da definiše, uspostavi i provodi proces upravljanja IKT incidentima radi pravovremenog otkrivanja IKT incidenata, upravljanja njima i obavještavanja o istim.	**Komentar:**	
	Član 41.	Upravljanje IKT incidentima i problemima	(2)		U procesu upravljanja IKT incidentima, Banka je dužna da definiše i uspostavi Politiku upravljanja IKT incidentima i procedure upravljanja IKT incidentima koji obuhvataju:		
	Član 41.	Upravljanje IKT incidentima i problemima	(2)	a)	pokazatelje za rano upozoravanje,		
	Član 41.	Upravljanje IKT incidentima i problemima	(2)	b)	evidenciju svih IKT incidenata i ozbiljnih cyber prijetnji,		
	Član 41.	Upravljanje IKT incidentima i problemima	(2)	c)	postupke za utvrđivanje i dosljedno i integrisano (centralizirano) praćenje i evidentiranje svih IKT incidenata i ozbiljnih cyber prijetnji,		

Član 41.	Upravljanje IKT incidentima i problemima	(2)	d)	kategorizaciju i klasifikaciju IKT incidenata u skladu s njihovim prioritetom i ozbiljnosti te kritičnosti zahvaćenih usluga, a uzimajući u obzir kriterije utvrđene članom 42. ove odluke,	1. da li će u okviru uputstva biti predviđena metrika za određivanje "značajnosti" incidenta? 2. molimo pojašnjenje "ozbiljnih" cyber prijetnji. Da li će uputstvima biti bliže definisan pojam "ozbiljne" prijetnje? 3. da li ovo znači da je banka u obavezi da uspostavi proces upravljanja dokazima i razvije kapacitete za digitalnu forenziku? 4. molimo detaljnije definisanje očekivanja sadržaja politike i sadržaja procedure uzimajući u obzir postojeće interne akte koji su definisani u bankama (veza član 41. stav (2)) 5. Dodatno pojašnjenje ili definisanje primjera 'pokazatelja za rano upozoravanje" veza stav (2) tačka a). 6. Molimo za dodatno pojašnjenje načina čuvanja dokaza u okviru stava (4), te pojašnjenje samog procesa pripreme podataka za forenziku. Također, da li već postoji referentni dokument za ovaj predmet u nekoj od nadležnih institucija na nivou države? 7. Nije jasno na šta se misli pod ozbiljnom cyber prijetnjom. Da li se radi o prijetnji koja potencijalno može biti incident i ako je to slučaj, kako voditi evidenciju takvih prijetnji? Da li se radi o objavama u sredstvima informisanja i društvenim mrežama i dr. na osnovu kojih je potrebno donijeti zaključak da takva prijetnja može potecijalno uticati na Banku i njene klijente? Ili se radi o prijetnjama koje će se razmjenjivati preko FBA platforme. Koja su očekivanja vezano za dalje postupke po pitanju cyber prijetnji, osim evidencije?	**<u>Komentar:</u>** 1. Da, u okviru smjernica će biti definisani kriteriji za procjenu značajnosti incidentata. 2. Da, u okviru uputstava će biti kriteriji za procjenu ozbiljnosti cyber prijetnji. 3. Da, banka treba uspostaviti proces upravljanja dokazima. Za potrebe digitalne forenzike banka može angažovati i vanjske saradnike, uz odgovarajuće adekvatne uslove, u slučaju potrebe za provođenjem aktivnosti forenzike. 4. U okviru navedenog člana su date glavne aktivnosti koje trebaju biti predmetom politika i procedura. 5. 'Pokazateljima za rano upozoravanje" u vezi stav (2) tačka a) se smatraju razne aktivnosti/notifikacije koje mogu ukazati na neželjene promjene u informacionom sistemu u njihovoj ranoj fazi, npr usporenje sistema, povećan izlazni saobraćaj i slično. 6. Banka se treba voditi najboljim praksama u toj oblasti. Forenzika u ovom smislu predstavlja skupljanje, očuvanje, validaciju, identifikaciju, analizu , interpretaciju, dokumentaciju i prezentaciju digitalnih dokaza proizašlih iz digatalnih izvora s ciljem provođenja ili pomoći pri rekonstrukciji događaja; dakle, banka treba definisati i primijeniti najbolje prakse iz ove oblasti, u onom obimu u kojem će biti primjenjivane u banci. 7. Kriteriji za klasifikaciju incidenata i cyber prijetnji će biti date dalje uputstvima. Sve gore navedeno se ubraja u cyber prijetnje. U slučaju evidentirane značajne cyber prijetnje, banka treba izvršiti pisanu procjenu uticaja cyber prijetnje na informacioni sistem banke i eventualne poduzete aktivnosti.
Član 41.	Upravljanje IKT incidentima i problemima	(2)	e)	postupke odgovora na IKT incidente, uključujući utvrđivanje i dokumentovanje njihovih osnovnih uzroka i daljnje postupanje i poduzimanje mjera, u cilju ublažavanja njihovog efekta i osiguravanja pravovremene dostupnosti i sigurnosti poslovnih funkcija banke,		
Član 41.	Upravljanje IKT incidentima i problemima	(2)	f)	postupke upravljanja problemima, što uključuje utvrđivanje, analizu i rješavanje glavnih uzroka jednog ili više incidenata, kako bi se spriječilo ponavljanje incidenta, te u skladu sa stečenim znanjima ažuriranje sigurnosnih mjera IKT sistema,		
Član 41.	Upravljanje IKT incidentima i problemima	(2)	g)	uloge i odgovornosti za različite vrste IKT incidenata (npr. pogreške, neispravni rad, cyber napadi i sl.),		
Član 41.	Upravljanje IKT incidentima i problemima	(2)	h)	planove za komunikaciju sa uposlenicima, eksternim učesnicima i medijima, a u skladu sa članom 20. ove odluke, planove za obavještavanje klijenata, postupke povezane sa internom eskalacijom, a što uključuje prigovore korisnika povezane s IKT sistemom i prema potrebi informisanje partnerskih finansijskih institucija,		
Član 41.	Upravljanje IKT incidentima i problemima	(2)	i)	izvještavanje organa banke najmanje o značajnim IKT incidentima, uz objašnjenje njihovog uticaja, odgovora na njih i dodatnih kontrola koje je potrebno uvesti.		
Član 41.	Upravljanje IKT incidentima i problemima	(3)		Banka je dužna evidentirati sve IKT incidente i ozbiljne cyber prijetnje.		
Član 41.	Upravljanje IKT incidentima i problemima	(4)		U okviru postupaka odgovora na incidente iz stava (2) tačka e) ovog člana, Banka je dužna implementirati postupke za adekvatno upravljanje potencijalnim dokazima, kad god je to moguće, vodeći računa o sljedećem:		
Član 41.	Upravljanje IKT incidentima i problemima	(4)	a)	održavanje lanca čuvanja svih povezanih dokaza (eng. chain of custody),		
Član 41.	Upravljanje IKT incidentima i problemima	(4)	b)	prilikom pokretanja digitalne forenzičke istrage, razmotriti moguće posljedice sa pravne tačke gledišta,		
Član 41.	Upravljanje IKT incidentima i problemima	(4)	c)	osigurati da nisu zanemareni kritični aspekti zadržavanja dokaza i		
Član 41.	Upravljanje IKT incidentima i problemima	(4)	d)	osigurati da su prikupljeni dokazi prihvatljivi na nadležnom sudu.		
Član 42.	Klasifikacija incidenata	(1)		Banka je dužna da klasifikuje IKT incidente i utvrdi njihov uticaj na osnovu sljedećih kriterija:		
Član 42.	Klasifikacija incidenata	(1)	a)	broj i/ili relevantnost zahvaćenih klijenata ili finansijskih partnera, gdje je to primjenjivo, iznos ili broj transakcija na koje je uticao IKT incident, kao i činjenice da li je IKT incident imao uticaj na ugled banke,		
Član 42.	Klasifikacija incidenata	(1)	b)	trajanje IKT incidenta, uključujući vrijeme zastoja u pružanju usluge,		
Član 42.	Klasifikacija incidenata	(1)	c)	geografska rasprostranjenost u smislu područja pogođenih IKT incidentom,		
Član 42.	Klasifikacija incidenata	(1)	d)	gubitak podataka prouzročen IKT incidentom, u smislu dostupnosti, autentičnosti, integriteta ili povjerljivosti podataka,		

UPRAVLJANJE IKT INCIDENTIMA	Član 42.	Klasifikacija incidenata	(1)	e)	kritičnost pogođenih usluga, uključujući transakcije i operacije banke i		
	Član 42.	Klasifikacija incidenata	(1)	f)	ekonomski uticaj IKT incidenta, posebno direktni i indirektni troškovi i gubici, u apsolutnom i relativnom smislu.		
	Član 42.	Klasifikacija incidenata	(2)		Banka je dužna da klasifikuje cyber prijetnju kao značajnu na osnovu kritičnosti usluge koja je izložena riziku, uključujući transakcije i operacije banke, broj i/ili relevantnost zahvaćenih klijenata ili finansijskih partnera, kao i geografsku rasprostranjenost područja izloženog riziku.		
	Član 43.	Učenje i razvoj	(1)		Banka je dužna uspostaviti procedure analiza i pregleda nakon značajnih IKT incidenata i cyber prijetnji, analizirajući uzroke poremećaja i identificirajući potrebna poboljšanja u IKT procesima ili u okviru plana kontinuiteta IKT-a definisanog članom 28. ove odluke.		
	Član 43.	Učenje i razvoj	(2)		Pregledom iz stava (1) ovog člana, banka je dužna utvrditi da li su poštovani uspostavljeni procesi i da li su preduzete kontrole bile efikasne, uključujući procjene sljedećeg:		
	Član 43.	Učenje i razvoj	(2)	a)	brzinu u odgovoru na sigurnosna upozorenja i utvrđivanje uticaja IKT incidenta i njegove ozbiljnosti,		
	Član 43.	Učenje i razvoj	(2)	b)	kvalitet i brzinu izvođenja forenzičke analize, gdje je to primjenjivo,		
	Član 43.	Učenje i razvoj	(2)	c)	efikasnost eskalacije incidenta unutar banke i		
	Član 43.	Učenje i razvoj	(2)	d)	efikasnost interne i eksterne komunikacije.		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(1)		Banka je dužna da odmah po saznanju o značajnom IKT incidentu, kako u dijelu IKT sistema koji se nalazi u banci, tako i u dijelu IKT sistema koji je eksternalizovan/povjeren na obavljanje trećim stranama pružaocima IKT usluga, obavijesti Agenciju.		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(2)		Za potrebe stava (1) ovog člana, Banka je dužna, nakon prikupljanja i analize svih relevantnih informacija, dostaviti inicijalno obavještenje i izvještaj, a u skladu sa stavom (3) i (5) ovog člana.		

	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(3)		Inicijalno obavještenje i izvještaj iz stava (2) treba da sadrže sve potrebne informacije kako bi Agencija bila u mogućnosti procijeniti značaj IKT incidenta i njegov uticaj na cjelokupni finansijski sektor.	**Komentar:** 1. vezano za stav (8), molimo za listu relevantnih organa i / ili institucija unutar države kojima bi se, u slučaju detektovanja cyber incidenta, informacija dostavila	-
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(4)		Banka je dužna odmah po saznanju o ozbiljnoj cyber prijetnji obavijestiti Agenciju, ukoliko smatra da je prijetnja relevantna za finansijski sektor, korisnike usluga ili klijente.		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(5)		U slučaju značajnog IKT incidenta koji ima uticaj na finansijske interese klijenata, banka je dužna, bez nepotrebnog odlaganja, čim sazna za taj incident, obavijestiti svoje klijente o značajnom IKT incidentu i poduzetim mjerama za ublažavanje negativnih efekata incidenta. U slučaju značajne cyber prijetnje, banka je dužna, ako je to primjenjivo, pravovremeno obavijestiti svoje klijente koji bi mogli biti zahvaćeni tom cyber prijetnjom, te dostaviti informaciju o svim odgovarajućim zaštitnim mjerama koje bi klijenti mogli razmotriti.		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(6)		Banka je dužna Agenciji dostaviti sljedeće:		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(6)	a)	inicijalno obavještenje,		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(6)	b)	prelazni izvještaj, nakon inicijalnog obavještenja iz tačke a) ovog stava, čim se status izvornog IKT incidenta značajno promijeni ili se postupanje u vezi sa značajnim IKT incidentom promijeni na osnovu novih dostupnih informacija, a nakon toga prema potrebi, ažurirana obavještenja svaki put kad se pojave relevantne novosti o statusu, kao i na poseban zahtjev Agencije i		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(6)	c)	konačni izvještaj, kada je analiza osnovnog uzroka IKT incidenta završena, neovisno o tome da li su mjere za ublažavanje uticaja već provedene i kada se procijenjene vrijednosti uticaja mogu zamijeniti stvarnim podacima o uticaju IKT incidenta.		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(7)		Nakon primanja informacije, Agencija će prema potrebi poduzeti sve potrebne mjere u svrhu zaštite stabilnosti finansijskog sistema.		
	Član 44.	Izvještavanje o IKT incidentu i cyber napadu	(8)		Ovisno o karakteristikama cyber incidenta, banka je dužna razmotriti obavezu obavještavanja ostalih relevantnih organa i institucija unutar države.		
	Član 45.	Uspostavljanje okvira upravljanja rizicima trećih strana	(1)		Neovisno o odredbama Odluke o upravljanju eksternalizacijom u banci („Službene novine FBiH“, 75/22), banka je dužna uspostaviti upravljanje IKT rizicima povezanim sa trećim stranama čije su aktivnosti vezane uz IKT usluge i IKT sisteme, kao sastavnim dijelom IKT rizika u okviru za upravljanje IKT rizicima, iz člana 12. ove odluke.		
	Član 45.	Uspostavljanje okvira upravljanja rizicima trećih strana	(2)		Upravljanje IKT rizicima povezanim sa trećim stranama pružaocima IKT usluga, banka je dužna uspostaviti u skladu sa sljedećim principima:		
	Član 45.	Uspostavljanje okvira upravljanja rizicima trećih strana	(2)	a)	banka koja ima sklopljene ugovore o obavljanju IKT usluga sa trećim stranama za potrebe svog poslovanja u svakom trenutku snosi potpunu odgovornost za poštovanje i izvršavanje svih obaveza iz ove odluke i primjenjivog zakonskog		
	Član 45.	Uspostavljanje okvira upravljanja rizicima trećih strana	(2)	b)	principom proporcionalnosti i uzimajući u obzir: i. prirodu, obim, složenost i važnost ovisnosti u području IKT sistema i ii. rizike koji proizilaze iz ugovora o upotrebi IKT usluga sklopljenih sa trećim stranama pružaocima IKT usluga, vodeći računa o ključnosti ili važnosti predmetne usluge, procesa ili funkcije, te o mogućem uticaju na kontinuitet i dostupnost usluga i aktivnosti na nivou banke i na nivou grupe.	**Komentar:** 1. da li stav (1) podrazumijeva da TPRM treba biti sastavni dio Risk-a ili može biti dio upravljanja sigurnosti ili neke treće organizacione jedinice?	**Komentar:** 1. Upravljanje IKT rizicima povezanim sa trećim stranama treba biti sastavni dio funkcije upravljanja IKT rizicima banke.

Član 45.	Uspostavljanje okvira upravljanja rizicima trećih strana	(3)		Banka je dužna propisati i provoditi Politiku o korištenju IKT usluga trećih strana, a posebno IKT usluga kojima se podržavaju prioritetne (važne) funkcije, te je primjenjivati na pojedinačnoj, i prema potrebi, na konsolidovanoj osnovi.		
Član 45.	Uspostavljanje okvira upravljanja rizicima trećih strana	(4)		Banka je dužna pravovremeno obavijestiti Agenciju o svim planiranim ugovorima o upotrebi IKT usluga kojima se podržavaju prioritetne (važne) funkcije, kao i o tome da je određena funkcija postala prioritetna (važna), poštujući odredbe člana 28., 29. i 30. Odluke o upravljanju eksternalizacijom u banci.		
Član 46.	Registar informacija			Banka je dužna održavati i redovno ažurirati, kako na nivou banke, tako i na i konsolidovanom nivou, registar informacija u vezi sa svim ugovorima o korištenju IKT usluga koje pružaju treće strane pružaoci IKT usluga.		
Član 47.	Procjena rizika	(1)		Prije sklapanja ugovora o pružanju IKT usluga banka je dužna:	**Komentar:** 1. Što se podrazumijeva pod pojmom "Nadzorni uslovi" u pogledu ugovaranja" a što je predviđeno stavom (1) tačka b)?	**Komentar:** 1. Pod pojmom "Nadzorni uslovi" u pogledu ugovaranja" stav (1) tačka b) smatraju se uslovi koji se odnose na mogućnost efikasnog nadzora pružanja usluga kod pružaoca usluga od strane regulatora, banke i od njih ovlaštenih strana, osiguravajući mogućnost nadzora na mjestu obavljanja usluge, pravovremeni pristup podacima i sistemima koji su predmetom nadzora, osiguravanje mogućnosti uzimanja fizičkih kopija dokaza i drugih relevantnih elemenata efikasnog nadzora.
Član 47.	Procjena rizika	(1)	a)	procijeniti da li ugovor obuhvata upotrebu IKT usluga kojima se podržava prioritetna ili važna funkcija,		
Član 47.	Procjena rizika	(1)	b)	procijeniti da li su ispunjeni nadzorni uslovi u pogledu ugovaranja,		
Član 47.	Procjena rizika	(1)	c)	utvrditi i procijeniti sve relevantne rizike povezane sa ugovorom, a u skladu sa članom 9. stav (1) Odluke o upravljanju eksternalizacijom, uključujući i rizik da taj ugovor doprinese jačanju koncentracijskog IKT rizika, u skladu sa članom 48.		
Član 47.	Procjena rizika	(1)	d)	provoditi dubinske analize potencijalnih trećih strana pružaoca IKT usluga i osiguravati adekvatnost treće strane pružaoca IKT usluga tokom cijelog procesa odabira i procesa procjene i		
Član 47.	Procjena rizika	(1)	e)	utvrditi i procijeniti sukobe interesa koje bi ugovor mogao izazvati.		
Član 47.	Procjena rizika	(2)		Banka je dužna ugovarati IKT usluge isključivo sa trećim stranama pružaocima IKT usluga koji ispunjavaju odgovarajuće standarde IKT sigurnosti. U slučaju da se ugovor odnosi na aktivnosti koje podržavaju prioritetne (važne) funkcije, banka je dužna, prije sklapanja ugovora, utvrditi da pružalac usluga koristi najsavremenije i najviše standarde IKT sigurnosti.		
Član 47.	Procjena rizika	(3)		Banka je dužna kontinuirano pratiti i tražiti garancije nivoa usklađenosti trećih strana pružaoca IKT usluga sa sigurnosnim ciljevima, mjerama i ciljevima banke.		
Član 47.	Procjena rizika	(4)		Banka je dužna osigurati i primjenjivati pravo pristupa podacima i reviziju treće strane pružaoca IKT usluga u skladu sa članom 25., 26. i 27. Odluke o upravljanju eksternalizacijom u banci.		
Član 48.	Preliminarna procjena koncentracijskog IKT			U slučaju da se ugovor odnosi na aktivnosti koje podržavaju prioritetne (važne) funkcije, banka je dužna prilikom utvrđivanja i procjene rizika iz člana 47. ove odluke, razmotriti i sljedeće:		
Član 48.	Preliminarna procjena koncentracijskog IKT rizika		a)	rizike definisane članom 16. tačka h) Odluke o upravljanju eksternalizacijom u banci, te koristi i troškove alternativnih rješenja, kao što je angažman različitih trećih strana pružaoca IKT usluga, uzimajući u obzir podudaraju li se predviđena rješenja sa poslovnim potrebama i ciljevim utvrđenim u strategiji digitalne otpornost i u kojoj mjeri,		
Član 48.	Preliminarna procjena koncentracijskog IKT rizika		b)	potencijalne koristi i rizike podugovaranja, naročito u slučaju da je podizvođač izvan države Bosne i Hercegovine, ukoliko je ugovorom predviđena mogućnost da treća strana pružalac IKT usluga može podugovoriti IKT usluge kojima se podržavaju prioritetne (važne) funkcije banke nekoj drugoj trećoj strani pružaocu IKT usluga,		

UPRAVLJANJE IKT RIZICIMA POVEZANIM SA TREĆIM STRANAMA	Član 48.	Preliminarna procjena koncentracijskog IKT		c)	odredbe prava o nesolventnosti koje bi se primjenjivale u slučaju stečaja treće strane pružaoca IKT usluga, kao i o svim ograničenjima do kojih bi moglo doći pri hitnom oporavku podataka banke,		
	Član 48.	Preliminarna procjena koncentracijskog IKT		d)	usklađenosti sa Zakonom o zaštiti podataka te o efikasnom izvršavanju zakonodavstva BiH, u slučaju da se treća strana pružalac IKT usluga nalazi izvan države Bosne i Hercegovine,		
	Član 48.	Preliminarna procjena koncentracijskog IKT		e)	uticaj potencijalno dugih ili složenih lanaca podugovaranja na sposobnost banke da u potpunosti prati ugovorene aktivnosti, kao i na sposobnost Agencije za izvođenje efikasnog nadzora nad bankom u tom slučaju.		
	Član 49.	Izlazna strategija i raskid ugovora	(1)		U slučaju da se ugovor odnosi na aktivnosti koje podržavaju prioritetne (važne) funkcije, banka je dužna donijeti izlaznu strategiju i postupke koji su u skladu sa politikom o korištenju IKT usluga i planovima kontinuiteta poslovanja banke, poštujući odredbe člana 23. Odluke o upravljanju eksternalizacijom u banci.		
	Član 49.	Izlazna strategija i raskid ugovora	(2)		Banka je dužna osigurati mogućnost raskida ugovora o upotrebi IKT usluga, u skladu sa članom 21. Odluke o upravljanju eksternalizacijom, uključujući i:		
	Član 49.	Izlazna strategija i raskid ugovora	(2)	a)	praćenjem IKT rizika povezanih s trećom stranom utvrđene su okolnosti za koje se smatra da bi mogle dovesti do promjena u izvršavanju aktivnosti koje se pružaju na osnovu ugovora, a što uključuje bitne promjene koje utiču na ugovor ili		
	Član 49.	Izlazna strategija i raskid ugovora	(2)	b)	uslijed slabosti pružaoca IKT usluga u vezi sa opštim upravljanjem IKT rizikom, a posebno u načinu na koji osigurava dostupnost, autentičnost, povjerljivost, integritet i sljedivost podataka, bilo da se radi o ličnim ili drugim osjetljivim		
	Član 49.	Izlazna strategija i raskid ugovora	(2)	c)	Agencija zbog uslova ugovora ili okolnosti povezanih sa ugovorom ne može (više) efikasno nadzirati banku.		
	Član 50.	Ugovor sa pružaocima IKT usluga	(1)		Banka je dužna prava i obaveze banke i treće strane pružaoca IKT usluga jasno definisati u pisanoj formi. Potpuni ugovor, koji uključuje i sporazume o nivou usluga, je potrebno osigurati u pisanoj formi koja je ugovornim stranama dostupna u papirnom obliku ili u dokumentu u nekom drugom trajnom i pristupačnom formatu koji se može preuzeti.		
	Član 50.	Ugovor sa pružaocima IKT usluga	(2)		Banka je dužna osigurati usklađenost ugovora iz stava (1) ovog člana sa članom 19. stav (3) Odluke o upravljanju eksternalizacijom u banci.		
	Član 50.	Ugovor sa pružaocima IKT usluga	(3)		Ugovori o korištenju IKT usluga, pored uslova iz stava (2) ovog člana, trebaju uključiti i sljedeće:		
	Član 50.	Ugovor sa pružaocima IKT usluga	(3)	a)	lokacije, posebno regije ili zemlje, na kojima će se pružati ugovorene ili podugovorene aktivnosti i IKT usluge, te na kojima će se obrađivati podaci, uključujući lokaciju čuvanja podataka, kao i zahtjev da treća strana pružalac IKT usluga unaprijed obavijesti banku ako namjerava promijeniti takve lokacije,		
	Član 50.	Ugovor sa pružaocima IKT usluga	(3)	b)	odredbe o dostupnosti, autentičnosti, integritetu i povjerljivosti u vezi sa zaštitom podataka, među ostalim i ličnih podataka,		
	Član 50.	Ugovor sa pružaocima IKT usluga	(3)	c)	odredbe o osiguravanju pristupa ličnim i ostalim podacima koje obrađuje banka te o osiguravanju njihova oporavka i vraćanja u lako dostupnom formatu u slučaju nesolventnosti, sanacije ili prestanka poslovanja treće strane pružaoca		
	Član 50.	Ugovor sa pružaocima IKT usluga	(3)	d)	obavezu treće strane pružaoca IKT usluga da pruži pomoć banci bez dodatnih troškova ili uz unaprijed utvrđene troškove u slučaju IKT incidenta koji je povezan s IKT uslugom koju ta treća strana pruža banci,		
	Član 50.	Ugovor sa pružaocima IKT usluga	(3)	e)	uslove za učestvovanje trećih strana pružaoca IKT usluga u programima za podizanje svijesti o sigurnosti u IKT i osposobljavanjima o digitalnoj operativnoj otpornosti koje provodi banke, a u skladu sa članom 21. ove odluke,		

	Član 50.	Ugovor sa pružaocima IKT usluga	(3)	f)	specifikacije životnog ciklusa podataka banke i		
	Član 50.	Ugovor sa pružaocima IKT usluga	(3)	g)	postupke rješavanja operativnih i sigurnosnih incidenata, uključujući postupke eskalacije i izvještavanja.		
	Član 50.	Ugovor sa pružaocima IKT usluga	(4)		Ugovori o korištenju IKT usluga koje podržavaju prioritetne (važne) poslovne funkcije, trebaju biti usaglašeni sa članom 19. stav (4) Odluke o upravljanju eksternalizacijom u banci i stavom (3) ovog člana, te trebaju uključiti i sljedeće:	**Komentar:** 1. Molimo pojašnjenje za stav (d) tačka f) šta se podrazumijeva pod specifikacijom životnog ciklusa podataka banke u kontekstu odredbi Ugovora koji se zaključuje sa sa pružaocima IKT usluga? 2. Molimo za pojašnjenje za stav (3) tačka g) šta se dodatno podrazumjeva pod postupcima rješavanja operatvnih i sigurnosnih incidenata u kontekstu Odluke o eksternalizaciji	**Komentar:** 1. Pod navedenim se smatra definisanje kontrola upravljanja rizicima povezanim uz podatke banke, u svim fazama, počev od kreiranja podataka, obrade, transporta, čuvanja i krajnjeg uništavanja podataka. 2. U okviru Ugovora je potrebno definisati postupke prilikom rješavanja operativnih i sigurnosnih incidenata, uključujući postupke eskalacije i izvještavanja prilikom istih. Dakle, u okviru ugovora banka je dužna definisati postupke za navedeno, uključujući maksimalne vremenske periode izvještavanja o incidentu, način izvještavanja, postupke izvještavanja, vremenski period rješavanja incidenta i slično.
	Član 50.	Ugovor sa pružaocima IKT usluga	(4)	a)	rokove za prethodne obavijesti i obaveze izvještavanja koje treća strana pružalac IKT usluga ima u odnosu na banku, uključujući i odredbe definisane članom 19. stav (3) tačka m) Odluke o upravljanju eksternalizacijom u banci,		
	Član 50.	Ugovor sa pružaocima IKT usluga	(4)	b)	zahtjeve da treća strana pružalac IKT usluga uvede i testira planove za nepredvidive situacije u poslovanju, kao i alate, politike i kontrole za sigurnost IKT sistema, uključujući i cyber sigurnost, kojima se banci osigurava odgovarajući nivo IKT sigurnosti za pružanje usluga, a u skladu sa prihvatljivim nivoom IKT rizika banke i primjenjivih regulatornih odredbi, a uključujući i zahtjeve u pogledu enkripcije podataka, mrežne sigurnosti i postupaka sigurnosnog praćenja,		
	Član 50.	Ugovor sa pružaocima IKT usluga	(4)	c)	obavezu treće strane pružaoca IKT usluga da učestvuje u TLPT-u banke, a u skladu sa članovima 25. – 27. ove odluke, te njegovu punu kooperativnost,		
	Član 50.	Ugovor sa pružaocima IKT usluga	(4)	d)	pravo kontinuiranog praćenja rada treće strane pružaoca IKT usluga, što uključuje sljedeće: i. odredbe definisane članom 19. stav (3) tačka g) Odluke o upravljanju eksternalizacijom u banci, uključujući i pravo na pristup i izradu kopija relevantne dokumentacije na licu mjesta pružaoca usluge, ako je prioritetna za poslovanje treće strane pružaoca IKT usluge, pri čemu drugi ugovorni aranžmani ili politike ne sprječavaju i ne ograničavaju efikasno ostvarivanje tih prava, ii. pravo ugovoranja alternativnih nivoa osiguranja ako su obuhvaćena prava drugih klijenata, iii. obavezu treće strane pružaoca IKT usluga da u potpunosti sarađuje tokom direktnih nadzora i revizija koje provodi Agencija, banka, uključujući i treće strane koje one imenuju i iv. obavezu dostavljanja pojedinosti o obimu, postupcima kojih se treba pridržavati i učestalosti takvih nadzora i revizija,		
	Član 50.	Ugovor sa pružaocima IKT usluga	(4)	e)	izlazne strategije, posebno određivanje obaveznog adekvatnog prelaznog razdoblja: i. tokom kojega će treća strana pružalac IKT usluga nastaviti pružati predmetne aktivnosti ili IKT usluge banci kako bi se smanjio rizik od poremećaja u radu banke ili kako bi se osigurala njena efikasna sanacija i restrukturiranje i ii. u kojem banka može preći na usluge druge treće strane pružaoca IKT usluga ili se prebaciti na interna rješenja, u skladu sa složenošću usluge koja se pruža.		
	Član 50.	Ugovor sa pružaocima IKT usluga	(5)		Tokom pregovora o ugovorima sa pružaocem IKT usluga, banka je dužna razmotriti primjenu standardnih ugovornih klauzula koja su propisana zakonskom regulativom za konkretne usluge, a gdje je primjenjivo.		
	Član 51.	Upravljanje odnosima s korisnicima platnih	(1)		Banka je dužna izraditi plan podizanja svijesti i nivoa razumijevanja korisnika platnih usluga o sigurnosnim rizicima povezanim s platnim uslugama, koji uključuje osiguravanje pomoći i uputstava korisnicima platnih usluga.		

UPRAVLJANJE ODNOSIMA SA KORISNICIMA PLATNIH USLUGA	Član 51.	Upravljanje odnosima s korisnicima platnih usluga	(2)		Pomoć i uputstva koje se nude korisnicima platnih usluga trebali bi se pravovremeno ažurirati s obzirom na nove prijetnje i ranjivosti, a o promjenama bi trebalo pravovremeno obavještavati korisnike platnih usluga.	**Komentar:** 1. U odnosu na stav (6) molimo pojašnjenje, nije jasno o čemu tačno je potrebno informisati klijente platnih usluga. Da li se misli na promjene u sigurnosnim postupcima za prijavu i autentikaciju klijenata na paltne servise?	**Komentar:** 1. Da, u navedenom se, između ostaloga, misli i na promjene u sigurnosnim postupcima za prijavu i autentikaciju klijenata na platne servise, te korištenje istih, te i sve druge vrste izmjena koje mogu uticati na sigurnost korištenja platnih usluga od strane klijenta.
	Član 51.	Upravljanje odnosima s korisnicima platnih usluga	(3)		Ako je to dopušteno u okviru funkcionalnosti proizvoda, banka je dužna dopustiti korisnicima platnih usluga da onemoguće određene platne funkcionalnosti povezane s platnim uslugama koje banka pruža korisniku platnih usluga.		
	Član 51.	Upravljanje odnosima s korisnicima platnih usluga	(4)		Ako je banka pristala na ograničenja potrošnje korisnika za platne transakcije izvršene putem određenog platnog instrumenta, banka je dužna korisniku omogućiti da prilagodi ta ograničenja do iznosa najvišeg dogovorenog ograničenja.		
	Član 51.	Upravljanje odnosima s korisnicima platnih usluga	(5)		Banka je dužna omogućiti da korisnici platnih usluga primaju upozorenja o iniciranju ili neuspjelim pokušajima iniciranja platnih transakcija čime im se omogućava da otkriju prevarno ili zlonamjerno korištenje njihovih računa.		
	Član 51.	Upravljanje odnosima s korisnicima platnih usluga	(6)		Banka je dužna informisati korisnike platnih usluga o ažuriranjima u pogledu sigurnosnih postupaka koja utiču na korisnike platnih usluga s obzirom na pružanje platnih usluga.		
	Član 51.	Upravljanje odnosima s korisnicima platnih usluga	(7)		Banka je dužna korisnicima platnih usluga pružiti pomoć s obzirom na sva pitanja, zahtjeve za podršku i obavijesti o nepravilnostima ili problemima u pogledu sigurnosnih pitanja povezanih s platnim uslugama. Korisnici platnih usluga trebali bi biti primjereno informisani o tome kako je moguće dobiti navedenu pomoć.		
RAZMJENA INFORMACIJA	Član 52.	Razmjena informacija	(1)		Banka je dužna sa Agencijom razmjenjivati informacije i obavještajne podatke o cyber prijetnjama, uključujući indikatore kompromitovanja, taktike, tehnike i procedure, upozorenja o cyber sigurnosti i alate za konfiguraciju, u mjeri u kojoj takve informacije i razmjena podataka:		
	Član 52.	Razmjena informacija	(1)	a)	ima za cilj poboljšati digitalnu operativnu otpornost bankarskog sistema, posebno kroz podizanje svijesti u vezi sa cyber prijetnjama, ograničavanje ili ometanje mogućnosti širenja cyber prijetnji, podržavanje odbrambenih sposobnosti, tehnika otkrivanja prijetnji, strategija ublažavanja ili odgovora i oporavka,		
	Član 52.	Razmjena informacija	(1)	b)	odvija se u okviru bankarskog sistema, što uključuje i razmjenu informacija sa svim ostalim subjektima za koje je Agencije izdala dozvolu za rad i		
	Član 52.	Razmjena informacija	(1)	c)	provodi se kroz aranžmane za razmjenu informacija koji štite potencijalno osjetljivu prirodu informacija koje se razmjenjuju i koji su uređeni pravilima poslovnog ponašanja u kojima se u potpunosti poštuju poslovna tajna, zaštita ličnih podataka i smjernica o politici tržišne konkurencije.		
	Član 52.	Razmjena informacija	(2)		U svrhu stava (1), Agencija će osigurati platformu i aranžmane za razmjenu informacija.		
	Član 52.	Razmjena informacija	(3)		Aranžmanima za razmjenu informacija iz stava (1) potrebno je definisati uslove za učešće i, prema potrebi, navesti detaljno, eventualno uključivanje javnih uprava i svojstvo u kojem oni mogu biti povezani na aranžmane za razmjenu informacija, uključivanje IKT pružaoca usluga, operativne elemente, uključujući i korištenje namjenskih IKT platformi.		

IZVJEŠTAVANJE AGENCIJE	Član 53.	Obavještavanje i izvještavanje Agencije	(1)		Banka je dužna Agenciji dostaviti sljedeće interne izvještaje i akte: a) Strategiju IKT sistema i operativne planove, definisanu članom 9. i 10. ove odluke, b) Politiku i procedure za upravljanje IKT rizicima, definisane članom 14. ove odluke, c) Politiku informacione sigurnosti, definisanu članom 17. ove odluke, d) Strategiju upravljanja kontinuitetom poslovanja, definisanu članom 28. ove odluke, e) Politiku i procedure upravljanja IKT incidentima, definisane članom 41. ove odluke, f) Politiku i procedure testiranja digitalne operativne otpornosti, definisane članom 23. ove odluke, g) Politiku o korištenju IKT usluga trećih strana, definisane članom 45. ove odluke, h) Analizu uticaja na poslovanje, Plan kontinuiteta poslovanja u području IKT sistema i planove odgovora i oporavka IKT sistema, definisane članom 28., 29. i 30. ove odluke, i) Planove komunikacije u krizi, definisane članom 20. ove odluke, j) Program podizanja svijesti o informacionoj sigurnosti, definisan članom 21. ove odluke, k) Registar informacija u vezi sa svim ugovorima povezanim sa trećim stranama pružaocima IKT usluga, definisan članom 46. ove odluke, l) Rezultate procjene IKT rizika, definisane članom 16. ove odluke, m) Izvještaje o upravljanju IKT rizicima, definisane članom 18. stav (8) ove odluke, n) Izvještaje prema organima banke, definisane članom 5. stav (1) tačka h), o) Izvještaje o obavljenim testovima digitalne operativne otpornosti iz člana 23. ove odluke		
	Član 53.	Obavještavanje i izvještavanje Agencije	(2)		Banka je dužna interne akte iz stava (1) tačke a) – j) dostavljati godišnje, odnosno odmah po njihovim izmjenama.		
	Član 53.	Obavještavanje i izvještavanje Agencije	(3)		Banka je dužna izvještaje iz tačke (1) l) – p) dostavljati Agenciji 7 dana po usvajanju od strane organa upravljanja.		
	Član 53.	Obavještavanje i izvještavanje Agencije	(4)		Uprava banke je dužna pravovremeno obavijestiti Agenciju o svakoj značajnoj i kompleksnoj promjeni koja može imati uticaja na IKT sistem banke, te dostaviti odgovarajuću dokumentaciju (metodologiju upravljanja IKT projektima sa pratećom dokumentacijom, procjenu IKT rizika navedene promjene i drugo).		
OBJAVA INFOR	Član 54.	Objava informacija značajnih za javnost			Agencija može objaviti informacije, uključujući i mjere, za koje procijeni da su od značaja za javnost, a koje se odnose na upravljanje IKT sistemima, sigurnošću IKT sistema, cyber rizicima, kao i drugim specifičnim oblastima vezanim uz upotrebu IKT sistema i IKT.		
PRELAZNE I ZAVRŠ	Član 55.	Dodatna uputstva za primjenu odluke			U svrhu primjene odredbi ove odluke direktor Agencije će donijeti pripadajuća uputstva.	**Komentar:** 1. Odgovarajuća uputstva trebala biti dostavljena unajkraćem mogućem roku, obzirom da će u njima biti definisani svi parametri o kojima ćemo morati izvještavati, a naravno prije toga implementirati odgovarajuće sistemske ili proceduralne pretpostavke. Najmanje 6-9 mjeseci prije datuma do kada Banka treba da se uskladi sa novom Odlukom.	**Komentar:** 1. Odgovarajuća uputstva će biti dostavljena u što kraćem mogućem periodu. U međuvremenu za potrebe implementacije odluke, banke se mogu pozvati na objavljene RTS kao popratne akte DORA regulativi.
	Član 56.	Prelazne i završne odredbe	(1)		Danom početka primjene ove odluke prestaje da važi Odluka o upravljanju informacionim sistemom u banci („Službene novine Federacije BiH“, broj 81/17).		

NE ODREDBE	Član 56.	Prelazne i završne odredbe	(2)		Banka je dužna uskladiti svoje poslovanje sa odredbama ove odluke do 01.06.2025. godine.	**Komentar:** Uzimajući u obzir značajne izmjene predviđene odlukom, te implementaciju koja će zahtijevati izmjenu operativnog modela, organizacije, izradu i usvajanje dodatnih internih akata, a što prolazi različite procese i nivoe odobravanja predviđene internim procedurama banka, molimo za prolongaciju roka do 31.12.2025.	**Komentar:** PRIHVATA SE.
	Član 57.	Stupanje na snagu			Ova odluka stupa na snagu osmog dana od dana objavljivanja u „Službenim novinama Federacije BiH“, a primjenjuje se od 31.12.2024. godine.		