UREDBA O INFORMACIONIM SISTEMIMA I UPRAVLJANJU SAJBER RIZICIMA

Sadržaj

Na osnovu člana 35, stav 1, podtačka 1.1 i člana 65, stavovi 1 i 2 Zakona br. 03/L-209 o Centralnoj banci Republike Kosovo (Službeni list Republike Kosovo, br. 77/16. avgust 2010. godine), izmenjen i dopunjen Zakonom br. 05/L-150 (Službeni list br. 10/03. april 2017. godine), članom 85 i 114 Zakona br. 04/L-093 o bankama, mikrofinansijskim institucijama i nebankarskim finansijskim institucijama (Službeni list/br. 11/11. maj 2012. godine), članom 8 Zakona br. 04/L-155, o platnom sistemu (Službeni list/br. 12, 03. maj 2013. godine), članom 4, stav 3 Zakona br. 05/L-045 o osiguranju (Službeni list br. 38/4. decembar 2015. godine), članom 29, stav 8 Zakona br. 04/L-018 o obaveznom osiguranju od odgovornosti za motorna vozila (Službeni glasnik br. U skladu sa članom 4 stav 1, članom 20 stav 1, članom 13 stav 13.1, podstavom (d) Zakona br. 04/L-101 o penzionim fondovima Kosova („Službeni list“ br. 10/8. maj 2012.) i članom 34 Zakona br. 08/L-295 o kripto imovini („Službeni list“ br. 21/22. novembar 2024.), Odbor Centralne banke Republike Kosovo, na sednici održanoj 29. avgusta 2025. godine, usvojio je sledeće:

UREDBA O INFORMACIONIM SISTEMIMA I UPRAVLJANJU SAJBER RIZICIMA

POGLAVLJE I
OPŠTE ODREDBE

Član 1
Svrha i obim

1. Ova uredba utvrđuje minimalne standarde, kriterijume i procedure za informacionu tehnologiju i sajber rizik za finansijske institucije (FI) koji se primenjuju, u zavisnosti od složenosti i nivoa korišćenja informacione tehnologije.
2. Ova Uredba se primenjuje na sve finansijske institucije - licencirane ili nadgledane FI od strane Centralne banke Republike Kosovo (CBK).
3. Ova uredba se ne primenjuje na nebankarske finansijske institucije koje obavljaju samo devizne poslove, kao ni na posrednike u osiguranju.

Član 2
Definicije

1. Termini i definicije koji se koriste u ovoj uredbi imaju sledeća značenja:
   1.1. **Apetit za rizikom**- Ukupan nivo i vrste rizika koje je finansijski stručnjak spreman da preuzme, unapred utvrđene i u okviru svog kapaciteta za upravljanje rizikom, kako bi ostvario svoje strateške ciljeve i poslovni plan.
   1.2. **Stavka konfiguracije(CI)**- Upravljana komponenta IT sistema (hardver, softver ili dokumentacija) koja se koristi za upravljanje promenama i pružanje usluga.
   1.3. **Prateća sredstva**- Ljudi, tehnologija, informacije i oprema neophodni za obavljanje kritičnih operacija.

1.4. **Višefaktorska autentifikacija (MFA)**- Bezbednosni mehanizam koji zahteva više oblika verifikacije (npr. lozinke, biometriju, bezbednosne tokene itd.) pre nego što se odobri pristup.

1.5. **Savetodavni odbor za promene (KAB)**- je struktura u okviru procesa upravljanja IT promenama koja je zadužena za pregled, procenu i odobravanje ili odbacivanje predloga za promene u IT okruženju.

1.6. **Upravni odbor (BD)**- Upravno telo, odgovorno za nadzor upravljanja IKT rizicima, operativne održivosti, politika sajber bezbednosti i usklađenosti sa regulatornim zahtevima finansijske institucije.

1.7. **Klaud računarstvo**- Korišćenje skalabilnih računarskih resursa na zahtev, kao što su: prostor za skladištenje podataka, procesorska snaga i softver - obezbeđeni putem interneta.

1.8. **DevSecOps**- Integrisanje bezbednosnih praksi u razvoj softvera i IT operacije, kako bi se osigurao bezbedan razvoj IT sistema.

1.9. **Šifrovanje podataka**- Proces kodiranja podataka radi sprečavanja neovlašćenog pristupa, obezbeđivanja poverljivosti i integriteta.

1.10. **Incident**- svaki neplanirani, nepredviđeni ili namerni događaj koji negativno utiče ili ima potencijal da negativno utiče na poverljivost, integritet, dostupnost ili autentičnost podataka, informaciono-komunikacionih tehnologija (IKT) sistema i usluga koje podržavaju kritične ili regulisane funkcije FI, uzrokujući operativne poremećaje, gubitak podataka, finansijsku štetu, rizik po stabilnost finansijskog tržišta ili štetu po kredibilitet i ugled institucije. To je događaj koji ima, ili bi potencijalno mogao imati, negativan uticaj na poverljivost, integritet ili dostupnost informacija ili informacionih sistema FI

1.11. **Finansijske institucije (FI)**–U svetlu ove uredbe, pod finansijskim institucijama, ili FI institucijama, koristićemo termin „banke“, mikrofinansijske institucije, nebankarske finansijske institucije, osiguravajuća društva, Kosovski osiguravajući biro, penzijske štedionice, operatere kriptovaluta i druge subjekte koji obavljaju finansijske aktivnosti, kako je definisano u bilo kom relevantnom zakonu za potrebe ove uredbe.

1.12. **Obaveštajne informacije o sajber pretnjama(CTI)**- Prikupljanje, analiziranje i deljenje informacija o pretnjama po sajber bezbednost radi poboljšanja otkrivanja i ublažavanja rizika.

1.13. **Klasifikacija podataka**- Proces kategorizacije podataka, na osnovu relevantnih važećih propisa, u zavisnosti od nivoa osetljivosti zahteva za usklađenost i bezbednosnih potreba.

1.14. **Okvir za upravljanje rizicima(RMF)**- Strukturirani pristup definisanju uloga, odgovornosti, proceni rizika, merama za ublažavanje i aktivnostima praćenja vezanim za IKT i sajber bezbednost.

1.15. **Nikad sam**- Princip bezbednosti koji zahteva da se kritične ili osetljive operacije obavljaju u prisustvu većeg broja ovlašćenih lica kako bi se sprečile prevare ili greške.

1.16. **Upravljanje zakrpama(Zakrpa)**- Politika koja reguliše primenu softverskih zakrpa za rešavanje bezbednosnih ranjivosti i održavanje integriteta sistema.

1.17. **Upravljanje bezbednim odlaganjem** - Procedure koje obezbeđuju bezbedno odlaganje IT sredstava i podataka, uz očuvanje privatnosti podataka i usklađenosti sa propisima o zaštiti životne sredine.

1.18. **Upravljanje pristupom identitetu(IAM)**- Okvir koji obezbeđuje bezbedan i kontrolisan pristup IT sistemima, primenjujući principe kao što su: pristup sa najmanjim privilegijama, podela dužnosti i kontrole pristupa zasnovane na ulogama.

1.19. **Upravljanje incidentima**- Sistematski pristup otkrivanju, reagovanju, ublažavanju i oporavku od sajber bezbednosnih i IKT incidenata.

1.20. **Autsorsing i upravljanje dobavljačima tehnoloških usluga – (OTSPM)**- Regulatorni okvir koji reguliše korišćenje spoljnih pružalaca usluga za kritične funkcije, obezbeđujući odgovornost i usklađenost.

1.21. **Upravljanje promenama**- Strukturirani proces koji osigurava da se promene IKT sistema procenjuju, odobravaju, implementiraju i dokumentuju uz minimalne poremećaje.

1.22. **Upravljanje tehnološkim rizicima – (TRM)**- Strukturirani pristup identifikovanju, proceni, ublažavanju i praćenju rizika vezanih za IKT i sajber bezbednost.

1.23. **Veštačka inteligencija(AI)**Upravljanje rizicima modela - Proces osiguravanja da su modeli veštačke inteligencije transparentni, objašnjivi, podložni reviziji i bez pristrasnosti.

1.24. **Upravljanje IKT rizicima**- Proces upravljanja rizicima vezanim za informaciono-komunikacione tehnologije, obezbeđujući bezbedno i otporno poslovanje.

1.25. **Upravljanje bezbednošću virtuelizovanih sistema** - Bezbednosne mere za virtuelizovana okruženja, uključujući: hipervizore, virtuelne mašine i infrastrukturu zasnovanu na oblaku.

1.26. **Bezbedno upravljanje centrima podataka**- Mere koje obezbeđuju fizičku i sajber zaštitu infrastrukture finansijskog centra podataka.

1.27. **Bezbedno upravljanje mrežom**- Politike i kontrole koje obezbeđuju bezbedan rad i segmentaciju IT mreže finansijske institucije.

1.28. **Upravljanje kontinuitetom poslovanja(BCM) -**Strateški pristup osiguravanju da kritične poslovne funkcije mogu da se nastave tokom i nakon prekida, bilo da su u pitanju sajber napadi, tehnički problemi ili prirodne katastrofe.

1.29. **Praćenje i izveštavanje o riziku-**Kontinuirana procena i izveštavanje o izloženosti riziku višem rukovodstvu i regulatornim organima.

1.30. **Podela dužnosti (SoD)**- Mehanizam kontrole koji osigurava da se ključne odgovornosti dele između više pojedinaca, kako bi se smanjio rizik od prevare, grešaka ili neovlašćenih radnji.

1.31. **Interfejsi za programiranje aplikacija(API**) - Interfejsi koji omogućavaju sistemima da bezbedno komuniciraju, sa kontrolama koje obezbeđuju poverljivost i integritet podataka.

1.32. **Osnova potrebe za korišćenjem**– Politika ograničenja gde se pristup sistemima, podacima ili resursima odobrava samo kada je to izričito potrebno za određeni zadatak ili funkciju.

1.33. **Pružalac tehnoloških usluga(TSP)**- Spoljni entitet koji pruža IT usluge, infrastrukturu ili aplikacije organizacijama, često na osnovu ugovornog sporazuma.

1.34. **Pružaoci usluga treće strane**- Spoljni entiteti koji pružaju usluge vezane za IKT, uključujući rešenja za računarstvo u oblaku, autsorsing i sajber bezbednost.

1.35. **Kritične operacije**- Čiji bi prekid uticao na kontinuirano poslovanje finansijskog uređenja ili njegovu ulogu u finansijskom sistemu. Da li je određeno poslovanje „kritično" zavisi od prirode finansijskog uređenja i njegove uloge u finansijskom sistemu.

1.36. **Usklađenost sa propisima za veštačku inteligenciju**- Zahtev za finansijske institucije da obezbede da aplikacije veštačke inteligencije u kritičnim funkcijama ispunjavaju zakonske i regulatorne standarde.

1.37. **Sprečavanje curenja podataka(Zaštita od gubitka energije)**- Bezbednosne mere i tehnologije dizajnirane za otkrivanje, praćenje i sprečavanje neovlašćenog pristupa, prenosa ili modifikacije osetljivih podataka.

1.38. **Fišing**-Obmanjujuća praksa slanja imejlova ili drugih poruka koje tvrde da dolaze od nekog drugog, sa namerom da se prevare pojedinci da otkriju svoje akreditive ili lične podatke, kao što su lozinke, brojevi kreditnih kartica ili druge poverljive informacije.

1.39. **Plan za reagovanje na sajber incidente**- Skup unapred definisanih akcija koje finansijski posrednik preduzima kako bi obuzdao, ublažio i oporavio se od sajber incidenta.

1.40. **Plan oporavka od katastrofe(DRP)**- Dokumentovana strategija za obnavljanje IKT sistema i podataka nakon većeg kvara ili sajber incidenta.

1.41. **Bezbedne prakse kodiranja**- Metodologije programiranja dizajnirane da spreče ranjivosti, kao što su: napadi ubrizgavanjem, kršenje podataka i sistemski eksploati.

1.42. **Najmanja privilegija**- Princip bezbednosti gde se korisnicima, aplikacijama ili sistemima dodeljuje samo minimalni nivo pristupa neophodan za obavljanje njihovih radnih funkcija.

1.43. **Centar za operacije sajber bezbednosti(SOC)**- Centralizovana jedinica odgovorna za praćenje, otkrivanje, analizu i reagovanje na pretnje po sajber bezbednost.

1.44. **Upravljanje i nadzor**- Interni okvir unutar finansijske institucije za razumno i efikasno upravljanje rizicima informaciono-komunikacione tehnologije (IKT) i sajber rizika.

1.45. **Upravljanje Klaud računarstvom**- Nadgledanje usluga zasnovanih na oblaku kako bi se osigurala bezbednost podataka, usklađenost sa propisima i operativna održivost.

1.46. **Upravljanje veštačkom inteligencijom (VI)**- Politike i okviri koji obezbeđuju etičku, odgovornu i regulatorno usklađenu upotrebu veštačke inteligencije u finansijskim uslugama.

1.47. **Operativna održivost**- To je sposobnost finansijske institucije (FI) da sprovodi kritične operacije uprkos operativnim ograničenjima. Ova sposobnost omogućava FI da identifikuje i zaštiti se od pretnji i potencijalnih kvarova, da reaguje i prilagođava se, kao i da se oporavi od i uči iz ometajućih događaja kako bi se minimizirao njihov uticaj na sprovođenje kritičnih operacija uprkos operativnim ograničenjima. Prilikom razmatranja

svoje operativne otpornosti, FI treba da pretpostavi da će do poremećaja doći i da uzme u obzir svoj ukupni apetit za rizikom i toleranciju na poremećaje.

1.48. **Ransomwer**- vrsta zlonamernog softvera koji šifruje ili zaključava podatke i sisteme korisnika ili institucije, zahtevajući plaćanje (otkupninu) da bi ih vratio u normalno stanje.

1.49. **Regulatorno izveštavanje o sajber incidentima**- Zahtev da finansijske institucije prijave incidente u vezi sa sajber bezbednošću Centralnoj banci Republike Kosovo (CBK) u određenim vremenskim okvirima.

1.50. **Suvišno**– posedovanje dodatnih ili dupliranih sistema, komponenti ili resursa za obezbeđivanje rezervne kopije u slučaju da primarni otkaže – obezbeđivanje kontinuiranog rada i visoke dostupnosti.

1.51. **Očuvanje i oporavak**- Proces bezbednog čuvanja kopija podataka i osiguravanja njihovog oporavka u slučaju oštećenja ili gubitka.

1.52. **Bezbednost krajnjeg uređaja**- Mere za zaštitu uređaja kao što su: radne stanice, laptopovi i mobilni uređaji od sajber pretnji.

1.53. **Nezavisna revizijska uverljivost**- Nezavisan proces pregleda kontrola bezbednosti IKT-a, upravljanja i usklađenosti sa propisima.

1.54. **Donesite svoj uređaj (BYOD)**- Politika koja dozvoljava zaposlenima da koriste svoje lične uređaje, kao što su pametni telefoni i laptopovi, u poslovne svrhe, nudeći fleksibilnost i praktičnost, ali zahtevajući pažljivo upravljanje bezbednosnim rizicima.

1.55. **Skeniranje ranjivosti**- Redovne procene IKT sistema radi identifikacije i ublažavanja bezbednosnih ranjivosti.

1.56. **IKT strategija**- Plan koji usklađuje IKT mogućnosti sa opštim poslovnim ciljevima finansijske institucije, obuhvatajući unapređenje sistema, politike sajber bezbednosti i zavisnosti od trećih strana.

1.57. **Test stresa u veštačkoj inteligenciji**- Proces evaluacije veštačke inteligencije (AI) pod različitim uslovima radi procene njihove stabilnosti i pouzdanosti.

1.58. **Distribuirani napad uskraćivanja usluge (DDoS)**- Distribuirani napad uskraćivanjem usluge (DDoS) je sajber napad koji preopterećuje ciljani sistem, mrežu ili veb lokaciju prekomernim saobraćajem iz više izvora, uzrokujući usporavanja ili prekide rada.

1.59. **Testiranje penetracije**- Simulirani sajber napadi sprovedeni radi procene zaštite i otpornosti sajber bezbednosti finansijske institucije.

1.60. **Upravljanje rizicima**- Sprovođenje mera za ublažavanje ili smanjenje rizika na prihvatljiv nivo.

1.61. **Transparentnost odluka veštačke inteligencije**- Zahtev da finansijski stručnjaci otkriju kada odluke vođene veštačkom inteligencijom utiču na klijente i da obezbede mehanizam za žalbe.

1.62. **Vežbe reagovanja na incidente**- Aktivnosti testiranja i obuke za procenu efikasnosti plana reagovanja na incidente finansijske institucije.

1.63. **Virtuelizacija**- korišćenje softverskih tehnologija ili tehnika za stvaranje sloja apstrakcije nad fizičkim resursima informacione tehnologije (serveri, mreže, skladišta podataka ili desktop računari), kako bi se omogućilo razdvajanje, izolovanje i izvršavanje nezavisnih logičkih okruženja na istoj fizičkoj infrastrukturi.

1.64. **Procena kompetentnosti dobavljača**- Procena trećih strana kako bi se osiguralo da ispunjavaju potrebnu stručnost za ugovorene IKT funkcije.

1.65. **Procena rizika** - Identifikovanje i procena pretnji, ranjivosti i potencijalnih posledica radi utvrđivanja verovatnoće i uticaja rizika.

1.66. **Procena rizika od pretnji i ranjivosti (TVRA)**- Proces koji procenjuje potencijalne pretnje i ranjivosti u IT i fizičkom okruženju organizacije, kako bi se utvrdili bezbednosni rizici i strategije za ublažavanje identifikovanih rizika.

1.67. **Glavni službenik za bezbednost informacija (CISO)**- Viši rukovodilac odgovoran za kreiranje i održavanje vizije, strategije i programa bezbednosti finansijskih institucija za zaštitu informacionih sredstava i IKT sistema.

1.68. **Glavni tehnološki direktor(Tehnički direktor)**- Rukovodilac odgovoran za nadgledanje tehnološke strategije, infrastrukture i digitalne održivosti finansijske institucije.

Član 3
Princip proporcionalnosti

2. Sve banke moraju da se pridržavaju zahteva propisanih ovom uredbom.
3. Pored institucija iz stava 1. ovog člana, ostale institucije na koje se primenjuje ova uredba odgovorne su za obezbeđivanje usklađenosti sa relevantnim zahtevima na osnovu svoje veličine, ukupnog profila rizika, unutrašnje organizacije i prirode, obima, složenosti i rizičnosti svojih usluga, aktivnosti i poslovanja, bez obzira na to da li se one trenutno pružaju ili su namenjene.
4. Prilikom nadzora finansijskih institucija, CBK će procenjivati usklađenost i sa tekstom i sa duhom i svrhom ove uredbe, a njene odluke o takvim pitanjima su konačne. Ovaj princip proporcionalnosti osigurava da su regulatorne obaveze na odgovarajući način prilagođene specifičnim karakteristikama i rizicima svake institucije, uz održavanje odgovornosti za usklađenost.
5. FI koji imaju viši nivo složenosti i tehnologije koju koriste mogu sprovesti dodatne odgovarajuće mere, uključujući upotrebu naprednih tehnologija, kako bi ublažili takve rizike.

POGLAVLJE II
UPRAVLJANJE I NADZOR

Član 4
Upravljanje i organizacija

1. FI mora imati okvir upravljanja i interne kontrole koji obezbeđuje efikasno i razumno upravljanje rizicima informaciono-komunikacione tehnologije (IKT) i sajber rizika, sa ciljem postizanja visokog nivoa digitalne operativne održivosti.
2. Upravni odbor (UO) treba da pregleda i odobri pristup operativnoj otpornosti finansijskog institucije, uzimajući u obzir ukupnu toleranciju finansijskog institucije na poremećaje u njegovim kritičnim operacijama. Prilikom formulisanja tolerancije na poremećaje finansijskog institucije, UO treba da uzme u obzir operativne mogućnosti finansijskog institucije, uzimajući u obzir širok spektar ozbiljnih, ali verovatnih scenarija koji bi uticali na njegove kritične operacije. UO treba da osigura da politike finansijskog institucije efikasno rešavaju slučajeve u kojima mogućnosti finansijskog institucije nisu dovoljne da ispune navedenu toleranciju na poremećaje.
3. Odbor je odgovoran za odobravanje svih politika koje se odnose na informacione sisteme (uključujući, ali ne ograničavajući se na, IKT, bezbednost informacija i/ili sajber bezbednost) i mora godišnje procenjivati adekvatnost politika i preispitati ih.
4. Upravni odbor i viši menadžment finansijske institucije moraju da obezbede da se primenjuju efikasne interne kontrole i prakse upravljanja rizicima kako bi se postigla bezbednost i pouzdanost njenog IKT operativnog okruženja.
5. Upravni odbor i viši menadžment treba da imaju članove sa potrebnim iskustvom za razumevanje i upravljanje tehnološkim rizicima, koji uključuju rizike koje predstavljaju sajber pretnje.
6. FI mora imati odgovarajuće funkcije vezane za upravljanje IKT-om, IKT rizikom, bezbednošću IKT sistema i kontinuitetom poslovanja.
7. FI mora da odredi osobu ili jedinicu odgovornu za bezbednost informacija, koja mora da upravlja bezbednošću informacionog sistema i koordinira politike i procese bezbednosti informacija u vezi sa funkcijama i tehnološkim platformama. Jedinica ili osoba odgovorna za bezbednost informacija mora da izveštava generalnog direktora i mora biti nezavisna od drugih organizacionih jedinica. Preko generalnog direktora, mora da izveštava najmanje jednom godišnje i po potrebi Upravni odbor, koji mora biti obavešten o poslovanju i funkcijama vezanim za bezbednost informacija.
8. FI će imenovati glavnog službenika za informacione tehnologije i glavnog službenika za informacionu bezbednost, koji poseduju neophodnu stručnost i iskustvo. CBK će biti obaveštena 30 dana pre takvih imenovanja, uz obrazloženje predloženih kandidata. CBK zadržava pravo da se usprotivi svakom takvom imenovanju tokom roka za obaveštenje ili u kasnijoj fazi. FI koja, u skladu sa članom 3 ove uredbe, odluči da ne imenuje takve pozicije, mora da obezbedi dovoljno stručnosti, iskustva i nezavisnosti za efikasno obavljanje takvih uloga.
9. FI treba da obezbedi dovoljan broj FI zaposlenih sa relevantnim veštinama za podršku njihovim operativnim potrebama u oblasti IKT i njihovim procesima upravljanja IKT rizicima, kao i da obezbedi sprovođenje njihove IKT strategije, dodelom neophodnih sredstava i pružanjem odgovarajuće obuke o IKT rizicima zaposlenima, uključujući nosioce ključnih funkcija, na godišnjem nivou ili češće ako je potrebno.

10. Upravni odbor i viši menadžment treba da obezbede da se ključne IKT odluke donose u skladu sa tolerancijom na rizik finansijske institucije.

11. Upravni odbor i viši menadžment treba da neguju snažnu kulturu svesti o tehnološkim rizicima i upravljanja njima, uključujući sajber higijenu na svim nivoima zaposlenih u finansijskim institucijama.

12. Upravni odbor ili odbor delegiran u okviru njega je odgovoran za:

    12.1. obezbeđivanje čvrstog i robusnog okvira za upravljanje rizicima;

    12.2. efikasno sprovođenje i održavanje politika, procedura i standarda za upravljanje IKT i sajber rizicima;

    12.3. obezbeđivanje funkcije upravljanja tehnološkim rizicima (TRM) radi nadgledanja Okvira i strategije upravljanja tehnološkim rizicima (TRMF), pružajući nezavisnu perspektivu o tehnološkim rizicima sa kojima se suočava finansijska institucija;

    12.4. obezbeđivanje dovoljnih ovlašćenja, resursa i pristupa Odboru višim menadžerima, koji su odgovorni za izvršenje TRMF-a FI;

    12.5. usvajanje izjave o toleranciji na rizik koja artikuliše prirodu i obim tehnoloških rizika koje je finansijski stručnjak spreman i sposoban da preuzme;

    12.6. redovan pregled TRMF-a radi kontinuirane relevantnosti;

    12.7. procena upravljačkih kompetencija za upravljanje tehnološkim rizicima i

    12.8. obezbeđivanje uspostavljanja nezavisne revizorske funkcije za procenu efikasnosti internog kontrolnog okruženja, upravljanja rizicima i upravljanja finansijske institucije.

13. Viši menadžment je odgovoran za:

    13.1. stvaranje TRMF-a;

    13.2. upravljanje tehnološkim rizicima u skladu sa definisanim TRMF-om;

    13.3. jasno definisanje uloga i odgovornosti zaposlenih u upravljanju tehnološkim rizicima i

    13.4. odmah obaveštavajući Upravni odbor o značajnim i nepovoljnim razvojima događaja i incidentima sa tehnološkim rizicima koji mogu imati veliki uticaj na IF.

Član 5
Strategija, politike i procedure

14. Za pravilno upravljanje informaciono-komunikacionom tehnologijom (IKT), FI mora:

    14.1. Usvojiti IKT strategiju

    14.2. Definisati akcione planove koji podržavaju sprovođenje IKT strategije i

    14.3. Kreirati procese za praćenje i merenje efikasnosti strategije.

15. Upravno telo ima ukupnu odgovornost za definisanje, odobravanje i nadgledanje sprovođenja IKT strategije finansijske institucije kao dela njihove ukupne poslovne strategije, kao i za uspostavljanje efikasnog okvira za upravljanje rizicima u vezi sa IKT i bezbednosnim rizicima kako bi se osigurala usklađenost sa važećim zakonskim propisima/propisima.

16. FI treba da uskladi IKT strategiju sa ukupnom poslovnom strategijom, kako bi obuhvatio:

    16.1. Kako bi trebalo da se razvija IKT da bi efikasno podržao i implementirao poslovnu strategiju, uključujući evoluciju organizacione strukture, promene IKT sistema i ključne zavisnosti sa trećim stranama;

    16.2. Planirana strategija i evolucija IKT arhitekture, uključujući zavisnosti od trećih strana; i

    16.3. Jasni ciljevi informacione bezbednosti, sa fokusom na IKT sisteme i IKT usluge, osoblje i procese.

17. U akcionom planu pomenutom u pasusu14, podstav14.2ovog člana, finansijski inspektor određuje aktivnosti koje treba preduzeti radi postizanja ciljeva IKT strategije. finansijski inspektor redovno preispituje akcione planove kako bi se osigurala njihova relevantnost i prikladnost.

18. FI treba da uspostavi politike, standarde i procedure i, gde je to prikladno, da uključi industrijske standarde i najbolje prakse za upravljanje tehnološkim rizicima i zaštitu informacionih sredstava. Politike, standarde i procedure takođe treba redovno preispitati i ažurirati (najmanje jednom godišnje), uzimajući u obzir razvoj tehnologije i okruženje sajber pretnji.

19. Politike upravljanja IKT-om treba da definišu najmanje sledeće elemente:

    19.1. Administracija i rad IKT sistema

    19.2. Organizaciona struktura za upravljanje IKT-om

    19.3. Hardverska i softverska infrastruktura IKT oblasti (konfiguracioni dijagrami)

    19.4. Klasifikacija dokumentacije i zaštita sistema i podataka

    19.5. Rezervna kopija podataka informacionih sistema

    19.6. Plan kontinuiteta poslovanja

    19.7. Sistemi za upravljanje promenama

    19.8. Upravljanje incidentima

    19.9. Upravljanje rizicima IT sistema

    19.10. Definisanje bezbednosnih mehanizama za IKT sisteme i

    19.11. Upravljanje trećim stranama.

20. Procedure treba da definišu konkretne korake i akcije za efikasnu implementaciju politika. One treba da obezbede dosledne, bezbedne i efikasne operacije u svim IKT sistemima. Svaki proceduralni element treba da bude u skladu sa definisanim oblastima politike, pokrivajući svakodnevne operacije, reagovanje u vanrednim situacijama i metode za zaštitu integriteta podataka i bezbednosti sistema.

21. FI treba u potpunosti da pregleda i proceni rizike povezane sa odstupanjima od odobrenih politika, standarda i procedura i da dobije odobrenje višeg rukovodstva za materijalna odstupanja. Odobrena odstupanja treba periodično preispitati kako bi se osiguralo da su preostali rizici na prihvatljivom nivou.

22. Trebalo bi implementirati procese usklađenosti (npr. model sa tri linije) kako bi se proverilo da li se politike, standardi i procedure poštuju. To uključuje procese praćenja u slučaju nepoštovanja propisa.

Član 6
Upravljanje IKT imovinom i informacijama

23. Da bi imali tačnu i potpunu sliku o IKT operativnom okruženju finansijske institucije, finansijske institucije treba da uspostave prakse upravljanja informacionom imovinom i da vode inventar svih sredstava, kako fizičkih tako i logičkih, koji uključuje sledeće:

    23.1. identifikacija informacionih sredstava koja podržavaju poslovanje i pružanje usluga finansijske institucije, uključujući vrstu sredstava, format, lokaciju, informacije o rezervnoj kopiji (gde je primenljivo), informacije o licenci i poslovnu vrednost.

    23.2. klasifikacija informacionih sredstava na osnovu njihove kritične važnosti.

    23.3. određivanje vlasništva nad informacionim sredstvima, kao i uloge i odgovornosti osoblja koje upravlja tim sredstvima. Vlasnik sredstava je odgovoran za:

    1.3.1. osiguravanje da su informacije i sredstva vezana za obradu informacija klasifikovani prema osetljivosti

    1.3.2. uspostavljanje i redovno preispitivanje ograničenja pristupa i klasifikacije; i

    1.3.3. uspostavljanje politika, standarda i procedura za upravljanje informacionim sredstvima na osnovu njihove kritičnosti.

Član 7
Upravljanje dobavljačima usluga treće strane

24. Bez obzira na propise o autsorsingu, pre sklapanja ugovornih sporazuma ili partnerstava sa trećim licima, finansijski stručnjak treba da proceni svoju izloženost tehnološkim rizicima koji mogu uticati na poverljivost, integritet i dostupnost IKT sistema i podataka i da upravlja takvim izloženostima tokom životnog ciklusa trećih lica. Pored toga, trebalo bi da ima odgovarajuću strategiju izlaska za rešavanje planiranih i neplaniranih odlazaka sa tehnologija koje se koriste.

25. Da bi se osigurao kontinuitet IKT usluga i IKT sistema, i bez ugrožavanja drugih važećih zahteva u skladu sa propisima o autsorsingu, finansijski institucionalni ...

    25.1. odgovarajući i srazmerni ciljevi i mere koje se odnose na bezbednost informacija, uključujući zahteve kao što su minimalni zahtevi za sajber bezbednost; specifikacije životnog ciklusa finansijskih podataka; sve zahteve koji se odnose na šifrovanje podataka, bezbednost mreže i procese praćenja bezbednosti, kao i lokaciju centara podataka, i

    25.2. operativne i bezbednosne procedure za rešavanje incidenata, uključujući eskalaciju i izveštavanje.

26. FI treba da prati i traži uveravanja o nivou usklađenosti ovih dobavljača sa bezbednosnim ciljevima, merama i ciljevima učinka FI.

27. FI mora kontinuirano voditi registar svih dobavljača usluga trećih strana (uključujući usluge u oblaku) i osigurati da ovi dobavljači održavaju visok standard brige u zaštiti poverljivosti i integriteta podataka, kao i u obezbeđivanju dostupnosti sistema.

Član 8
Pregled kompetencija i iskustva

28. FI treba da osigura da osoblje, uključujući izvođače radova i pružaoce usluga, ima potreban nivo kompetencija i veština za obavljanje IKT funkcija u IKT okruženju, kako bi upravljalo tehnološkim rizicima. Svi IKT zaposleni treba da imaju detaljne opise poslova, dužnosti i odgovornosti kako bi se osiguralo da su uloge, odgovornosti i potrebne veštine adekvatno definisane.

29. Trebalo bi sprovoditi provere prošlosti osoblja koje ima pristup finansijskim podacima i IKT sistemima kako bi se ublažio insajderski rizik, uključujući rizik od kršenja podataka, sabotaže i prevare od strane osoblja, izvođača radova i pružalaca usluga.

30. FI mora dokumentovati procese u skladu sa ovim članom kako bi ispunio zahteve iz ovog člana.

Član 9
Svest o bezbednosti informacija i obuka

31. Fiskalne institucije (FI) treba da uspostave sveobuhvatni program obuke o bezbednosti IKT kako bi održale visok nivo svesti među svim zaposlenima u FI. Program obuke treba, kao minimum, da sadrži informacije o preovlađujućem okruženju sajber pretnji i njegovim implikacijama, politikama i standardima bezbednosti IKT FI i odgovornosti svakog pojedinca za zaštitu informacionih sredstava. Svo osoblje treba da bude upoznato sa važećim zakonima, propisima i smernicama koje se odnose na korišćenje i pristup informacionim sredstvima.

32. Program obuke mora se sprovoditi najmanje jednom godišnje za sve zaposlene, izvođače radova i pružaoce usluga koji imaju pristup kritičnim informacionim sredstvima finansijske institucije.

33. Rukovodioci upravnog odbora treba da prođu obuku kako bi se povećala svest o rizicima povezanim sa upotrebom tehnologije i kako bi se učvrstilo njihovo razumevanje praksi upravljanja strategijom upravljanja rizikom.

34. Program obuke treba periodično preispitati kako bi se osiguralo da njegov sadržaj ostane aktuelan i relevantan. Pregled treba da uzme u obzir promene u politikama bezbednosti IKT finansijske institucije, preovlađujuće i nove rizike, evoluirajuće okruženje sajber pretnji, lekcije naučene iz prethodnih inicijativa za obuku i sve potrebe za obukom identifikovane kroz posmatranje ponašanja, npr. nenajavljeni testovi fišinga zaposlenih.

Član 10
Prognoza budžeta

35. FI treba da izdvoje dovoljna budžetska sredstva kako bi se postigao odgovarajući nivo sajber pripremljenosti.

36. Budžet za sajber bezbednost treba da bude nezavisan od ukupnog IKT budžeta finansijske institucije, kako bi se osiguralo da razvoj poslovnih sistema ne konkuriše za resurse dodeljene zaštiti IKT sistema.

37. Prilikom raspodele budžeta za svaku godinu, trebalo bi uzeti u obzir i potrebe za obukom osoblja za informacione sisteme/kibernetičku bezbednost.

POGLAVLJE III
TEHNOLOGIJA I UPRAVLJANJE SAJBER RIZICIMA

Član 11
Okvir za upravljanje rizicima

38. FI treba da uspostavi Okvir za upravljanje rizicima kako bi se efikasno bavio rizicima u oblasti IKT i sajber industrije. Treba uspostaviti odgovarajuće strukture i procese upravljanja, sa dobro definisanim ulogama, odgovornostima i linijama izveštavanja u svim različitim organizacionim funkcijama.

39. Sve identifikovane tehnološke rizike treba dodeliti vlasnicima rizika, odgovornim za uspostavljanje i sprovođenje odgovarajućih mera za upravljanje rizicima.

40. Proces upravljanja rizicima treba da se izvršava više puta i redovno, uključujući sledeće komponente:

    40.1. procena rizika, koja se sastoji od identifikacije i analize rizika, kako bi se razumeli rizici sa kojima se suočava finansijska institucija;

    40.2. rešavanje rizika, fokusirajući se na sprovođenje mera za ublažavanje rizika koje štite poverljivost, integritet i dostupnost informacionih sredstava; i

    40.3. praćenje rizika, pregled i izveštavanje o rizicima, omogućavajući zainteresovanim stranama da odmah identifikuju i saopšte promene u rizicima.

41. S obzirom na to da se poslovno, IT okruženje i okruženje sajber pretnji vremenom razvijaju, finansijska institucija treba redovno da preispituje adekvatnost i efikasnost svog okvira za upravljanje rizicima i da po potrebi sprovodi korektivne mere.

42. FI mora dokumentovati metodologiju upravljanja rizicima koju koristi i odobriti je od strane Upravnog odbora.

43. FI treba sveobuhvatno da dokumentuje sve iteracije procesa upravljanja rizicima i njihove rezultate, kao što su kriterijumi za procenu, korišćeni podaci, registri rizika i planovi sanacije.

44. Kao minimum, svake godine treba pripremiti rezimirani izveštaj o rezultatima procesa upravljanja rizicima, registar rizika i detaljan plan sanacije na odobrenje odbora.

45. Upravljanje tehnološkim rizicima (TRM) treba da obuhvati sve integrisane informacione sisteme finansijske institucije u svim fazama njihovog razvoja.

46. Upravljanje rizicima informacionog sistema trebalo bi da uključuje godišnji plan podizanja svesti zaposlenih u finansijskim institucijama o odgovarajućem korišćenju usluga koje se pružaju putem informacionog sistema finansijskih institucija.

Član 12
Procena rizika

47. Najmanje jednom godišnje ili u slučaju bilo kakvih značajnih promena zahteva za bezbednost IKT sistema, finansijski institucionalni stručnjak (FI) će sprovesti analizu rizika IKT sistema kako bi se osiguralo da se ovaj rizik drži u granicama tolerancije u odnosu na aktivnost FI. Rezultati analize rizika moraju biti dokumentovani.

48. Tokom procesa identifikacije rizika, finansijski stručnjak treba da:

    48.1. identifikuje pretnje po svoje informacione resurse;

    48.2. identifikuje ranjivosti koje pretnje mogu iskoristiti;

    48.3. identifikuje postojeće kontrole; i

    48.4. identifikuje potencijalne posledice u različitim scenarijima ako pretnje iskoriste identifikovane ranjivosti. Prilikom identifikovanja potencijalnih posledica, finansijski stručnjak treba da uzme u obzir finansijske, operativne, pravne, reputacione i regulatorne faktore.

49. Tokom procesa analize rizika, finansijski stručnjak treba da proceni

    49.1. verovatnoću pretnji koje iskorišćavaju identifikovane ranjivosti;

    49.2. obim posledica ako pretnje iskoriste identifikovane ranjivosti, i

    49.3. odredi metriku nivoa rizika svakom riziku, na osnovu ovih procena.

Član 13
Upravljanje rizicima

50. FI treba da razvije i implementira mere za ublažavanje rizika koje su u skladu sa kritičnošću informacionih sredstava i prihvaćenim nivoom tolerancije na rizik.

51. FI treba da proceni da li su rizici smanjeni na prihvatljiv nivo nakon sprovođenja mera za ublažavanje. Kriterijumi i ovlašćenja za odobravanje prihvatanja preostalog rizika treba da budu jasno definisani i treba da budu u skladu sa tolerancijom FI na rizik.

52. Gde god je to moguće, finansijski stručnjak treba da razmotri osiguranje za različite osiguravajuće tehnologije kako bi ublažio finansijske uticaje, kao što su troškovi oporavka i nadoknade.

Član 14
Praćenje, pregled i izveštavanje o riziku

53. FI treba da uspostavi proces za procenu i praćenje promena rizika.

54. Značajne rizike treba pažljivo pratiti i izveštavati Odbor i viši menadžment. Učestalost praćenja i izveštavanja treba da bude srazmerna nivou rizika.

55. Da bi se olakšalo izveštavanje menadžmenta o rizicima, trebalo bi razviti metrike tehnološkog rizika kako bi se istakla informaciona sredstva sa najvećom izloženošću riziku. Ove metrike treba da uzmu u obzir rizične događaje, nalaze revizije i relevantne regulatorne zahteve.

Član 15
Okvir za upravljanje projektima

56. Za velike projekte, trebalo bi osnovati upravni odbor projekta kako bi se osigurao njihov efikasan nadzor i upravljanje.

57. Trebalo bi uspostaviti okvir za upravljanje projektima kako bi se osigurala doslednost u praksi upravljanja projektima i ostvarivanje rezultata koji ispunjavaju ciljeve i zahteve projekta. Okvir treba da obuhvati politike, standarde, procedure, procese i aktivnosti od pokretanja projekta do njegovog završetka.

58. Detaljnu dokumentaciju IKT projekata treba da kreira, održava i odobri relevantni poslovni i IKT menadžment. Dokumentacija treba da definiše poslovni slučaj, obim i budžet projekta, kao i glavne faze, aktivnosti i rezultate za svaku fazu projekta. Uloge i odgovornosti osoblja uključenog u projekat treba da budu jasno definisane.

Član 16
Nabavka IT sistema

FI treba da uspostavi standarde i procedure za procenu i izbor dobavljača kako bi se osiguralo da je izabrani dobavljač kvalifikovan i sposoban da ispuni zahteve projekta. Nivo procene treba da bude u skladu sa važnošću očekivanja projekta za FI.

Član 17
Životni ciklus razvoja sistema i bezbednost po dizajnu

59. FI treba da uspostavi okvir za upravljanje životnim ciklusom razvoja sistema (SDLC) kako bi jasno definisao procese, procedure i kontrole u svakoj fazi životnog ciklusa, kao što su početak/planiranje, analiza zahteva, projektovanje, implementacija, testiranje i prihvatanje. Treba održavati standarde i procedure za različite faze.

60. FI treba da uključi bezbednosne specifikacije u dizajn sistema, da sprovodi kontinuirane bezbednosne procene i da se pridržava bezbednosnih praksi tokom celog životnog ciklusa razvoja sistema. Bezbednosni zahtevi treba da pokrivaju ključne oblasti kontrole, kao što su kontrola pristupa, autentifikacija, autorizacija, integritet i poverljivost podataka, evidentiranje aktivnosti, praćenje bezbednosnih događaja i rukovanje izuzecima. Životni ciklus razvoja sistema treba da uključuje funkciju IT bezbednosti u svakoj fazi životnog ciklusa.

Član 18
Analiza sistemskih zahteva

61. FI treba da identifikuje, definiše i dokumentuje funkcionalne zahteve za IT sisteme. Pored funkcionalnih zahteva, treba definisati i dokumentovati ključne zahteve kao što su performanse sistema i bezbednosne kontrole.

62. Prilikom određivanja bezbednosnih zahteva, finansijska institucija treba da proceni potencijalne pretnje i rizike povezane sa svojim IT sistemima određivanjem nivoa bezbednosti neophodnog za zadovoljavanje svojih poslovnih potreba.

Član 19
Projektovanje i implementacija sistema

63. Kao deo faze projektovanja, finansijski investitor treba da pregleda predloženu arhitekturu i dizajn IT sistema, uključujući IT i kontrole bezbednosti informacija koje će biti ugrađene u sistem, kako bi se osigurala usklađenost sa navedenim zahtevima.

64. FI mora da proveri da li su zahtevi iz sistemskog dizajna ispunjeni tokom projektovanja i implementacije sistema. Bilo kakve izmene ili odstupanja od definisanih zahteva moraju biti odobrene od strane relevantnih zainteresovanih strana.

65. Relevantni stručnjaci u ovoj oblasti treba da budu angažovani da učestvuju u pregledu projekta.

Član 20
Testiranje i prihvatanje sistema

66. Treba definisati metodologiju za testiranje sistema. Obim testiranja treba da obuhvati poslovnu logiku, funkcionalnost sistema, bezbednosne kontrole i performanse sistema pod različitim uslovima opterećenja i stresa. Plan testiranja treba da bude definisan i odobren pre testiranja.

67. Problemi identifikovani tokom testiranja, uključujući sistemske nedostatke ili softverske greške, treba da budu dokumentovani i rešeni na odgovarajući način. Veći problemi koji bi mogli negativno uticati na poslovanje finansijskih institucija ili pružanje korisničkih usluga treba da budu prijavljeni upravnom odboru projekta i rešeni pre primene u proizvodnom okruženju.

68. Svi rezultati ispitivanja moraju biti dokumentovani i odobreni od strane relevantnih zainteresovanih strana.

69. Kao deo planiranja projekta, trebalo bi odrediti metrike kvaliteta očekivanih performansi.

70. Nezavisni entitet treba da obezbedi garanciju kvaliteta za velike projekte i ne bi trebalo da postoji sukob interesa između tog entiteta i investitora.

Član 21
Bezbedno kodiranje, pregled izvornog koda i testiranje bezbednosti aplikacija

71. FI treba da usvoji standarde o bezbednom kodiranju, pregledu izvornog koda i testiranju bezbednosti aplikacija.

72. Ovi standardi treba da obuhvate bezbedne programske prakse, validaciju ulaznih podataka, kodiranje izlaznih podataka, kontrole pristupa, autentifikaciju, kriptografske prakse i rukovanje greškama i izuzecima.

73. Trebalo bi uspostaviti politike i procedure o korišćenju softverskog koda trećih strana i softvera otvorenog koda kako bi se osigurao pregled i testiranje pre integracije u softver finansijske institucije.

74. Da bi se olakšalo blagovremeno ispravljanje ranjivosti, finansijski institucionalni ...

75. FI mora da osigura da su njegovi programeri obučeni ili da imaju neophodna znanja i veštine za implementaciju bezbednog kodiranja i standarda bezbednosti aplikacija tokom razvoja aplikacija.

76. FI treba da kreira sveobuhvatnu strategiju za sprovođenje bezbednosne validacije i testiranja aplikacije.

77. Svi softverski problemi i greške otkriveni pregledom izvornog koda i testiranjem bezbednosti aplikacije treba da budu zabeleženi i da se mogu pratiti. Veće softverske probleme i greške treba ispraviti pre implementacije.

Član 22
Upravljanje DevSecOps-om

78. Ako se usvoji DevSecOps pristup, finansijski stručnjak treba da osigura da su relevantne aktivnosti i procesi u skladu sa okvirom životnog ciklusa razvoja sistema i procesima upravljanja IT uslugama (npr. upravljanje konfiguracijom, upravljanje promenama ili upravljanje izdanjima softvera).

79. FI treba da implementira odgovarajuće bezbednosne mere i da implementira podelu dužnosti za razvoj, testiranje i objavljivanje softvera u svojim DevSecOps procesima.

Član 23
Aplikacioni programski interfejsi (API)

80. FI mora da uspostavi dovoljne mere zaštite za upravljanje razvojem i obezbeđivanjem interfejsa za programiranje aplikacija (API) za bezbedno pružanje usluga. Svi zahtevi za bezbedno kodiranje, pregled izvornog koda i testiranje bezbednosti aplikacija podjednako se primenjuju i na razvoj API-ja.

81. Pre nego što dozvoli trećim licima da se povežu sa njegovim IT sistemima putem API-ja, FI mora da sprovede procenu rizika i da osigura da su bezbednosne kontrole za svaki API u skladu sa osetljivošću i poslovnom kritičnošću podataka koji se razmenjuju, kao i zahtevima poverljivosti i integriteta ovih podataka.

82. Investicioni fondovi (IF) treba da uspostave bezbednosne standarde za dizajn i razvoj bezbednih API-ja. Standardi treba da uključuju mere za zaštitu API ključeva ili pristupnih tokena, koji se koriste za ovlašćivanje pristupa API-ju radi razmene poverljivih podataka. Treba definisati i sprovoditi razuman vremenski okvir za isteka pristupnih tokena kako bi se smanjio rizik od neovlašćenog pristupa.

83. Treba usvojiti jake standarde šifrovanja i kontrole upravljanja ključevima kako bi se obezbedio prenos osetljivih podataka putem API-ja.

84. Rigorozno bezbednosno testiranje API-ja mora se izvršiti između finansijskog stručnjaka i povezanih strana pre njegovog primene.

85. Sesije koje uključuju povezane strane mora da evidentira IF. Zapisi moraju da sadrže detalje kao što su identitet strane koja uspostavlja API vezu, datum i vreme, kao i izvršene transakcije i pristupljeni podaci. Ovi zapisi moraju biti dostupni za potrebe revizije po potrebi.

POGLAVLJE IV
UPRAVLJANJE IT USLUGAMA

Član 24
Dokumentacija

86. FI mora da održava kompletnu i ažurnu dokumentaciju o infrastrukturi, aplikacijama i sistemima, bezbednosti, operativnim faktorima i drugim važnim faktorima vezanim za IT aktivnosti.

87. Sistemi i usluge treba da budu dokumentovani na način koji omogućava zamenskom osoblju da obavlja IT operacije sa minimalnim poremećajima, što se može postići razvojem sveobuhvatnih operativnih priručnika.

88. Sva ažuriranja treba da se evidentiraju, a dokumentacija treba da se blagovremeno revidira kako bi odražavala sve promene u infrastrukturi, aplikacijama ili regulatornim zahtevima.

89. FI treba da implementira kontrole pristupa zasnovane na ulogama kako bi ograničio pristup osetljivoj dokumentaciji i osigurao da samo ovlašćeno osoblje može da pregleda ili menja dokumente.

90. Svu kritičnu dokumentaciju treba pregledati najmanje jednom godišnje ili kad god dođe do značajnih promena, i odobriti je od strane višeg rukovodstva.

Član 25
Fizičke provere

91. FI treba da preduzme neophodne zaštitne mere kako bi sprečio svaki neovlašćeni fizički pristup, ometanje ili oštećenje informacija, opreme za obradu informacija i poslovanja FI, na osnovu međunarodnih standarda i najboljih praksi. Trebalo bi sprovoditi redovne revizije kako bi se osigurao integritet i bezbednost fizičke imovine.

92. FI mora da uspostavi procedure pristupa i rada za bezbedna područja za sve zaposlene i spoljne strane. Bezbedna područja moraju biti zaštićena kontrolama pristupa kako bi se osiguralo da samo ovlašćeni zaposleni imaju pristup.

93. FI mora da vodi sveobuhvatnu dokumentaciju o politikama, procedurama i kontrolama fizičke bezbednosti i da vodi detaljne evidencije o svim bezbednosnim procenama, incidentima i aktivnostima održavanja.

94. FI mora da implementira višefaktorsku autentifikaciju (MFA) za pristup bezbednim oblastima i da vodi detaljne evidencije svih pristupa bezbednim oblastima i da ih redovno pregleda.

95. Svaki pristup trećih lica i posetilaca mora biti zabeležen i oni moraju biti u pratnji sve vreme dok se nalaze u bezbednim zonama.

96. Sva bezbedna područja treba da budu opremljena nadzornim kamerama i da obezbeđuju potpunu pokrivenost područja, osiguravajući da nijedan prostor ne ostane nepokriven.

97. Sistem nadzora mora biti u skladu sa relevantnim propisima i standardima o privatnosti, uključujući protokole za zaštitu podataka, kako bi se zaštitio snimljeni snimak.

98. FI mora da implementira sve neophodne kontrole u data centru kako bi efikasno upravljao faktorima okoline, uključujući, ali ne ograničavajući se na temperaturne ekstreme, sisteme za detekciju i suzbijanje požara.

99. FI mora da obezbedi sisteme koji osiguravaju kontinuitet napajanja, kao što su UPS (neprekidno napajanje), rezervni generatori ili slično, kako bi se osiguralo da ne dođe do prekida rada tokom nestanka struje.

Član 26
Softver kao usluga

100. Softver kao usluga (SaaS) treba da se upravlja odgovarajućim merama. FI treba da implementira šifrovanje podataka u stanju mirovanja i u prenosu kako bi zaštitio osetljive informacije i jake prakse upravljanja ključevima kako bi obezbedio ključeve za šifrovanje. FI treba da implementira formalne procese konfiguracije i dokumentacije.

101. FI treba da koristi rešenja ili procese za upravljanje identitetom i pristupom kako bi implementirao stroge kontrole pristupa, zaštitu krajnjih tačaka i bezbednosno praćenje radi zaštite od kršenja podataka i infekcija zlonamernim softverom/virusom.

102. FI treba da sprovodi redovne procene rizika specifične za upravljanje softverom i SaaS aplikacije, kako bi identifikovao ranjivosti i pretnje.

103. FI mora da vodi sveobuhvatnu dokumentaciju o svim procesima upravljanja softverom, uključujući razvoj, testiranje, implementaciju i bezbednosne mere.

Član 27
Upravljanje konfiguracijom

104. FI mora da razvije efikasan proces upravljanja konfiguracijom kako bi se osiguralo efikasno i usklađeno upravljanje IT sredstvima i uslugama, uključujući, ali ne ograničavajući se na hardver, softver i dokumentaciju;

105. FI mora da utvrdi kriterijume za identifikaciju i klasifikaciju stavki konfiguracije (CI) i da održava evidenciju registra CI;

106. Proces upravljanja konfiguracijom treba da bude integrisan sa procesima upravljanja promenama kako bi se osiguralo da se sve promene u CA evidentiraju, procenjuju i upravljaju na odgovarajući način;

107. FI mora da implementira mehanizme za praćenje i izveštavanje o statusu konfiguracionih podataka.

108. Prakse upravljanja konfiguracijom biće predmet redovnih pregleda i procena kako bi se identifikovale mogućnosti za poboljšanje;

109. FI treba da koristi standardizovane konfiguracije softvera i slike kad god je to moguće.

Član 28
Upravljanje osvežavanjem tehnologije

110. FI treba da izradi i održava Strategiju tehnološkog ažuriranja koja opisuje pristup planiranju i izvršenju tehnoloških osveženja.

111. FI treba da uspostavi procedure za procenu potrebe za tehnološkim nadogradnjama. To uključuje procenu performansi i pouzdanosti postojeće tehnologije.

112. Sav softver (uključujući operativne sisteme) i hardver (uključujući mrežnu opremu) moraju biti u okviru životnog ciklusa koji je pokriven aktivnom podrškom provajdera (uključujući i produženu podršku), ako je primenljivo.

113. Ugovori o održavanju ili licenciranju moraju biti na snazi za pristup ažuriranjima, manjim poboljšanjima i drugim kritičnim funkcijama održavanja.

114. Trebalo bi sprovesti procene rizika za hardver i softver koji se približavaju datumima isteka podrške (EOS) kako bi se procenili rizici njihovog daljeg korišćenja i trebalo bi primeniti efikasne mere za ublažavanje rizika.

115. Proces upravljanja osvežavanjem tehnologije treba redovno da se preispituje i procenjuje kako bi se identifikovale oblasti za poboljšanje i optimizovale prakse osvežavanja.

Član 29
Upravljanje zakrpama

116. FI treba da razvije i implementira sveobuhvatnu Politiku upravljanja zakrpama. Ova politika treba da definiše principe i procedure koji regulišu identifikaciju, procenu, raspoređivanje i verifikaciju zakrpa.

117. FI treba da uspostave procedure za identifikaciju relevantnih zakrpa. To uključuje kupovinu zakrpa od dobavljača i proizvođača koje rešavaju bezbednosne ranjivosti ili pružaju ažuriranja.

118. Trebalo bi sprovesti formalni proces procene kako bi se procenili uticaj, rizik i koristi zakrpa, kao i plan oporavka, pre primene. Ova procena treba da uključuje testiranje zakrpa u kontrolisanom okruženju kako bi se osigurala usklađenost.

119. Sve promene vezane za implementaciju zakrpa treba da budu dokumentovane, uključujući detalje zakrpa, akcije implementacije i sve probleme koji su se pojavili.

120. FI mora da implementira procedure za proveru da li su zakrpe pravilno primenjene i da efikasno rešava identifikovane ranjivosti ili probleme.

121. Aktivnosti upravljanja zakrpama treba integrisati sa procesima upravljanja promenama kako bi se osiguralo da su implementacije zakrpa planirane, odobrene i dokumentovane u skladu sa protokolima za upravljanje promenama.

Član 30
Upravljanje promenama

122. FI mora da uspostavi odgovarajuće politike i procedure za upravljanje promenama kako bi kontrolisao promene u IT okruženju i minimizirao poremećaje.

123. Investicioni fondovi treba da uspostave formalizovani mehanizam upravljanja promenama, kojim bi nadgledao Savetodavni odbor za promene (CAB), sastavljen od ključnih zainteresovanih strana, uključujući poslovni menadžment i IT, kako bi odobravali, pregledali i prioritizovali promene. Sve promene treba da budu pravilno testirane i odobrene, a rezultati testiranja treba da budu prihvaćeni i odobreni pre nego što se promene primene u proizvodnom okruženju.

124. Sve planirane promene treba da budu dobro dokumentovane i procenjeni rizici, a zahtevi za promene treba da budu pravilno evidentirani, kategorisani i rangirani po prioritetu. Analiza rizika treba da obuhvati faktore kao što su bezbednost i implikacije promena u odnosu na druge informacione resurse.

125. Pre implementacije promena, treba napraviti rezervnu kopiju informacionih sredstava i kreirati plan oporavka kako bi se vratio na prethodno stanje ako se pojave bilo kakvi problemi tokom ili nakon implementacije promene. Ovaj plan treba testirati kao deo životnog ciklusa projekta i implementacije.

126. FI treba jasno da definiše procedure za procenu, odobravanje i sprovođenje hitnih promena. Treba identifikovati one koji odobravaju hitne promene, a hitne promene treba pratiti i evidentirati.

127. FI treba da sprovede pregled nakon implementacije kako bi se osiguralo da promene postižu željene rezultate.

Član 31
Upravljanje incidentima

128. FI mora da implementira sveobuhvatnu Politiku upravljanja incidentima i relevantne procese i procedure za rukovanje, kategorizaciju i određivanje prioriteta IT incidenata, uključujući incidente sajber bezbednosti.

129. FI mora da razvije i redovno ažurira plan reagovanja na incidente, da formira tim za reagovanje na incidente i da ih opremi potrebnim alatima i resursima za rukovanje i upravljanje incidentima;

130. FI definiše uloge i odgovornosti osoblja i eksternih strana uključenih u evidentiranje, analiziranje, eskalaciju, odlučivanje, rešavanje i praćenje incidenata.

131. FI treba da vodi dnevnik incidenata kako bi pratio i upravljao incidentima tokom njihovog životnog ciklusa, od otkrivanja i evidentiranja do rešavanja i zatvaranja. Incidente treba kategorizovati na osnovu njihove vrste, kritičnosti i uticaja.

132. Da bi se poboljšale strategije reagovanja i osigurala usklađenost sa dogovorenim nivoima usluga, trebalo bi sprovoditi redovne preglede i procene podataka o incidentima kako bi se identifikovali trendovi u strategijama reagovanja.

133. FI mora da implementira mehanizme za prijavljivanje incidenata od strane korisnika;

134. FI mora da obezbedi dostupnost alata ili mehanizama za otkrivanje, analizu i reagovanje na incidente.

135. FI mora da obezbedi vraćanje pogođenih sistema i usluga u normalno stanje i da se uveri da su bezbedni pre nego što ih vrati u upotrebu;

136. FI mora da obezbedi efikasnu komunikaciju unutar institucije tokom i nakon incidenta, uključujući komunikaciju sa spoljnim stranama. FI mora da obezbedi da se plan komunikacije razvija i redovno preispituje.

137. FI mora obavestiti i prijaviti incident CBK-u, najkasnije 4 sata nakon njegovog otkrivanja. Početni izveštaj ili obaveštenje moraju da sadrže informacije o značajnoj pretnji, kao i o pogođenim sistemima. Privremeni izveštaj mora biti podnet u roku od 72 sata, a konačni izveštaj u roku od 30 dana. Šabloni za podnošenje izveštaja dati su u prilozima ovog dokumenta.

Član 32
Pregled nakon incidenta i naučene lekcije

138. FI mora da vodi detaljne evidencije o procesu rešavanja incidenata, uključujući preduzete mere i donete odluke.

139. FI priprema i podnosi izveštaje relevantnim zainteresovanim stranama, uključujući upravna i regulatorna tela.

140. FI treba da preispita politike i procedure za reagovanje na incidente na osnovu povratnih informacija i lekcija naučenih iz incidenata.

Član 33
Upravljanje identitetom i pristupom

141. FI treba da uspostavi odgovarajuću politiku za identifikaciju i upravljanje pristupom. Politika treba da precizira politiku lozinki, višefaktorsku autentifikaciju i kriterijume za privilegovani pristup, uključujući i treće strane. FI treba da implementira jake kontrole lozinki za pristup korisnika IT sistemima i dvofaktorsku ili višefaktorsku autentifikaciju za naloge sistemske administracije i udaljeni pristup.

142. FI treba da primenjuje principe kao što su „nikad sam“, „podela dužnosti“ i „najmanje privilegije“ prilikom odobravanja pristupa zaposlenima informacionim sredstvima.

143. Prava i privilegije pristupa sistemu treba da budu dodeljene u skladu sa ulogama i odgovornostima osoblja i trećih lica.

144. FI mora da implementira proces upravljanja korisničkim pristupom kako bi dodelio, izmenio i opozvao prava pristupa informacionim sredstvima. Prava pristupa moraju biti ovlašćena i odobrena od strane odgovarajućih strana, kao što su vlasnici informacionih sredstava.

145. FI treba da osigura da se korisnicima dodeljuju prava pristupa samo na osnovu potrebe za korišćenjem. Prava pristupa koja više nisu potrebna, kao što je promena radnih obaveza ili radnog statusa korisnika, treba odmah opozvati ili deaktivirati. Pružaoci usluga sa pristupom informacionim sredstvima FI treba da budu podložni istom praćenju i ograničenjima pristupa kao i osoblje FI.

146. Pristup privilegovanim nalozima, kao što je pristup programera radnom okruženju radi rešavanja problema, trebalo bi da se odobrava samo po potrebi i na minimalno neophodan period; aktivnosti ovih naloga trebalo bi da se beleže i pregledaju kao deo kontinuiranog praćenja finansijskog stručnjaka.

147. FI treba da sprovode periodične preglede prava pristupa korisnika najmanje svakih 6 meseci, kako bi se osiguralo da ona ostaju odgovarajuća, s ciljem identifikacije i ispravljanja svakog neovlašćenog pristupa.

148. FI mora da vodi sveobuhvatne evidencije događaja pristupa kako bi podržao praćenje, reviziju i usklađenost.

Član 34
Upravljanje mrežom

149. FI treba da kreira i dokumentuje sveobuhvatne politike bezbednosti mreže.

150. FI mora da instalira uređaje za mrežnu bezbednost, kao što su zaštitni zidovi (fajervol), kako bi obezbedio mrežu između FI i interneta, kao i veze sa trećim licima.

151. FI treba da sprovede stroge kontrole pristupa mrežnoj opremi i infrastrukturi, osiguravajući da samo ovlašćeno osoblje može da vrši izmene ili pristupa osetljivim podacima. Pravila kontrole pristupa mreži za mrežnu opremu treba da budu dokumentovana i redovno preispitivana.

152. Informativna sredstva IF treba grupisati u mrežne segmente na osnovu kritičnosti sistema, funkcionalne uloge sistema ili osetljivosti podataka.

153. Implementacija kontrole pristupa mreži kako bi se otkrilo i sprečilo povezivanje neovlašćenih uređaja na mrežu i osiguralo da su osetljivi podaci koji se prenose preko mreže šifrovani kako bi se zaštitili od prisluškivanja i neovlašćenog pristupa.

154. FI bi trebalo da razmotri izolovanje aktivnosti pregledanja interneta od svojih krajnjih uređaja korišćenjem fizičkih ili logičkih kontrola kako bi se minimizirala izloženost sajber napadima.

155. FI mora da implementira efikasno rešenje za distribuiranu zaštitu od uskraćivanja usluge (DDoS) kako bi otkrio i odgovorio na različite vrste takvih napada.

156. FI treba da sprovodi redovne procene rizika mrežne arhitekture, uključujući dizajn bezbednosti mreže, kao i periodične procene sistemskih i mrežnih međusobnih veza kako bi identifikovao potencijalne ranjivosti u oblasti sajber bezbednosti.

157. FI mora da kreira i održava planove oporavka za mrežne konfiguracije, uređaje i podatke kako bi se osigurao kontinuitet poslovanja i usklađenost.

158. FI treba da preduzme zaštitne mere i uspostavi mehanizme za zaštitu interne mreže od pretnji koje dolaze iz spoljnih izvora, kao što su sajber napadi i drugi pokušaji kršenja interne infrastrukture. Ove zaštitne mere treba da uključuju:

158.1. detaljna dokumentacija o mrežnim krajnjim uređajima; i

158.2. politike i procedure za pristup i praćenje saobraćaja.

Član 35
Upravljanje bezbednošću virtuelizacije

159. FI treba da dokumentuje i implementira bezbednosne politike posebno prilagođene tehnologijama virtuelizacije. Takve politike treba da pokrivaju bezbednost, kreiranje, distribuciju, skladištenje, pravljenje rezervnih kopija, korišćenje, preuzimanje i uništavanje virtuelnih slika.

160. FI treba da osigura da su bezbednosni standardi uspostavljeni za sve komponente rešenja za virtuelizaciju. Osigurati da samo ovlašćeno osoblje ima pristup slojevima virtuelizacije (hipervizorima) i operativnim sistemima hosta, u skladu sa principom najmanje potrebnih prava.

161. FI treba da koristi tehnike segmentacije mreže i izolacije kako bi razdvojio virtuelna okruženja.

162. FI mora da održava tačan i ažuriran inventar virtuelnih resursa i konfiguracija.

163. IF osigurava da su podaci sačuvani u virtuelnim mašinama šifrovani i da su razvijene odgovarajuće procedure za pravljenje rezervnih kopija i oporavak podataka kako bi se zaštitili od gubitka podataka i kršenja pravila.

164. FI treba da sprovode redovne revizije praksi bezbednosti virtuelizacije kako bi osigurale usklađenost sa internim politikama i regulatornim zahtevima.

Član 36
Bezbednost i privatnost podataka

165. FI treba da razvije sveobuhvatne politike sprečavanja gubitka podataka i da usvoji mere za otkrivanje i sprečavanje neovlašćenog pristupa, izmene, kopiranja ili prenosa svojih osetljivih podataka. Treba uzeti u obzir podatke u tranzitu, podatke u mirovanju i podatke u upotrebi.

166. FI mora da sprovede odgovarajuće mere za sprečavanje i otkrivanje krađe podataka, kao i neovlašćenih modifikacija sistema i krajnjih uređaja. Mehanizmi praćenja moraju biti implementirani kako bi se otkrili potencijalni incidenti gubitka podataka ili kršenja politika.

167. FI treba da uspostavi politiku klasifikacije podataka kako bi kategorizovao podatke na osnovu osetljivosti i zahteva za usklađenost i da implementira stroge kontrole pristupa kako bi se osiguralo da samo ovlašćeno osoblje može pristupiti osetljivim podacima.

168. FI mora da osigura da su osetljivi podaci šifrovani i tokom prenosa i u stanju mirovanja, i da su zaštićeni jakim kontrolama pristupa.

169. FI treba da razvije strategiju za vraćanje ključnih podataka u slučajevima kada su podaci koji se koriste i onlajn rezervne kopije ugroženi.

170. FI mora da osigura da sistemi kojima upravljaju dobavljači usluga budu u skladu sa njihovim politikama bezbednosti podataka FI i regulatornim obavezama.

171. Da bi se sprečilo curenje podataka, treba implementirati odgovarajuće kontrole u neaktivnim radnim okruženjima.

172. FI treba da ograniči upotrebu osetljivih podataka iz aktivnih radnih okruženja na neaktivna radna okruženja. Trebalo bi bar da se implementira anonimizacija ili maskiranje podataka, kada se podaci aktivnog radnog okruženja moraju koristiti u testnim okruženjima.

173. FI mora da definiše i implementira politike čuvanja podataka koje su u skladu sa regulatornim zahtevima, a podaci moraju biti trajno izbrisani sa medija za skladištenje, sistema i krajnjih uređaja, pre uništenja ili redistribucije.

Član 37
Upravljanje bezbednošću ličnih uređaja u radnom okruženju

174. FI treba da kreira jasnu i sveobuhvatnu politiku za lične uređaje u radnom okruženju (BYOD – Donesi svoj uređaj) koja definiše prihvatljivu upotrebu, bezbednosne zahteve i odgovornosti korisnika.

175. FI mora sprovesti sveobuhvatnu procenu rizika i preduzeti odgovarajuće bezbednosne mere prilikom korišćenja ličnih uređaja u radnom okruženju (BYOD).

176. FI mora da sprovede kontrole i mere kako bi sprečio gubitak podataka na personalnim računarima ili mobilnim uređajima koji se koriste za pristup informacionim sredstvima FI.

177. FI mora da koristi šifrovanje za osetljive podatke koji se čuvaju na ličnim uređajima i za podatke koji se prenose između tih uređaja i resursa institucije.

178. FI mora da obezbedi mogućnost daljinskog brisanja podataka sa ličnih uređaja u slučaju gubitka, krađe ili otpuštanja zaposlenog.

179. FI mora da implementira bezbednosne mere za uređaje koji pristupaju njenoj mreži, kao što su zaštitni zidovi (fajervol), VPN mreže (VPN) i sistemi za detekciju upada kako bi pratio i štitio od pretnji.

180. FI osigurava da se institucionalni podaci čuvaju odvojeno od ličnih podataka na uređaju, korišćenjem kontejnerizacije ili rešenja za upravljanje mobilnim uređajima.

Član 38
Bezbedno upravljanje odlaganjem

181. FI mora da obezbedi da su na snazi odgovarajuće procedure za odlaganje IT sredstava, kako sa stanovišta privatnosti podataka, tako i sa stanovišta zaštite životne sredine.

182. FI treba da sprovodi redovne procene rizika kako bi identifikovao potencijalne pretnje povezane sa uništavanjem podataka i kreirao strategije za ublažavanje.

183. FI treba da definiše prihvatljive metode odlaganja za različite vrste podataka (npr. fizičko uništenje, brisanje podataka) u fizičkom i virtuelnom okruženju kako bi se osiguralo da se podaci ne mogu rekonstruisati i treba da vodi kompletnu dokumentaciju o procesima i rezultatima uništavanja.

184. FI treba redovno da preispituje i ažurira svoje prakse upravljanja bezbednim odlaganjem, na osnovu novih pretnji, regulatornih promena i najboljih praksi.

POGLAVLJE V
OPERACIJE SAJBER BEZBEDNOSTI

Član 39
Obaveštajni podaci o sajber pretnjama i razmena informacija

185. FI treba da uspostavi proces za prikupljanje, obradu i analizu informacija vezanih za sajber bezbednost zbog njihove relevantnosti i potencijalnog uticaja na poslovno i IT okruženje. Informacije vezane za sajber bezbednost treba da uključuju sajber događaje, obaveštajne podatke o sajber pretnjama i informacije o sistemskim ranjivostima. Ovo treba da uključuje dobrovoljne i kolaborativne industrijske mreže ili nacionalne mreže za razmenu informacija, gde takve mreže postoje.

186. FI treba da razmotri implementaciju usluga praćenja sajber obaveštajnih podataka i aktivno učestvuje u sporazumima o razmeni informacija o sajber pretnjama sa pouzdanim stranama.

Član 40
Praćenje i otkrivanje sajber događaja

187. Da bi se olakšalo kontinuirano praćenje i analiza sajber događaja, kao i otkrivanje i brz odgovor na sajber incidente, finansijska institucija (FI) treba da obavlja funkcije praćenja, otkrivanja, odgovora i oporavka. U tom smislu, FI treba da razmotri osnivanje Centra za bezbednosne operacije (SOC) ili sticanje usluga upravljanja bezbednošću u skladu sa članom 3. ove uredbe. Treba definisati procese, uloge i odgovornosti za bezbednosne operacije.

188. FI treba da razmotri davanje unapred delegiranih ovlašćenja za određene hitne mere kako bi se obuzdali incidenti i ograničilo širenje. Ovo može da uključuje, ali nije ograničeno na, opremu za hitne slučajeve ili prekid usluge kada nema vremena za formiranje tima/plana za reagovanje na incident.

189. Trebalo bi uspostaviti proces za prikupljanje, obradu, pregled i čuvanje sistemskih logova kako bi se olakšale operacije praćenja bezbednosti finansijskog institucionalnog identifikatora. Trebalo bi uspostaviti osnovnu listu minimalnih zahteva za evidentiranje (npr. evidentiranje

uspešnih i neuspešnih događaja prijavljivanja, promena privilegija itd.). Ovi logovi treba da budu zaštićeni od neovlašćenog pristupa.

190. Da bi se olakšala identifikacija anomalija, finansijski inspektor treba da kreira osnovni profil rutinskih aktivnosti svakog IT sistema i da analizira sistemske aktivnosti u odnosu na osnovne profile. Profile treba redovno preispitati i ažurirati.

191. Da bi se identifikovali sumnjivi obrasci ili anomalije sistemske aktivnosti u sistemskim dnevnicima, trebalo bi izvršiti korelaciju više zabeleženih događaja.

192. Trebalo bi uspostaviti proces za neposredno eskaliranje sumnjivih ili anomalnih sistemskih aktivnosti ili ponašanja korisnika nadležnim zainteresovanim stranama.

Član 41
Reagovanje, upravljanje i izveštavanje o sajber incidentima

193. FI treba da uspostavi plan za reagovanje i upravljanje sajber incidentima kako bi se brzo izolovala i neutralisala sajber pretnja i bezbedno nastavilo pružanje pogođenih usluga. Plan treba da definiše procedure komunikacije, koordinacije i reagovanja za rešavanje potencijalnih scenarija sajber pretnji i treba da bude integrisan sa širim planovima za reagovanje i upravljanje krizama u celoj FI.

194. Kao deo plana, finansijski informator mora uspostaviti proces za istraživanje i identifikaciju nedostataka u bezbednosti ili kontroli koji su doveli do kršenja bezbednosti. Istraga takođe mora proceniti puni obim uticaja na finansijskog informatora i sve povezane treće strane.

195. Informacije iz sajber obaveštajnih podataka i lekcije naučene iz sajber incidenata trebalo bi da se koriste za poboljšanje postojećih kontrola ili poboljšanje plana za upravljanje sajber incidentima.

Član 42
Izveštavanje o incidentima

Sajber incidenti i tehnološki kvarovi moraju se prijaviti nadležnim regulatornim organima, prema 0-Upravljanje incidentima ove Uredbe.

POGLAVLJE VI
ODGOVOR I OPORAVAK

Član 43
Dostupnost sistema

IKT sistemi treba da budu projektovani i implementirani tako da se postigne nivo dostupnosti sistema koji je u skladu sa njegovim poslovnim potrebama. Prihvatljivi nivoi usluge ili dostupnosti sistema treba da budu definisani za svaku poslovnu funkciju i zabeleženi u internim ili eksternim ugovorima o nivou usluge.

Član 44
Upravljanje kontinuitetom poslovanja i oporavak od katastrofe

196. FI treba da uspostavi dobar proces upravljanja kontinuitetom poslovanja kako bi maksimizirali svoju sposobnost kontinuiranog pružanja usluga, postigli svoje ciljeve dostupnosti navedene u ugovorima o nivou usluge i minimizirali gubitke u slučaju ozbiljnih poremećaja u poslovanju.

197. Kao deo dobrog upravljanja kontinuitetom poslovanja, finansijske institucije treba da sprovedu analizu uticaja na poslovanje (BIA) analizirajući svoju izloženost i uticaj poremećaja u poslovanju. Treba razmotriti niz scenarija, uključujući i one najteže, ali verovatne.

198. Analiza uticaja na poslovanje treba takođe da uzme u obzir važnost identifikovanih i klasifikovanih poslovnih funkcija, pratećih procesa, trećih strana i informacionih sredstava, kao i njihovu međuzavisnost.

199. FI treba da odredi ciljeve vremena oporavka sistema i ciljeve tačaka oporavka koji su u skladu sa rezultatima analize uticaja na poslovanje.

200. FI treba da obezbede da su karakteristike dostupnosti IKT sistema u skladu sa rezultatima analize uticaja na poslovanje. Na primer, za neke kritične komponente može se implementirati redundantnost kako bi se sprečili prekidi izazvani događajima koji utiču na te komponente.

201. Na osnovu analize uticaja na poslovanje koju sprovodi finansijska institucija, finansijske institucije treba da razviju planove za obezbeđivanje kontinuiteta poslovanja i oporavka od katastrofe. Ovi planovi, koje treba da dokumentuju i odobre njihova upravljačka tela, treba posebno da uzmu u obzir rizike koji bi mogli uticati na IKT sisteme i usluge. FI treba da se koordinišu sa relevantnim internim i eksternim zainteresovanim stranama, prema potrebi, prilikom razvoja ovih planova.

202. Zaposleni treba da budu obučeni za korišćenje planova, a planove treba preispitati, ažurirati i testirati najmanje jednom godišnje ili nakon značajnih promena IKT sistema ili poslovnih procesa.

Član 45
Test plana za oporavak od katastrofe

203. Relevantne zainteresovane strane, uključujući one u poslovnim i IKT funkcijama, trebalo bi da učestvuju u testovima kontinuiteta poslovanja i oporavka od katastrofe kako bi se upoznale sa procesima oporavka i utvrdile da li sistemi funkcionišu kako se očekuje.

204. Test kontinuiteta poslovanja/oporavka od katastrofe treba da se zasniva na planu testiranja koji uključuje ciljeve i obim, scenarije testiranja, sa detaljima o aktivnostima koje treba obaviti tokom i nakon testiranja i kriterijume za merenje uspeha testiranja.

205. Testiranje treba da obuhvati različite potencijalne scenarije prekida rada, uključujući potpune i delimične prekide rada primarnog data centra i veće kvarove sistema. Takođe treba da se bavi zavisnostima oporavka između različitih informacionih sredstava, uključujući i ona kojima upravljaju treće strane.

206. Tamo gde informacionim sredstvima upravljaju dobavljači usluga, finansijski stručnjak treba da proceni njihove mogućnosti oporavka od katastrofe i da osigura da su aranžmani za oporavak od katastrofe za ta informaciona sredstva uspostavljeni, testirani i verifikovani kako bi zadovoljili poslovne potrebe finansijskog stručnjaka. finansijski stručnjak treba da angažuje svog dobavljača usluga da testira korake oporavka koji zahtevaju koordinisane akcije.

Član 46
Rezervna kopija i oporavak

207. FI treba da uspostavi politike i procedure za redovne rezervne kopije koje omogućavaju oporavak u slučaju prekida rada sistema, oštećenja ili brisanja podataka. Arhiviranje podataka za dugoročno skladištenje treba da bude uključeno u politike i procedure.

208. Da bi se osiguralo da je dostupnost podataka u skladu sa poslovnim zahtevima finansijske institucije, finansijska institucija treba da uspostavi politiku za upravljanje životnim ciklusom rezervnih kopija podataka. Ovo treba da uključuje učestalost pravljenja rezervnih kopija podataka, period čuvanja podataka, broj onlajn i oflajn rezervnih kopija, upravljanje mehanizmima za skladištenje podataka i bezbedno uništavanje medija za rezervne kopije na kraju njihovog životnog ciklusa.

209. Da bi se rešili rizici od ransomware-a, finansijski inspektor bi trebalo da razmotri kreiranje rezervnih kopija sa zaštićenim prostorom ili nepromenljivih rezervnih kopija.

210. FI treba periodično da testira oporavak sistema i rezervne kopije podataka kako bi proverio efikasnost procedura oporavka. Za kritične sisteme, testove oporavka treba sprovoditi najmanje svakih šest meseci, dok za nekritične sisteme, testove treba sprovoditi najmanje jednom godišnje.

211. Da bi zaštitio rezervne kopije od neovlašćenog pristupa i modifikacija, finansijski inspektor mora da osigura da su svi poverljivi podaci sačuvani na medijumu za rezervne kopije bezbedni (npr. šifrovani).

212. Rezervne kopije podataka o klijentima i drugih podataka kritičnih za rad finansijskog institucionalnog identifikatora treba da budu redundantne (npr. najmanje dve ekvivalentne kopije) i da se čuvaju na odvojenim, bezbednim lokacijama koje verovatno neće biti pogođene istom katastrofom.

Član 47
Centar podataka

213. FI treba da sprovede Procenu rizika od pretnji i ranjivosti (TVRA) za svoje centre podataka (DC) kako bi identifikovao potencijalne ranjivosti, slabosti i zaštitne mere koje treba uspostaviti radi zaštite centara podataka (DC) od fizičkih i ekoloških pretnji. Pored toga, procena treba da uzme u obzir političku i ekonomsku klimu zemlje u kojoj se centri podataka nalaze. Procena rizika od pretnji i ranjivosti treba da se preispita kad god dođe do značajne promene u okruženju pretnji ili kada dođe do materijalne promene u okruženju centra podataka.

214. FI treba da obezbedi dovoljnu redundantnost za napajanje, mrežnu povezanost, hlađenje i druge električne i mehaničke sisteme unutar sistema za upravljanje električnim resursima kako bi se eliminisao rizik od kvara na jednom mestu. Pažnju treba obratiti na sledeće:

214.1. diverzifikacija komunikacije podataka, mrežnih puteva i dobavljača;

214.2. raspoređivanje energetske opreme, kao što su UPS i rezervni generatori, i

214.3. implementacija odgovarajuće redundantne opreme za hlađenje (npr. rashladni tornjevi, dovod hladne vode i klima uređaji u računarskoj sali) radi kontrole nivoa temperature i vlažnosti u data centru i sprečavanja potencijalno štetnih fluktuacija za sisteme.

215. Kao deo kontrole životne sredine u data centru, finansijski inspektor treba da implementira uređaje ili sisteme za detekciju i suzbijanje požara, kao što su detektori dima ili toplote, sistemi za gašenje inertnim gasom i sistemi za prskanje vlažnom ili suvom vodom.

216. Sekundarni centar podataka ili centar za oporavak od katastrofe finansijskog stručnjaka treba da bude geografski odvojen od svog primarnog ili operativnog centra. Ovo će osigurati da poremećaji u osnovnoj infrastrukturi (npr. telekomunikacije i napajanje) i/ili ekološke opasnosti na datoj lokaciji ne utiču na obe lokacije istovremeno.

217. Fizičke i ekološke bezbednosne kontrole DC-a moraju se pratiti 24/7.

218. Planovi i procedure reagovanja na fizičke i ekološke incidente u CD treba da budu definisani i testirani za određeni nivo eskalacije.

219. Domen podataka treba da ima odgovarajuće kontrole fizičkog pristupa. Najbolje prakse uključuju:

219.1. odobravanje pristupa zaposlenima na osnovu potrebe da znaju, odmah opozivajući pristup kada više nije potreban;

219.2. implementacija odgovarajućih protokola za obaveštavanje i odobravanje posetilaca data centra. Sve posetioce mora pratiti ovlašćeno osoblje sve vreme dok se nalaze u data centru;

219.3. obezbeđivanje i praćenje fizičkih pristupnih tačaka centru podataka u svakom trenutku;

219.4. ograničavanje i praćenje pristupa regalima za opremu;

219.5. osiguravanje da osoblje sa fizičkim pristupom policama za opremu nema i pristup informacionim sistemima;

219.6. ograničavanje pristupa ključevima i drugim fizičkim uređajima samo na ovlašćeno osoblje, njihova brza zamena ili promena ukoliko se zagube, izgube ili ukradu, i

219.7. odvajanje zajedničkih prostorija od osetljivih bezbednosnih područja.

POGLAVLJE VII
SKENIRANJE, TESTIRANJE, VEŽBE I PREKID

Član 48
Skeniranje ranjivosti

FI treba da uspostavi proces za redovno skeniranje ranjivosti kako bi identifikovao bezbednosne ranjivosti i blagovremeno rešio rizike povezane sa njima. Učestalost skeniranja treba da bude u skladu sa kritičnošću IT sistema i bezbednosnim rizikom kojem su izloženi.

Član 49
Test penetracije

220. FI treba da sprovede test penetracije kako bi stekao dubinsko razumevanje svoje sajber bezbednosne zaštite.

221. Spoljne digitalne usluge finansijskog stručnjaka moraju biti podložne testovima penetracije u redovnim intervalima. Za finansijske stručnjake kategorisane prema članu 3 stav 1, testovi penetracije moraju se sprovoditi najmanje jednom godišnje i nakon svake veće izmene osnovnih sistema. Za sve ostale finansijske stručnjake, testovi penetracije moraju se sprovoditi najmanje svake dve godine i nakon svake veće izmene sistema.

222. Testiranje moraju sprovoditi osobe sa dovoljnim znanjem i stručnošću, kao i one koje su kompetentne za obavljanje takvih aktivnosti.

Član 50
Vežbe za reagovanje na incidente

223. FI treba da sprovodi redovne sajber vežbe kako bi validirao procedure za reagovanje na sajber incidente i oporavak, uključujući planove komunikacije. Ove vežbe mogu da uključuju vežbu na terenu i simulacije napada. Pored toga, mogu se kombinovati sa testiranjem prodora i testiranjem BCP/DRP (planiranje kontinuiteta poslovanja/planiranje oporavka od katastrofe).

223.1. Za potrebe ovog članka, veliki sajber napad bi mogao biti scenario prekida rada u testu planiranja oporavka od katastrofe.

224. U zavisnosti od ciljeva vežbe, FI treba da uključi relevantne zainteresovane strane, uključujući viši menadžment, poslovne jedinice, stručnjake za korporativne komunikacije, timove za upravljanje krizama, pružaoce usluga i tehničko osoblje zaduženo za otkrivanje, reagovanje na i oporavak od sajber pretnji.

Član 51
Upravljanje korektivnim merama

225. Fizički institucije treba da uspostave sveobuhvatan proces korektivnih mera za praćenje i rešavanje problema identifikovanih putem skeniranja ranjivosti, testova penetracije i sajber vežbi. Proces treba da obuhvati, najmanje, sledeće:

225.1. procena kritičnosti i klasifikacija problema (uključujući označavanje i verifikaciju lažno pozitivnih rezultata);

225.2. vremenski okvir za rešavanje problema različitog značaja, i

225.3. procena rizika i strategije ublažavanja za upravljanje odstupanjima od okvira.

POGLAVLJE VIII
NEZAVISNA GARANCIJA

Član 52
Revizija

226. Na reviziju informacionog sistema primenjuju se zahtevi utvrđeni Uredbom o internim kontrolama i internoj reviziji finansijskih institucija.

227. Funkcija interne revizije treba da sprovodi interne revizije IT sistema, kontrola sajber bezbednosti, upravljanja, usklađenosti i procesa autsorsinga od strane revizora sa dovoljnim znanjem, veštinama i kompetencijama u oblasti IT i bezbednosnih rizika, kako bi se odboru i višem menadžmentu pružila nezavisna uveravanja o njihovoj efikasnosti. Revizori treba da budu nezavisni unutar ili izvan finansijske institucije, a učestalost i fokus takvih revizija treba da budu u skladu sa relevantnim IT i bezbednosnim rizicima.

228. Upravni odbor finansijske institucije treba da odobri godišnji plan revizije, uključujući sve IT revizije i sve njihove materijalne izmene. Plan revizije i njegovo izvršenje, uključujući učestalost revizije, treba da odražavaju i budu srazmerni inherentnim IT i bezbednosnim rizicima finansijske institucije i treba da se ažuriraju. Obim i učestalost revizija treba da budu u skladu sa kritičnošću i profilom rizika informacionih sredstava, funkcija i procesa.

229. Trebalo bi uspostaviti formalni proces praćenja, uključujući odredbe za blagovremenu verifikaciju i ispravljanje kritičnih nalaza IT revizije.

230. Zapažanja visokog rizika i preduzete korektivne mere treba bez nepotrebnog odlaganja prijaviti Upravnom odboru.

231. Kao minimum, FI treba da zaposli osoblje interne revizije sa kompetencijama i veštinama za razvoj godišnjeg plana revizije tehnološkog rizika i za razumevanje nalaza, rizika i preporuka specijalizovanih spoljnih dobavljača.

232. Aktivnosti u oblasti IT-a trebalo bi da budu predmet najmanje jednom godišnjeg periodičnog pregleda koji se fokusira na metodologiju zasnovanu na riziku.

233. FI treba da osigura da njegovi revizori tehnološkog rizika imaju potreban nivo kompetencija i veština da efikasno procene adekvatnost implementiranih IT politika, procedura, procesa i kontrola.

POGLAVLJE IX
UPRAVLJANJE DOBAVLJAČIMA AUTSORSINGA TEHNOLOŠKIH USLUGA

Član 53
Proporcionalnost

Prilikom sprovođenja zahteva utvrđenih ov0m uredbom, finansijske institucije treba da uzmu u obzir složenost autsorsovanih funkcija, rizike koji proizilaze iz aranžmana o autsorsingu, kritičnost autsorsovanih funkcija i potencijalni uticaj autsorsinga na kontinuitet njihovih aktivnosti.

Član 54
Upravljanje

234. Delegiranje funkcija ili korišćenje dobavljača tehnoloških usluga (TSP) ne oslobađa odbor njegovih odgovornosti. FI ostaju odgovorni i u potpunosti odgovorni za ispunjavanje svih svojih regulatornih obaveza, uključujući i mogućnost nadgledanja autsorsinga kritičnih ili važnih funkcija.

235. FI mora da osigura da pružaoci tehnoloških usluga (TSP), uključujući i one koji se bave autsorsingom, ne dovode do povećanog tehnološkog i sajber rizika.

236. Za pravilno upravljanje delegiranjem funkcija ili korišćenjem dobavljača tehnoloških usluga, finansijski stručnjak mora:

236.1. jasno raspodeliti odgovornosti za dokumentaciju, upravljanje i kontrolu ugovora o autsorsingu;

236.2. izdvojiti dovoljno resursa kako bi se osigurala usklađenost sa svim zakonskim i regulatornim zahtevima, uključujući smernice i dokumentaciju i praćenje svih spoljnih sporazuma;

236.3. uspostaviti funkciju autsorsinga ili odrediti starijeg člana osoblja koji izveštava odbor (npr. nosioca ključne funkcije) i koji je odgovoran za upravljanje i nadgledanje rizika aranžmana autsorsinga kao dela okvira interne kontrole institucije i nadgledanje dokumentacije aranžmana autsorsinga.

237. Prilikom autsorsinga, finansijski stručnjak mora da obezbedi najmanje sledeće:

237.1. odobravanje i sprovođenje odluka koje se odnose na njegove poslovne aktivnosti i kritične ili važne funkcije;

237.2. održavanje urednog razvoja svog poslovanja i pružanje finansijskih usluga;

237.3. identifikacija, procena, upravljanje i adekvatno ublažavanje rizika koji proizilaze iz autsorsinga;

237.4. gde je to primenljivo, odgovarajuće aranžmane za poverljivost podataka i drugih informacija;

237.5. održavanje odgovarajućeg toka relevantnih informacija sa dobavljačima usluga;

238. U slučaju neplaniranog prekida ugovorenih usluga, kritičnih ili važnih funkcija, institucija je dužna da preduzme najmanje jednu od sledećih mera, u odgovarajućem vremenskom roku:

238.1. prenos funkcije na alternativne pružaoce usluga;

238.2. reintegracija funkcije u instituciju; ili

238.3. prestanak poslovnih aktivnosti koje zavise od funkcije; i

238.4. Kada lične podatke obrađuju pružaoci usluga koji se nalaze u trećim zemljama, podaci se obrađuju u skladu sa Zakonom o zaštiti ličnih podataka.

Član 55
Procena rizika

239. FI mora da utvrdi da li delegiranje obavljanja procesa, usluga ili aktivnosti od strane institucije pružaocu usluga spada pod definiciju autsorsinga.

240. Za potrebe ove uredbe, sledeće odluke se neće smatrati autsorsingom:

240.1. globalne finansijske komunikacione usluge (npr. SWIFT) ako se glavni resursi informacionog sistema neophodni za pružanje takve usluge nalaze unutar institucije;

240.2. funkcija koju je zakonski obavezan da obavlja pružalac usluga (npr. zakonska revizija);

240.3. usluge tržišnih informacija (npr. pružanje podataka od Bloomberg, Moody&, Standard & Poor & Fitch);

240.4. globalne mrežne infrastrukture (npr. Visa, MasterCard) i telekomunikacione usluge;

240.5. sporazumi o kliringu i poravnanju između klirinških kuća, centralnih kontragenta i institucija za poravnanje i njihovih članova;

240.6. globalne infrastrukture za razmenu finansijskih poruka koje podležu nadzoru nadležnih organa;

240.7. korespondentske bankarske usluge;

240.8. kupovina usluga koje institucija inače ne bi obavljala (npr. saveti arhitekte, pružanje pravnog mišljenja i zastupanje pred sudom i upravnim organima, čišćenje, baštovanstvo i održavanje prostorija institucije, medicinske usluge, servisiranje službenih automobila, ugostiteljstvo, usluge automata za prodaju, administrativne usluge, turističke usluge, usluge pošte, usluge recepcionara, sekretara i operatera telefonskih centrala), robe (npr. plastične kartice, čitači kartica, kancelarijski materijal, personalni računari, nameštaj) ili usluga (npr. struja, gas, voda, telefonske linije);

240.9. softver koji je, budući da je gotov, komercijalno dostupan na tržištu i ne zahteva značajnu adaptaciju; i

240.10. druge usluge slične onima navedenim u podtačkama 2.1 do 2.9 ovog stava, pod uslovom da CBK da prethodno mišljenje da se odredbe ove uredbe ne primenjuju na korišćenje ovih usluga.

241. FI treba da proceni potencijalni operativni rizik korišćenja usluga pružaoca tehnoloških usluga (TSP) i sklapanja ugovornog aranžmana. FI treba da uzme u obzir rezultate procene kako bi usmerio odluke o autsorsingu usluga i preduzeo odgovarajuće korake kako bi izbegao dodatne operativne rizike pre sklapanja ugovornog aranžmana.

242. FI treba uvek da smatra funkciju kritičnom ili važnom u sledećim situacijama:

242.1. kada bi nedostatak ili neuspeh u njegovom obavljanju značajno naštetio finansijskom učinku i kontinuitetu aktivnosti institucije.

242.2. Kada se operativni zadaci funkcija interne kontrole prepuštaju spoljnim izvršnim saradnicima, treba sprovesti procenu kako bi se utvrdilo da li bi neuspeh u pružanju

ugovorene funkcije ili njeno neadekvatno pružanje negativno uticalo na efikasnost funkcije interne kontrole.

243. Da bi se upravljalo rizikom autsorsinga, neophodno je utvrditi kritičnost ili važnost funkcije koja se autsorsuje.

244. FI treba da definiše kriterijume i definiše metodologiju za procenu kritičnosti ili važnosti funkcije, uključujući njen uticaj na usklađenost sa propisima i licenciranje, uticaj na finansijske performanse, doprinos operativnoj održivosti i kontinuitetu usluga, značaj u održavanju poverenja klijenata i kvaliteta usluga, potencijalni uticaj na reputaciju ili poziciju institucije na tržištu i stepen zavisnosti od osnovnih poslovnih operacija.

245. Procena važnosti ili kritičnosti je kontinuirani proces koji treba sprovoditi u redovnim intervalima. Redovno preispitujte procenu kritičnosti ili važnosti kako biste osigurali da ona ostane relevantna kako se poslovni uslovi, propisi i operacije menjaju tokom vremena.

246. Procena kritičnih ili važnih funkcija podrazumeva strukturirani pristup za određivanje važnosti svake funkcije za poslovanje institucije i regulatorne obaveze. Ova procena je neophodna za donošenje informisanih odluka u vezi sa autsorsingom i osiguravanje da aranžmani o autsorsingu ne ugrožavaju operativnu održivost ili usklađenost sa propisima.

Član 56
Ugovorni odnos između finansijskog stručnjaka i pružaoca usluga

247. Prilikom zaključivanja ugovora sa pružaocem usluga, finansijski stručnjak treba da osigura da su obim i sadržaj ugovornih odredbi prikladni rizicima povezanim sa autsorsingom i obimu i složenosti autsorsovanih funkcija.

248. Institucije moraju da zaključe pisani ugovor sa pružaocem usluga, koji mora da sadrži najmanje sledeće:

248.1. detaljan opis ugovorene funkcije koja je predmet sporazuma;

248.2. datum početka i datum završetka ispunjenja ugovornih obaveza;

248.3. finansijske obaveze stranaka;

248.4. odredbe koje regulišu način na koji institucija kontinuirano prati obavljanje funkcije koja je predmet sporazuma, uključujući vrste izveštaja koje institucija mora da primi od pružaoca usluga i učestalost njihovog podnošenja;

248.5. obaveza pružaoca usluga da blagovremeno obavesti instituciju o svim činjenicama i promenama okolnosti koje imaju ili mogu imati značajan uticaj na ispunjenje ugovornih obaveza;

248.6. dogovoreni nivo usluge i kvalitet obavljenih funkcija, uključujući kvalitativne i, gde je primenljivo, kvantitativne ciljeve učinka za ugovorenu funkciju, koji omogućavaju instituciji da blagovremeno preduzme korektivne mere;

248.7. kada je to prikladno, obaveza poslovne tajne i obaveza i način zaštite poverljivih i ličnih podataka, uključujući odredbe o pristupu, dostupnosti, integritetu, privatnosti i bezbednosti relevantnih podataka;

248.8. kada je potrebno, lokacija(e) gde će se pružati ugovorena funkcija i gde će se čuvati, obrađivati i skladištiti relevantni podaci, uključujući zahtev da se institucija obavesti ako pružalac usluga predloži promenu lokacije(a);

248.9. odredbe o tome da li je dozvoljeno podizvođačko izvođenje funkcije;

248.10. obaveza pružaoca usluga da pruža usluge na način koji je u potpunosti u skladu sa relevantnim zakonodavstvom Republike Kosovo;

248.11. obaveza pružaoca usluga da obezbedi CBK pristup i prava na kontrolu na licu mesta, na način naveden u članu 5. stav 2. ove uredbe;

248.12. odredbe kojima se osigurava da se podacima u vlasništvu institucije može pristupiti u slučaju raspuštanja ili prestanka poslovanja pružaoca usluga (npr. stečaj, rešavanje problema, likvidacija ili slični postupci);

248.13. odredbe o tome da li pružalac usluga mora da pribavi polisu osiguranja od profesionalne odgovornosti i, ako je primenljivo, nivo potrebnog osiguranja;

248.14. obaveza pružaoca usluga da sarađuje sa CBK kao nadležnim organima i organima za restrukturiranje institucije;

248.15. trajanje ugovornog odnosa ili naznaka da je ugovor na neodređeno vreme;

248.16. opis uslova za raskid i/ili otkazivanje ugovora sa otkaznim rokovima utvrđenim za instituciju i pružaoca usluga;

248.17. prava institucije da raskine ili otkaže ugovor sa pružaocem usluga, ako ga ima, po nalogu CBK;

248.18. izbor merodavnog prava; i

248.19. metod rešavanja sporova.

249. Kada finansijski stručnjak i pružalac usluga zaključe ugovor o autsorsingu kritičnih ili važnih funkcija, ugovor, pored sadržaja navedenog u stavu 2. ovog člana, mora da sadrži i sledeće:

249.1. obaveza pružaoca usluga da obezbedi pristup i prava revizije instituciji na način utvrđen članom 57. stav 2. ove uredbe;

249.2. odredbe o sprovođenju i testiranju planova za vanredne situacije u poslovanju;

249.3. obaveze pružaoca usluga u slučaju prenosa delegirane funkcije na drugog pružaoca usluga ili nazad instituciji, uključujući obaveze u vezi sa obradom podataka;

249.4. definisanje odgovarajućeg prelaznog perioda tokom kojeg će pružalac usluga, nakon prestanka ili otkazivanja ugovora o autsorsingu, nastaviti da pruža ugovorenu funkciju kako bi se ublažio rizik od prekida; i

249.5. obaveza pružaoca usluga da podrži instituciju u urednom prenosu ili reintegraciji funkcije u slučaju otkazivanja ili raskida ugovora

250. Ugovor treba da precizira da li je dozvoljeno podizvođačko obavljanje kritičnih ili važnih funkcija, ili njihovih bitnih delova.

251. Ako je dozvoljeno podizvođačko ugovaranje kritičnih ili važnih funkcija, institucije moraju utvrditi da li je deo funkcije koji se podizvođački ugovara, kao takav, kritičan ili važan (tj. materijalni deo kritične ili važne funkcije) i, ako jeste, evidentirati ga u registru.

252. Kada ugovor o autsorsingu kritičnih ili važnih funkcija uključuje mogućnost podizvođačkog ugovaranja, pored sadržaja navedenog u stavovima 2 i 3 ovog člana, taj ugovor mora da sadrži najmanje sledeće:

252.1. obaveza pružaoca usluga da obavesti instituciju o svakom planiranom podizvođačkom ugovaranju ili bitnim izmenama istog, u roku koji bi instituciji omogućio da sprovede procenu rizika predloženih izmena i, gde je to potrebno, da blagovremeno uloži prigovor na planirano podizvođačko ugovaranje ili bitne izmene istog;

252.2. Pravo na raskid/prekid ugovora kada podizvođačko ugovaranje povećava rizike za instituciju ili kada pružalac usluga podizvođački ugovara bez obaveštavanja institucije i u drugim opravdanim slučajevima;

252.3. kada podizvođaštvo podrazumeva obradu ličnih podataka, obaveza pružaoca usluga da dobije pismeno ovlašćenje od institucije;

252.4. obaveza pružaoca usluga da nadgleda one usluge koje je podizvođaču poverio;

252.5. uslovi koji moraju biti ispunjeni u slučaju podizvođačkog ugovaranja;

252.6. vrste funkcija koje se ne mogu prepustiti podizvođačima;

252.7. obaveza pružaoca usluga da zatraži pismeno odobrenje od institucije za svako planirano podugovaranje ili bitne izmene istog, ili pravo na prigovor na planirano ugovaranje; i

252.8. obaveza pružaoca usluga da pregovara sa podizvođačem o pravima pristupa i revizije ili ispitivanja na licu mesta na način utvrđen u članu 57. stav 1. ove uredbe.

253. FI može dozvoliti podizvođačko ugovaranje samo kada se podizvođač obaveže da će postupati u skladu sa važećim zakonom i regulatornim zahtevima, da će ispuniti relevantne ugovorne obaveze i da će instituciji i CBK obezbediti ista prava pristupa i revizije ili ispitivanja na licu mesta kao ona koja je dodelio pružalac usluga u skladu sa članom 57. ove uredbe.

254. FI će osigurati da pružalac usluga adekvatno nadgleda podizvođače usluga, u skladu sa politikom koju je utvrdila institucija. Ako bi predloženo podizvođačko ugovaranje moglo imati značajne negativne efekte na aranžman o podizvođačkom ugovaranju kritične ili važne funkcije ili bi dovelo do značajnog povećanja rizika, uključujući i slučajeve kada uslovi iz stava 7. ovog člana ne bi bili ispunjeni, institucija će iskoristiti svoje pravo da se usprotivi podizvođačkom ugovaranju, ako je takvo pravo dogovoreno, i/ili da raskine ugovor.

Član 57
Prava pristupa i revizija ili ispitivanje na licu mesta

255. FI mora da obezbedi, u okviru ugovora o autsorsingu sa pružaocem usluga, da pružalac usluga pruži Centralnoj banki (CBK) ili bilo kojoj osobi koju je CBK imenovala u tu svrhu, sledeće:

255.1. Blagovremen i potpun pristup poslovnim prostorijama, uključujući opremu, sisteme, mreže, informacije i podatke koji se koriste za obavljanje ugovorene funkcije, uključujući relevantne finansijske informacije, osoblje i eksterne revizore pružaoca usluga; i

255.2. Sprovođenje ispitivanja na licu mesta dela aktivnosti pružaoca usluga koji jeste ili može biti povezan sa autsorsingom, kao i ispitivanja na licu mesta obavljanja funkcija koje su predmet ugovora sa pružaocem usluga, kako bi mu se omogućilo praćenje ugovorenog ugovora i osigurala usklađenost sa svim važećim regulatornim i ugovornim zahtevima.

256. Što se tiče autsorsinga kritičnih ili važnih funkcija, institucije moraju da obezbede, u okviru ugovora o autsorsingu kritičnih ili važnih funkcija sa pružaocem usluga, da pružalac usluga obezbedi instituciji, njenim eksternim revizorima i drugim licima koje imenova u tu svrhu i CBK kao organima za rešavanje/zatvaranje institucija određenih u skladu sa zakonskim propisima koji regulišu ovu oblast, sledeće:

256.1. blagovremen i potpun pristup poslovnim prostorijama, uključujući opremu, sisteme, mreže, informacije i podatke koji se koriste za obavljanje funkcije autsorsinga, uključujući relevantne finansijske informacije, osoblje i eksterne revizore pružaoca usluga; i

256.2. sprovođenje revizija ili pregleda dela poslovanja pružaoca usluga koji jeste ili može biti povezan sa autsorsingom, kao i pregleda obavljanja autsorsovanih funkcija koje su predmet sporazuma sa pružaocem usluga, kako bi im se omogućilo da prate ugovorni sporazum i da osiguraju usklađenost sa svim važećim regulatornim i ugovornim zahtevima.

257. FI treba da osigura, u okviru ugovornog sporazuma sa pružaocem usluga, da njegova funkcija interne revizije bude u mogućnosti da pregleda ugovorenu funkciju, koristeći pristup zasnovan na riziku.

258. Institucije treba da ostvare svoja prava pristupa i revizije navedena u ovom članu i da odrede učestalost revizija i oblasti koje će biti revidirane, koristeći pristup zasnovan na riziku.

259. Radi sprovođenja revizija i pregleda iz stava 2, podtačke 2.2, ovog člana, institucija može koristiti:

259.1. zajedničke revizije organizovane, zajedno sa drugim klijentima istog pružaoca usluga, a sprovedene od strane institucije i tih klijenata ili od strane treće strane koju su oni imenovali; i

259.2. sertifikati treće strane i izveštaji treće strane ili interne revizije koje je stavio na raspolaganje pružalac usluga.

260. Za autsorsing kritičnih ili važnih funkcija, institucija će proceniti da li su sertifikati i izveštaji treće strane, kako je navedeno u stavu 5, podstavu 5.2, ovog člana, prikladni i dovoljni za sprovođenje odgovarajućih revizija i pregleda aranžmana o autsorsingu i neće se oslanjati isključivo na ove izveštaje tokom vremena.

261. Kada ugovorni sporazum nosi visok nivo tehničke složenosti, na primer u slučaju ugovaranja usluga u „Oblaku“, institucija treba da proveri:

261.1. da li lica navedena u stavu 5. ovog člana koja sprovode reviziju i/ili procenu imaju odgovarajuće i relevantne veštine i znanja za efikasno sprovođenje relevantnih revizija i/ili procena; i

261.2. da li osoblje institucije koje pregleda sertifikate i/ili izveštaje lica navedenih u stavu 5. ovog člana poseduje odgovarajuće i relevantne veštine i znanje za efikasno sprovođenje relevantnih revizija i/ili pregleda.

Član 58
Nadzor nad autsorsovanim funkcijama

262. FI treba kontinuirano da prati učinke pružalaca usluga u vezi sa svim aranžmanima o autsorsingu na osnovu pristupa zasnovanog na riziku i sa prvenstvenim fokusom na autsorsing kritičnih ili važnih funkcija, uključujući obezbeđivanje dostupnosti, integriteta i bezbednosti podataka i informacija. Tamo gde se rizik, priroda ili obim autsorsovane funkcije značajno promenio, institucije treba da ponovo procene kritičnost ili značaj te funkcije u skladu sa članom 6. ove uredbe.

263. FI mora pokazati veštine i dužnu pažnju prilikom praćenja i upravljanja ugovorenim sporazumima.

264. FI treba redovno da ažurira procenu rizika i periodično izveštava upravljačko telo o rizicima identifikovanim u vezi sa autsorsingom kritičnih ili važnih funkcija.

265. FI treba da kontinuirano obezbede da ugovorni aranžmani, sa prvenstvenim fokusom na prepuštanje kritičnih ili važnih funkcija spoljnim ugovorima, ispunjavaju odgovarajuće standarde učinka i kvaliteta u skladu sa njihovim politikama, tako što će:

265.1. osigurati da dobijaju odgovarajuće izveštaje od pružalaca usluga;

265.2. proceniti učinke pružalaca usluga, koristeći alate kao što su ključni indikatori učinka, ključni indikatori kontrole, izveštaji o pružanju usluga, samosertifikacija i nezavisni pregledi; i

265.3. pregledati sve ostale relevantne informacije primljene od pružaoca usluga, uključujući izveštaje o merama za kontinuitet poslovanja i testiranju.

266. FI treba da preduzme odgovarajuće mere ako identifikuju nedostatke u pružanju ugovorene funkcije. Posebno, institucije treba da prate sve indikatore da pružaoci usluga možda ne obavljaju ugovorenu kritičnu ili važnu funkciju efikasno ili u skladu sa važećim zakonima i regulatornim zahtevima. Ako se identifikuju nedostaci, finansijske institucije treba da preduzmu odgovarajuće korektivne ili sanacione mere. Takve mere mogu uključivati raskid ugovora, sa trenutnim dejstvom, ako je potrebno.

Član 59
Kompetentnost dobavljača

FI treba da zaključuje ugovore samo sa dobavljačima koji pokažu visoku kompetentnost i kvalifikovano osoblje za delegirane funkcije i efikasno upravljanje tehnološkim rizicima (TRM).

Član 60
Klaud računarstvo

267. CBK treba da bude obaveštena o planovima za sklapanje ugovora sa dobavljačima usluga u oblaku (CSP) za pružanje ili materijalnu podršku kritičnim uslugama, uz dovoljno obaveštenja (jedan mesec) pre angažmana, kako bi supervizor mogao da sprovede procenu rizika i izrazi eventualne zabrinutosti.

268. Korišćenje usluga zasnovanih na oblaku za kritične usluge/funkcije mora da odobri odbor, a registar svih usluga u oblaku koje finansijski stručnjak koristi za poslovne funkcije mora biti dostupan u svakom trenutku.

269. Odbor i finansijski stručnjak moraju razumeti i ispuniti svoje odgovornosti u vezi sa bezbednošću oblačnih resursa pod njihovom kontrolom („Bezbednost oblaka“), uz istovremeno dobijanje nezavisne garancije da postoji dovoljna posvećenost i kapacitet službenika za bezbednost u vezi sa bezbednošću infrastrukture gore pomenutih oblačnih resursa („Bezbednost oblaka“).

270. FI mora da održava kontrolu nad lokacijom finansijskih i ličnih podataka koji se čuvaju i obrađuju unutar CSO-a.

271. Čuvanje i obrada finansijskih i ličnih podataka u oblaku trebalo bi da bude ograničeno na jurisdikcije sa relevantnim zakonima ili međunarodnim ugovorima koji pružaju isti nivo zaštite finansijskih i ličnih podataka kao i domaće zakonodavstvo.

272. FI treba da zahteva od službe za bezbednost građevinskih usluga (CSO) da dobije izjavu o nepostojanju primedbi pre nego što podugovori delove ugovorene usluge.

273. FI bi trebalo da zahteva od CSO-a da obezbedi strogo logičko odvajanje svojih virtuelizovanih podataka i resursa od drugih korisnika CSO-a.

274. Politike raskida treba da obezbede uredan izlazak i prenos podataka ako finansijski stručnjak ili dobavljač usluga u oblaku želi da raskine ugovor.

POGLAVLJE X

VEŠTAČKA INTELEGENCIJA

Član 61

Razvoj i primena rešenja omogućenih veštačkom inteligencijom

275. FI treba da uspostavi okvir upravljanja veštačkom inteligencijom (VI) kako bi nadgledao upotrebu VI.

276. FI treba da usklade razvoj i primenu veštačke inteligencije sa svojim strateškim ciljevima, etičkim smernicama i politikama upravljanja rizicima.

277. Upravni odbori treba da obezbede da su sistemi veštačke inteligencije u skladu sa regulatornim zahtevima i u okviru njihovog apetita za rizik. Fiskalne institucije treba da obezbede svest i odgovornost na nivou upravnog odbora za primenu veštačke inteligencije.

278. FI treba da sprovede sveobuhvatne procene rizika za sisteme veštačke inteligencije, uključujući operativne, finansijske, reputacione i pravne rizike.

279. FI treba da obezbede da su sistemi veštačke inteligencije nepristrasni, da se pridržavaju principa pravednog tretmana i da ne dovode do diskriminatornih ishoda. Modeli veštačke inteligencije treba da budu dokumentovani, osiguravajući da su objašnjivi i da se mogu revidirati.

280. Sistemi veštačke inteligencije koji se koriste u kritičnim funkcijama trebalo bi da prođu kroz testiranje opterećenja kako bi se procenili njihovi učinci pod različitim uslovima.

281. FI mora da osigura da su podaci koji se koriste u sistemima veštačke inteligencije tačni, potpuni i nepristrasni.

282. FI mora da validira modele veštačke inteligencije pre primene i redovno nakon toga.

283. FI treba da osigura da su sistemi veštačke inteligencije razumljivi za interne zainteresovane strane i, gde je to primenljivo, za klijente.

284. FI treba da obavesti klijente kada se veštačka inteligencija koristi u odlukama koje se na njih odnose (npr. odobravanje kredita, profilisanje rizika). Trebalo bi da se obezbede kanali za klijente da se žale na odluke podržane veštačkom inteligencijom.

285. FI mora odmah prijaviti incidente koji uključuju kvarove, prekršaje ili negativne rezultate veštačke inteligencije.

286. FI mora da se pridržava principa pravičnosti, odgovornosti, transparentnosti i dizajna usmerenog na čoveka.

287. Implementacija rešenja omogućenih veštačkom inteligencijom u kritičnim funkcijama trebalo bi da zahteva prethodno regulatorno odobrenje.

POGLAVLJE XI
ZAVRŠNE PRELAZNE ODREDBE

Član 62
Sprovođenje, korektivne mere i administrativne kazne

Svako kršenje odredbi ove uredbe podleže korektivnim merama, administrativnim kaznama i novčanim sankcijama kako je navedeno u Zakonu br. 03/L-209 o Centralnoj banci Republike Kosovo, kako je izmenjen i dopunjen Zakonom br. 05/L–150, Zakonom br. 04/L-093 o bankama, mikrofinansijskim institucijama i nebankarskim finansijskim institucijama, Zakonom br. 04/L-155 o platnom sistemu, Zakonom br. 05/L-045 o osiguranju, Zakonom br. 04/L-101 o penzionim fondovima Kosova, kao i Zakonom br. 04/L-018 o obaveznom osiguranju od autoodgovornosti.

Član 63
Primenljivost

Ova uredba ima prednost nad svim odredbama normativnih podzakonskih akata CBK kojima se regulišu informacioni sistemi i upravljanje sajber rizicima finansijskih institucija, a koje nisu u skladu sa ovom uredbom.

Član 64
Aneksi

288. Sledeći prilozi su sastavni deo ove uredbe:

288.1. Prilog 1 – Šablon za izveštavanje o neposrednim informacijama

288.2. Prilog 2 - Šablon detaljnog izveštaja o incidentu.

289. Prilog 1 - Šablon za izveštavanje o neposrednim informacijama i Prilog 2 - Šablon za detaljan izveštaj o incidentu sadrže minimalne definicije i zahteve. Oni mogu biti dopunjeni i zamenjeni posebnim uputstvima koje izdaje CBK.

Član 65
Smernice

Radi sprovođenja ove uredbe, CBK će izdati posebna uputstva.

Član 66
Ukidanje

290. Stupanjem na snagu ove uredbe, sledeće odredbe se ukidaju:

290.1. Uredba o informacionoj tehnologiji za banke;

290.2. Uredba o bezbednosti sistema i informacija za penzione fondove;

290.3. Član 7 - Zahtevi za serversku sobu, iz: Uredbe o minimalnim bezbednosnim zahtevima

290.4. Član 3, stav 2.d, iz: Uredbe o delegiranju funkcija osiguravača.

Član 67
Stupanje na snagu

Ova uredba stupa na snagu 15. septembra 2025. godine. Finansijske institucije - FI su dužne da se pridržavaju zahteva ove uredbe, od 1. juna 2026. godine.

Dr. sc. Baškim Nurboja,
Predsednik Upravnog odbora Centralne banke Republike Kosovo.

PRILOG 1 - ŠABLON ZA IZVEŠTAVANJE O NEPOSREDNIM INFORMACIJAMA

	IZVEŠTAJ O NEPOSREDNIM INFORMACIJAMA
Beleške:	

a	Incident mora biti prijavljen u roku od 4 sata od njegove identifikacije. Drugi izveštaj u propisanom formatu mora biti dostavljen nakon početne istrage, u roku od 72 sata od događaja. Ažuriranja moraju biti dostavljena kad god se dogode bilo kakvi razvoj događaja do podnošenja izveštaja o zatvaranju.
b	Izveštaj o incidentu treba poslati Odeljenju za nadzor informacionih sistema na adresu dmsi@bqk-kos.org
c	Izveštaju treba prethoditi neposredni telefonski razgovor sa službenicima CBK (dok se izveštaj priprema).
d	Izveštaj mora da potpiše CISO.
Osnovne informacije	
1	Naziv i adresa banke koja podnosi izveštaj
2	Imena dva kontakta visokog nivoa. Navesti brojeve telefona i imejl adrese.
Rezime incidenta	
1	Priroda incidenta (npr. DDoS, ransomware, kršenje/krađa podataka, kloniranje ili uništavanje veb stranice)
2	Kratak opis incidenta
3	Vreme incidenta i vreme otkrića
4	Pogođeni sistemi (npr. CBS, Trezor, trgovinske finansije, onlajn bankarstvo, bankomati, platni sistemi kao što su SWIFT, RTGS, ACH), sa naznakom da li su pogođeni sistemi kritični ili nekritični.
Detalji izveštavanja	
1	Datum i vreme prijavljivanja nadređenom/drugim organima vlasti
2	Ime osobe koja prijavljuje
3	Ime i kontakt podaci CISO-a (najmanje dva broja telefona i imejl adresa)
Neposredno saznanje o uzroku incidenta	
1	Kratak opis šta je uzrokovalo uspeh napada
Uticaj incidenta	
1	Očekivani poremećaji kritičnih sistema koji utiču na transakcije kupaca i sisteme plaćanja
2	Obim i priroda kršenja podataka
3	Finansijski uticaj u smislu ukradenog novca, poremećenih poslovnih transakcija itd.
4	Dostupnost tehničkog osoblja za rešavanje situacije i da li je prisutno sve određeno osoblje. Ako ne, navesti alternativne aranžmane koji su napravljeni, uključujući i ugovorno angažovano osoblje.
Preduzete korektivne mere	
1	Privremene mere za ublažavanje/rešavanje problema i razlozi za preduzimanje takvih mera
2	Mere preduzete za zaštitu podataka i drugih detalja neophodnih za forenzičku reviziju
3	Koraci preduzeti/koji treba preduzeti za čišćenje sistema od daljeg oštećenja
4	Predloženi koraci za sprečavanje daljeg ponavljanja ove štete
Upravljanje medijima i zainteresovanim stranama	
1	Bilo kakva komunikacija sa medijima i raznim zainteresovanim stranama/organima (npr. sajber policijom). Treba priložiti kopiju takve komunikacije.
2	Ako dokumenti za komunikaciju nisu prikupljeni, navesti razloge zašto nisu prikupljeni i sledeće korake u vezi sa tim.

Potpis CISO-a
Ime i kontakt podaci - dva broja telefona, adresa e-pošte

PRILOG 2 - ŠABLON DETALJNOG IZVEŠTAJA O INCIDENTU

	DETALJAN IZVEŠTAJ O INCIDENTU
Naziv i adresa banke	
Detalji reference	
1	Referentni broj i datum podnetog Izveštaja o neposrednim informacijama (IIR)
2	Priroda incidenta prijavljenog u IIR-u
3	Ažurirajte broj i datum ovog izveštaja
Kontakt informacije:	
1	Ime osobe koja podnosi izveštaj i potpisuje ga
	Funkcija
	Kontakt telefoni (najmanje dva)
	Adresa e-pošte osobe koja podnosi prijavu
2	Ime alternativnog izveštača
	Funkcija
	Kontakt telefoni (najmanje dva)
	Adresa e-pošte osobe koja podnosi prijavu
3	Ime osobe koja je podnela osnovni izveštaj
	Funkcija
	Kontakt telefoni (najmanje dva)
	Adresa e-pošte osobe koja podnosi prijavu
	(Prepisku treba poslati osobi koja podnosi izveštaj i kopirati je drugim kontaktima. Očekuju se brzi odgovori na prepisku.)
Detalji incidenta	
1	Ozbiljnost incidenta (molimo navesti detalje o različitim korišćenim skalama)
2	Detaljan opis napada
3	Pogođene aplikacije/mreže okrenute ka korisnicima
4	Kako je napad prvi put otkriven?
5	Ko je prvi otkrio napad?
6	Koje su neposredne mere preduzete da se zaustavi širenje ili uticaj napada?
7	Do kog nivoa je akcija eskalirala?
8	Ime proizvođača hardvera, programera softvera, marke/modela itd. pogođenih aplikacija, uključujući i sisteme/mreže na kojima aplikacije rade
9	Da li su gore navedeni prodavci obavešteni i kakva je bila njihova reakcija?
10	Detalji o TCP ili UDP portovima koji su učestvovali u incidentu
11	IP adresa pogođenog sistema i napadača, ako je dostupna
12	Status preduzetih mera za čišćenje sistema i rešavanje problema
13	Kada se može očekivati nastavak normalnog poslovanja?
14	Koji su aranžmani napravljeni za naknadnu reviziju?
15	Koji su aranžmani napravljeni za istražnu reviziju?
16	Da li je lanac čuvanja dokaza održavan? To uključuje vođenje detaljne evidencije koja pokazuje ko je prikupljao, obrađivao, prenosio ili analizirao dokaze od početka istrage.

17	Koji dokazi se zaplenjuju i čuvaju na sigurnom mestu za analizu i kao istražni dokazi? Dokazi mogu da uključuju servere, čvrste diskove, CD-ROM-ove, imejlove, slike, dokumente, logove itd.
18	Koji su istražni alati korišćeni za prikupljanje dokaza?
19	Koji vektori su bili uključeni u napad? Navesti detalje o uređajima, aplikacijama itd. i šta je pošlo po zlu.
	Oprema: serveri, ruteri, uređaji za skladištenje podataka, IPS, zaštitni zidovi, VPN, Wi-Fi, Active Directory, IDS, ISAM, pošta, DHCP, DNS, krajnje tačke, mobilni uređaji, oblak, SaaS, aplikacije trećih strana itd. **Priroda napada**: kompromitovanje lozinke, ljudska intervencija, (fišing), socijalni inženjering, spam, pošta sa zlonamernim softverom, ukradeni sertifikati, neotkrivena ranjivost, uskraćivanje usluge, napad nultog dana, napad ransomverom, krađa podataka
20	IP adrese i imena domena do kojih se može pratiti napad
21	Neuobičajen saobraćaj, neobična aktivnost sa lokacija gde se poslovanje obično ne obavlja, neobični zahtevi od privilegovanih korisnika i administratora, veliki broj pokušaja prijavljivanja, višestruki zahtevi za istu datoteku, velika količina zahteva za podatke, neobične promene u sistemu, neobični domeni, neovlašćena podešavanja, promene konfiguracije itd.