Request for Information (RFI)

Eksterna revizija IT sistema

(provjera usklađenosti BH Telecoma sa COBIT 2019 okvirom i spremnosti za usklađivanje sa NIS 2 direktivom)

1. UVOD

Dioničko društvo BH TELECOM Sarajevo je privredno društvo organizirano kao otvoreno dioničko društvo sa najboljom praksom korporativnog upravljanja. Društvom upravljaju dioničari u skladu sa Zakonom o privrednim društvima ("Službene novine Federacije BiH", broj: 81/15), Zakonom o tržištu vrijednosnih papira ("Službene novine Federacije BiH", br. 85/08, 109/12, 86/15 i 25/17), Pravilnikom o upravljanju dioničkim društvima ("Službene novine Federacije BiH", br. 19/10), te drugim relevantnim zakonima, podzakonskim aktima i ovim Statutom.

Poslovi (odgovornosti i ovlaštenja) rukovodilaca svih organizacionih jedinica i drugih ključnih funkcija u Društvu, definisani su zakonima, Statutom i drugim internim aktima Društva, te dokumentima integrisanog sistema upravljanja (IMS).

Uspostavljanjem procesno orijentisane organizacije u BH Telecomu je povećana vrijednost organizacije kroz komunikaciju i saradnju unutar i između organizacionih cjelina. U BH Telecomu se potpuno i stalno primjenjuju procesi koji su upravljani, mjereni, nadzirani i kroz transformaciju i inovaciju kontinuirano unaprjeđivani.

Više informacija o samoj organizaciji može se naći na linku.

2. CILJANA PUBLIKA

Ovaj dokument je namijenjen firmama koje imaju dokazano iskustvo u provođenju eksterne revizije IT sistema, posebno s poznavanjem COBIT 2019 okvira i direktive NIS 2. Zainteresovana firma treba da ima zaposlene sa minimalno 3 godine iskustva u reviziji IT sistema u skladu sa COBIT 2019 okvirom i zaposlene sa iskustvom u određivanju stepena usklađenosti sa zahtjevima NIS 2 direktive. Potrebno je posjedovanje i odgovarajućih tehničkih znanja s ciljem detaljnije provjere pojedinih segmenata u poslovnim procesima.

3. TERMINOLOGIJA

IMS - Integrisani sistem upravljanja (Sistem upravljanja kvalitetom (QMS), Sistem za upravljanje sigurnošću informacija (ISMS) i Sistem upravljanja rizicima (ERM))
QMS - Quality Management System – Sistem upravljanja kvalitetom
ERM - Enterprise risk management - Sistem upravljanja rizicima
ISMS - (Information security management system) - Sistem za upravljanje sigurnošću informacija
COBIT – (Control Objectives for Information and Related Technologies) - Okvir koji je kreirao ISACA za upravljanje informacijskom tehnologijom (IT) i IT upravljanje. Okvir je poslovno usmjeren i definira skup generičkih procesa za upravljanje IT-om, pri čemu je svaki proces definiran zajedno s ulazima i izlazima procesa, ključnim aktivnostima procesa, ciljevima procesa, mjerama učinkovitosti i osnovnim modelom zrelosti.
NIS 2 - Direktiva (EU) 2022/2555, je zakonodavni akt Europske Unije koji ima za cilj postići visoku zajedničku razinu cyber sigurnosti unutar Unije. Ova direktiva uvodi obaveze koje zahtijevaju od država članica da usvoje nacionalne strategije cyber sigurnosti, kao i da odrede ili uspostave nadležna tijela, tijela za upravljanje kibernetičkim krizama, jedinstvene kontakt tačke za cyber sigurnost i timove za odgovor na računarske sigurnosne incidente (CSIRT).

4. TRENUTNO STANJE

BH Telecom d.d. Sarajevo trenutno ima implementiran integrisani sistem upravljanja u cijelom Društvu, prema, koji uključuje:

- QMS prema 9001:2015 standardu,
- ISMS prema 27001:2022 standardu,
- ERM prema ISO 31000:2009 standardu.

BH Telecom posjeduje i Industrijsku sigurnosnu dozvolu koju je izdalo Ministarstvo sigurnosti Bosne i Hercegovine.

U Društvu se redovno provode:

- Interni i eksterni auditi implementiranih sistema upravljanja,
- Interne revizije,
- Eksterna revizija finansijskog aspekta u kojem je uključen i IT segment.

U BH Telecomu se potpuno i stalno primjenjuju procesi koji su upravljani, mjereni, nadzirani i kroz transformaciju i inovaciju kontinuirano unaprjeđivani. Poslovni procesi su definisani na način, da bilo direktno bilo indirektno, budu u funkciji zadovoljenja potreba i zahtjeva kupaca i drugih zainteresovanih strana

Na osnovu procjene značaja i uticaja na rezultate poslovanja, svi procesi su podijeljeni u 3 kategorije:

I. Upravljački procesi (Procesi po osnovu vlasništva i registracije Društva i korporativni procesi), procesi koji su ključni za strateško odlučivanje i upravljanje kompanijom, uključujući vlasničke strukture i korporativno upravljanje
II. Glavni (CORE) proces, obuhvata ključne aktivnosti koje direktno doprinose primarnim ciljevima i uslugama
III. Pomoćni (prateći) procesi, podržavaju glavne procese i osiguravaju da su resursi i operacije efikasno upravljani i održavani.

IT i TK infrastruktura:

- Heterogenost: BH Telecom koristi različita tehnička rješenja od mnogih proizvođača, što omogućava fleksibilnost i prilagodljivost potrebama korisnika.
- Održavanje: Infrastruktura se održava kombinacijom internih resursa i usluga od strane vendora, osiguravajući pouzdanost i efikasnost.
- Razvoj: BH Telecom razvija vlastita aplikativna rješenja, ali također koristi i rješenja vodećih svjetskih proizvođača, čime se osigurava inovativnost i konkurentnost na tržištu.

BH Telecom, kao i mnoge telekomunikacijske kompanije, suočava se s različitim sigurnosnim izazovima koji mogu ugroziti njihove assete. Prema izvorima, telekomunikacijske kompanije moraju biti posebno oprezne kada je riječ o cyber sigurnosti. BH Telecom je prepoznao ove rizike i implementirao ISMS, koji omogućava primjenu ključnih principa sigurnosti kao što su integritet, dostupnost i povjerljivost informacija. Ova politika sigurnosti je usmjerena na stalno povećanje nivoa sigurnosti poslovnih procesa i zaštite u skladu s identificiranim rizicima.

Obzirom na veličinu kompanije (BH Telecom ima oko 3.000 zaposlenih), koji su geografski raspoređeni po čitavoj BiH, u kompaniji se za pristup IT sistemima koriste raznorazni tipovi radnih stanica za različitim operativnim sistemima.

Pored toga, s obzirom na to da zaposlenici jako često imaju potrebu da pristupaju resursima kompanije putem udaljenog pristupa, tj. VPN-a, koristi se i veliki broj radnih stanica za ove potrebe, a koje su pod kontrolom BH Telecom-a. Nerijetko se koriste i mobilni uređaji za pristup kolaborativnim alatima.

BH Telecom, kao vlasnik kritične infrastrukture, provodi aktivnosti na planiranim izmjenama zakonskog i regulatornog okvira koji se odnosi na evropske standarde u oblasti informacione sigurnosti.

5. ZAHTJEVI

Za uspješnu provjeru usklađenosti BH Telecoma sa COBIT 2019 okvirom i spremnosti za usklađivanje sa NIS 2 direktivom, potrebno je detaljno analizirati postojeće procese i politike unutar organizacije. Fokus bi trebao biti na sljedećim aspektima:

1. Izvršna direkcija za informacione tehnologije (ID IT):
   - Analiza usklađenosti upravljačkog okvira i njegove implementacije sa COBIT 2019 standardom.
   - Ocjena sposobnosti ID IT da upravlja rizicima i osigura integritet, dostupnost i povjerljivost informacija u skladu sa NIS 2 direktivom.
2. Direkcija za servise u Izvršnoj direkciji za tehnologiju i razvoj servisa (Direkcija za servise u ID TIRS):
   - Analiza procesa razvoja, održavanja i upravljanja servisima kako bi se osiguralo da su u skladu sa COBIT 2019.
   - Procjena mjera za upravljanje sigurnosnim incidentima i kontinuitetom poslovanja u skladu sa zahtjevima NIS 2 direktive.
3. Direkcija za konvergentno jezgro u Izvršnoj direkciji za tehnologiju i razvoj servisa (Direkcija za konvergentno jezgro u ID TIRS):
   - Analiza infrastrukture i usluga koje su ključne za podršku konvergentnom jezgru. Ova analiza treba uključivati detaljnu procjenu usklađenosti s COBIT 2019 okvirom i NIS 2 direktivom, što je neophodno za osiguravanje visokih standarda sigurnosti i pouzdanosti. Pritom je važno identificirati potencijalne rizike i ranjivosti
   - Analiza sigurnosnih mjera i postupaka zaštite podataka, uključujući fizičku i logičku sigurnost, kao i mjere zaštite od cyber prijetnji.

Osnovni cilj u ID IT jeste osigurati kontinuirani razvoj informacionog sistema u skladu sa potrebama BH Telecom, uz razvoj savremene i funkcionalne IT arhitekture i uz pružanje adekvatne IT podrške dinamičnom razvoju ponude BH Telecom u svim tržišnim segmentima uz pružanje kvalitetne podrške funkcionisanju IT servisa i efikasne eksploatacije IS, kako bi u konačnici imali stabilnu i pouzdanu IT platformu i efikasne mjere sigurnosti i zaštite podataka. Također, IDI IT vrši upravljanje životnim ciklusom razvoja IT rješenja iz domena Direkcije, vrši kreiranje i kontrolu provođenja politike sigurnosti i zaštite podataka informacionog sistema, te održava ključne IT resursa uz kontinuirani razvoj kvalitetnih znanja i vještina kod radnika.

Direkcija za servise u ID TIRS ima za cilj da osigura optimalan razvoj i integralnu izgradnju servisnih platformi koje će omogućiti pružanje visokokvalitetnih „n-play“ usluga krajnjim korisnicima. Ovo uključuje ne samo implementaciju naprednih tehnoloških rješenja, već i brzo rješavanje svih tehničkih problema koji bi mogli nastati. Također, jedan od primarnih ciljeva je pružanje aplikativnih rješenja visokog tehničkog kvaliteta, koja su dostupna korisnicima putem različitih pristupnih mreža i na različitim terminalima. Ovo osigurava da korisnici imaju konzistentno iskustvo bez obzira na to kako i gdje pristupaju uslugama, čime se postiže visok nivo zadovoljstva korisnika i jača njihova lojalnost.

Direkcija za konvergentno jezgro u ID TIRS ima ključnu ulogu u BH Telecomu, s fokusom na razvoj i održavanje jezgra mreže. Njihov cilj je osigurati visokokvalitetne usluge i brzo rješavanje tehničkih problema, što je od suštinskog značaja za zadovoljstvo korisnika. Također, teže optimalnoj tranziciji sa uskopojasnih na širokopojasne telekomunikacijske platforme, čime se osigurava kontinuitet u kvaliteti govornih usluga.

Kako se kroz usklađenost sa standardom ISO 27001 pokriva većina mjera iz COBIT 2019 i NIS 2 Direktive, a BH Telecom ima implementiran i certificiran ISMS u skladu sa zahtjevima ISO 27001:2022, planiranom postupkom se očekuje detaljna revizija implementacije procesnih, tehničkih i organizacijskih mjera.

Kroz usluge revizije treba da se identificiraju i daju preporuke za potencijalna poboljšanja u pogledu usklađenosti prema zahtjevima COBIT 2019 okvira i spremnosti za usklađivanje sa NIS 2 direktivom i pozicioniranje organizacionih jedinica BH Telecoma u skladu sa određenim područjima, i to za:

COBIT 2019:
Uraditi procjenu usklađenosti informacionog sistema BH Telecoma sa COBIT 2019 okvirom, imajući u vidu da je potrebno detaljnom analizom dati informaciju kako i u kojoj mjeri BH Telecom upravlja informacionim i tehnološkim resursima, odnosno da li IT strategija i operacije odgovaraju na zahtjeve ovog okvira, a što uključuje:

- **Evaluaciju IT strategije** - fokus na to kako IT ciljevi podržavaju poslovne prioritete i kako se planovi usklađuju sa strateškim smjernicama,
- **Upravljanje IT ulaganjima** – izvršiti ocjenjivanje kako organizacija definira, prati i kontrolira IT ulaganja u skladu s poslovnim ciljevima,
- **Praćenje i mjerenje IT performansi**, kako bi se provjerilo da li su uspostavljane jasne metrike i KPI-jevi koji bi omogućili efikasno praćenje i ocjenjivanje IT uspjeha,
- **Service desk** - provjera vrlo važnog segmenta za koje je potrebno provjeriti da li zahtjevi i incidenti upravljanih usluga doprinose postizanju cilja usklađivanja kod IT isporuka u skladu sa poslovnim zahtjevima,
- **Upravljanje IT projektima** - planiranje projekata, kako se izvode i prate, te kako se osigurava da su u skladu sa širim poslovnim ciljevima,
- **Upravljanje IT rizicima i promjenama** – da li se primjenjuje sistematičan pristup identifikaciji, evaluaciji i upravljanju rizicima, kao i efikasno upravljanje promjenama kako bi se minimizirali potencijalni negativni uticaji na poslovanje,
- **Upravljanje IT imovinom** - da li se provode efikasni procesi u upravljanju IT imovinom,
- **Unapređenje IT procesa, standarda i procedura** – procjena u cilju identifikacije i implementacije potrebnih poboljšanja u IT procesima, standardima i procedurama,
- **Razvoj IT kompetencija i znanja** – procjena trenutnog stanja IT kompetencija, znanja i vještina unutar BH Telecoma te identifikacija područja za razvoj i poboljšanje.

NIS 2:
Uraditi procjenu spremnosti za usklađivanje sa ovom direktivom, tako da se provede analiza da li je uz organizacione jedinice iz revizijom definisanog opsega potrebno uključiti i druge koje bi trebale biti tretirane ovom regulativom i to na osnovu provedene analize i ocjene implementiranih organizacijskih i tehničkih mjera u područjima:

- **Politike analize rizika i sigurnosti informacionih sistema** - u cilju jačanja i pojednostavljenja zahtjeva u pogledu sigurnosti i izvještavanja uvođenjem pristupa upravljanju rizicima kojim se osigurava minimalni popis osnovnih sigurnosnih elemenata koje je potrebno primijeniti.
- **Postupanje s incidentima** – uspostava ravnoteže između potrebe za brzim reagovanjem i izvještavanjem kako bi se izbjeglo potencijalno širenje incidenata i potrebe za detaljnim izvještavanjem i kako bi se izvukle vrijedne pouke iz pojedinačnih incidenata.

- **Kontinuitet poslovanja, kao što je upravljanje sigurnosnim kopijama i oporavak od katastrofe, te upravljanje krizama** - utvrđivanje ukupnih učinaka prekida rada kritične infrastrukture koje uključuju: ljudske gubitke - procjenjuje se mogući broj smrtno stradalih ili ozlijeđenih zbog prekida rada pojedine kritične infrastrukture, privredne gubitke - procjenjuju se s obzirom na važnost privrednog gubitka i/ili smanjenja kvaliteta proizvoda ili usluga, uključivo i moguće učinke na okoliš, uticaj na javnost - koji se procjenjuje s obzirom na uticaj na povjerenje javnosti, remećenje svakodnevnog života, uključivo i gubitak osnovnih te javnih usluga.
- **Sigurnost lanca nabave, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih direktnih dobavljača ili pružatelja usluga** – zahtjev prema pojedinačnim preduzećima da riješe cyber sigurnosne rizike u lancima nabave i odnosima s dobavljačima.
- **Politike i postupke za procjenu djelotvornosti mjera upravljanja cyber sigurnosnim rizicima** - utvrđivanje i dokumentacija poznatih ovisnosti i ranjivosti.
- **Osnovne prakse „cyber higijene" i osposobljavanje o cyber sigurnosti** – način zaštite pohranjenih, poslanih ili na drugačiji način obrađenih podataka od slučajnog ili neovlaštenog uništavanja, gubitka ili izmjene ili nedostatka dostupnosti tokom cijelog životnog ciklusa proizvoda, usluge ili procesa IKT.
- **Sigurnost ljudskih resursa, politike kontrole pristupa i upravljanje imovinom** - evidentiranje kojim se podacima, uslugama ili funkcijama pristupilo i koji su podaci, usluge ili funkcije upotrijebljeni ili na drugi način obrađeni, kada i ko je to učinio.
- **Korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sistema u hitnim slučajevima -** omogućavanje, gdje je potrebno, da se koristi viši nivo sigurnosti prilikom pristupa imovini.

U sklopu odgovora na RFI, pored tehničkih detalja, potrebno je dostaviti:
- informativnu cijenu,
- vremenski okvir potreban za realizaciju implementacije ovog projekta,
- planiranu metodologiju prema kojoj će se raditi revizija/procjena,
- dokaz da je firma u periodu 2020-2024. godine uspješno završila ili ima u realizaciji minimalno 2 (dva) ugovora eksterne revizije IT sistema u firmama sa 500 i više zaposlenih.
- sve reference firme i certifikate uposlenih koji su relevantni za ove poslove (kao što je CISA i/ili druge odgovarajuće certifikate kojima se dokazuje sposobnost provjere usklađenosti sa za COBIT 2019 okvirom i usklađenosti sa NIS 2 direktivom),
- eventualne dodatne prijedloge i sugestije koji nisu prethodno navedeni u okviru RFI dokumenta.