14.10.2025. g
01/9-1042/8-25

UGOVOR O JAVNOJ NABAVCI

Ovaj ugovor zaključen je između:

Naručioca: KOMISIJA ZA TRŽIŠTE KAPITALA sa sjedištem u Podgorici, ulica Kralja Nikole 27A/III, PIB: 02322439, koga zastupa predsjednik komisije, Željko Drinčić, (u daljem tekstu: Naručilac)

i

Ponudača: "COMPLIANT RISK TECHNOLOGY" D.O.O. ZAGREB, sa sjedištem na adresi Remetinečka cesta 7A, 10000 Zagreb, Republika Hrvatska, PIB: 30872422309, Broj racuna: Bank IBAN: HR1124840081106002978, Bank SWIFT: RZBHHR2X, koji se vodi kod Raiffeisenbank Austria d.d. Zagreb, koga zastupa Dragan Oremuš, direktor (u daljem tekstu: Izvršilac).

OSNOV UGOVORA:

Tenderska dokumentacija za otvoreni postupak javne nabavke za nabavku usluga – Implementacija SupTech rješenja za nadzor tržišta kapitala za potrebe Komisije za tržište kapitala (ponovljeni postupak), broj 01/9-1042/3-25 od 09.09.2025.godine.

Broj i datum Odluke o izboru najpovoljnije ponude 01/9-1042/8-25 od 06.10.2025. godine.

Ponuda Izvršioca "COMPLIANT RISK TECHNOLOGY" D.O.O. ZAGREB broj 140776 od 23.09.2025. godine.

Član 1

Predmet ovog ugovora je nabavka usluge - Implementacija SupTech rješenja za nadzor tržišta kapitala za potrebe Komisije za tržište kapitala (ponovljeni postupak), prema Tenderskoj dokumentaciji broj: 01/9-1042/3-25 od 09.09.2025.godine, Odluci o izboru najpovoljnije ponude broj: 01/9-1042/8-25 od 06.10.2025. godine i ponudi Izvršioca broj: 140776 od 23.09.2025. godine sa specifikacijom:

Obim ove nabavke uključuje nabavku, instalaciju, opsežnu konfiguraciju i neophodna prilagođavanja (u okviru predloženog COTS rješenja), testiranje, puštanje u rad i pokretanje sveobuhvatnog nadzornog sistema zasnovanog na COTS-u. Potrebne usluge takođe uključuju:

- Licenciranje i implementacija softvera: Obezbjeđivanje svih neophodnih softverskih licenci za predloženi sistem. Predloženo rješenje treba da bude tržišno dokazan COTS proizvod. Model implementacije (on-premise ili cloud-based) će se razmatrati na osnovu predloga koji ispunjavaju bezbjednosne i operativne zahtjeve Komisije, sa daljim detaljima definisanim u nastavku.
- Migracija podataka: Podrška za migraciju postojećih relevantnih podataka iz zastarjelih sistema i baza podataka SCMN-a u novi sistem, kako je specificirala Komisija.
- Integracija sistema: Integracija novog sistema sa postojećom IT infrastrukturom SCMN-a i drugim relevantnim internim ili eksternim sistemima identifikovanim tokom projekta,

koristeći standardne integracione sposobnosti COTS rješenja gdje je to moguće, uključujući i IAM rješenja.

●Obuka: Sveobuhvatni programi obuke za različite korisničke grupe SCMN-a, uključujući krajnje korisnike, administratore sistema i tehničko osoblje, koji pokrivaju sve aspekte funkcionalnosti i konfiguracionih sposobnosti COTS sistema.

●Dokumentacija: Obezbjeđivanje kompletne sistemske dokumentacije na engleskom i/ili crnogorskom jeziku, uključujući standardne priručnike za COTS proizvod, kao i vodiče specifične za konfiguraciju, korisničke priručnike, administrativne vodiče, tehničke priručnike i materijale za obuku.

●Podrška i održavanje nakon implementacije: Sveobuhvatan ugovor o podršci i održavanju za COTS rješenje, uključujući definisane Ugovore o nivou usluge (SLA), za tekuću tehničku podršku, ispravke grešaka, ažuriranja i nadogradnje, osiguravajući da sistem ostane usklađen sa regulatornim promjenama i tehnološkim napretkom. Ovo uključuje mehanizme za prilagođavanje evoluirajućim regulatornim zahtjevima (npr. nove taksonomije, pravila validacije) putem ažuriranja proizvoda i konfiguracije.

●Obezbjeđivanje neproizvodnih okruženja: Nabavka i postavljanje neophodnih neproizvodnih okruženja kako je navedeno u odjeljku Tehnički zahtjevi. 4. Funkcionalni zahtjevi Nadzorni sistem mora pružiti sveobuhvatan skup funkcionalnosti, dostupnih kao standardne ili konfigurabilne karakteristike predloženog COTS rješenja, kako bi podržao regulatorni i nadzorni mandat SCMN-a. Zahtjevi su kategorisani u nastavku. Dobavljači treba jasno da naznače da li je svaka karakteristika Obavezna (M), Poželjna (D) ili Opciona (O) sposobnost. 4.1. Unos, upravljanje i skladištenje podataka

●(M) Bezbjedan prijem podataka: Sposobnost bezbjednog primanja podnesaka podataka od nadziranih subjekata putem različitih kanala, uključujući namjenski online portal i potencijalno sistemske API-je, kao konfigurabilne opcije unutar COTS rješenja.

●(M) Podrška za različite formate podataka: Sposobnost unosa, obrade i upravljanja podacima u više formata, uključujući, ali ne ograničavajući se na XML, XBRL, iXBRL, CSV, Excel i običan tekst, koristeći standardne ili konfigurabilne parsere.

●(M) Mehanizam za validaciju podataka: Robustne mogućnosti validacije podataka, koje mogu konfigurisati korisnici SCMN-a, za automatsku provjeru podnijetih podataka u odnosu na unaprijed definisana pravila, taksonomije (npr. relevantne nacionalne i međunarodne standarde) i poslovnu logiku kako bi se osigurala tačnost, potpunost i konzistentnost. Ovo uključuje identifikaciju grešaka (razlikovanje nivoa ozbiljnosti, npr. upozorenje, kritična greška) i izvještavanje podnosiocima.

●(M) Transformacija i mapiranje podataka: Alati unutar COTS rješenja za transformaciju i mapiranje dolaznih podataka u standardizovani interni format pogodan za obradu, skladištenje i analizu unutar tehnologije za obradu ili ugrađene analitike.

●(M) Centralizovano skladište podataka: Bezbjedno i skalabilno centralno skladište podataka (npr. sposobnosti data warehouse-a ili data lake-a inherentne ili podržane od strane COTS rješenja) za čuvanje svih regulatornih i nadzornih podataka.

●(M) Upravljanje kvalitetom podataka: Funkcionalnost za tekuće praćenje, čišćenje i obogaćivanje kvaliteta podataka, koju može konfigurisati SCMN.

●(D) Optičko prepoznavanje znakova (OCR) i upravljanje dokumentima: ○(M) Osnovno upravljanje dokumentima: Sposobnost čuvanja i upravljanja nestrukturiranim dokumentima (npr. PDF-ovima) povezanim sa nadziranim subjektima ili nadzornim procesima. ○(O) Napredni OCR i ekstrakcija podataka (konfigurabilna obrada podataka): Sposobnost obrade skeniranih dokumenata i ekstrakcije strukturiranih podataka pomoću OCR tehnologije za dalju obradu i integraciju u sistem. Ovo uključuje

konfigurabilne tokove posla za obradu ekstrahovanih podataka, omogućavajući rutiranje i validaciju zasnovanu na pravilima. 4.2. Regulatorno izvještavanje

●(M) Automatsko generisanje izvještaja: Sposobnost automatskog generisanja unaprijed definisanih regulatornih izvještaja za internu upotrebu SCMN-a i za podnošenje drugim nacionalnim ili međunarodnim tijelima, na osnovu prikupljenih podataka, koristeći konfigurabilne predloške izvještaja.

●(M) Obavezna podrška za okvire i taksonomije izvještavanja EU: Sistem mora pružiti dokazanu, konfigurabilnu podršku za sljedeće regulatorne okvire EU. Dobavljač mora opisati svoje iskustvo i modul/funkcionalnost za svaki od njih: ○EBA okviri:

■DORA (Digital Operational Resilience Act): Sposobnost upravljanja i izvještavanja o velikim incidentima vezanim za ICT i upravljanja registrom rizika trećih strana u oblasti ICT-a kako je propisano DORA-om.

■EBA Reporting Gateway: Sistem mora biti u stanju da pripremi pakete podataka za podnošenje EBA-i putem EUCLID platforme. ○ESMA okviri:

■ESEF (European Single Electronic Format): Puna podrška za primanje godišnjih finansijskih izvještaja u iXBRL formatu.

■Izvještavanje o fondovima: Podrška za AIFMD (Alternative Investment Fund Managers Directive) i MMFR (Money Market Fund Regulation) izvještavanje.

■Izvještavanje o tržišnim podacima: Sposobnost budućeg skaliranja i pripreme podataka u skladu sa okvirima kao što su FIRDS (Financial Instruments Reference Data System) i CSDR (Central Securities Depository Regulation). ○ESG i okviri održivosti: Sistem mora uključivati fleksibilan modul za prikupljanje, validaciju i izvještavanje podataka u skladu sa zahtjevima CSRD (Corporate Sustainability Reporting Directive) i SFDR (Sustainable Finance Disclosure Regulation).

●(M) Podrška za međusektorske taksonomije: Prednost će se dati dobavljačima koji mogu dokazati da njihova platforma takođe podržava taksonomije iz drugih finansijskih sektora, što ukazuje na visoku fleksibilnost i buduću održivost. Ovo uključuje: ○EIOPA okviri: Podrška za Solvency II (SII) i/ili IORP (Institutions for Occupational Retirement Provision) taksonomije izvještavanja.

●(M) Samostalno dizajniranje, upravljanje i verzionisanje izvještaja: Sistem (COTS rješenje) mora pružiti korisnicima SCMN-a intuitivne ugrađene alate za nezavisno dizajniranje, kreiranje, modifikovanje i upravljanje regulatornim izvještajima. Ovo uključuje sposobnosti za definisanje izvora podataka, izgleda izvještaja, proračuna i robusnu kontrolu verzija za predloške i definicije izvještaja, zajedno sa jasnim revizorskim tragom za promjene u dizajnu izvještaja.

●(M) Upravljanje promjenama za definicije izvještavanja: Sistem mora uključivati funkcije ili podržavati definisan proces za upravljanje promjenama u definicijama izvještaja i predlošcima za prikupljanje podataka. Ovo uključuje praćenje različitih verzija, upravljanje datumima stupanja na snagu, dokumentovanje promjena i olakšavanje procesa odobravanja modifikacija izvještaja ili struktura podataka, putem konfiguracije sistema.

●(M) Interno testiranje, simulacija i životni ciklus implementacije definicija izvještaja: Sistem mora pružiti robusne sposobnosti za korisnike SCMN-a da interno testiraju, validiraju i upravljaju životnim ciklusom implementacije novodizajniranih ili modifikovanih definicija izvještaja i njihovih povezanih pravila za validaciju podataka prije nego što postanu dostupne u sandbox okruženju subjekta ili proizvodnom okruženju. To će uključivati: ○Mehanizam za simulaciju procesa podnošenja podataka za datu definiciju izvještaja unutar kontrolisanog internog okruženja (različitog od sandboxa koji koriste eksterni subjekti za testiranje sa živim podacima). ○Alate za

korisnike SCMN-a za unos ili učitavanje uzoraka/testnih podataka u odnosu na definiciju izvještaja kako bi se temeljno testirala sva validaciona logika i pravila obrade podataka. ○Korisnički prilagođen interfejs za simulaciju i pregled kako bi sistem obradio podnijete podatke, kako bi se oni pojavili u nacrtima formata izvještaja i kako bi funkcije nadzora (npr. kontrolne table, analitički prikazi) interagovale sa ovim podacima. ○Jasne procedure ili funkcionalnosti kojima upravlja SCMN za promovisanje ili implementaciju potpuno testiranih i validiranih definicija izvještaja iz ove faze internog testiranja/simulacije u namjensko Testno okruženje (navedeno u odjeljku 5.7) za dalje UAT, zatim u Sandbox okruženje za testiranje od strane subjekata, i konačno u Proizvodno okruženje.

●(M) Alati za ad-hoc izvještavanje: Korisnički prilagođeni ugrađeni alati, kao dio COTS rješenja, za osoblje SCMN-a da kreira prilagođene izvještaje i upite na osnovu dostupnih podataka bez potrebe za obimnom IT intervencijom ili programerskim vještinama.

●(M) Verzionisanje i arhiviranje izvještaja: Održavanje istorijskih verzija generisanih izvještaja i osiguravanje bezbjednog arhiviranja kako izlaznih rezultata izvještaja tako i njihovih osnovnih definicija.

●(D) Upravljanje podnescima: Funkcije za upravljanje procesom podnošenja izvještaja od strane nadziranih subjekata, uključujući praćenje statusa podnesaka, rokova i podsjetnika. 4.3. Automatizacija toka posla obrade nadzornih podataka

●(M) Konfigurabilni mehanizam za tokove posla obrade podataka: "No-code" konfigurabilni mehanizam za obradu tokova posla, kao osnovna konfigurabilna komponenta COTS rješenja, fokusiran na konfigurisanje i automatizaciju tokova obrade podataka vezanih za regulatorne podneske. Ovo mora uključivati sposobnosti za SCMN da definiše: ○Faze i zadatke za unos, validaciju i preliminarnu procjenu podataka. ○Uloge odgovorne za svaku fazu/zadatak. ○Prelaze između faza, uključujući automatsko rutiranje ili sistemske akcije (npr. označavanje za pregled, davanje uslovnog ili automatskog odobrenja za dalju obradu/prihvatanje u glavni repozitorijum) na osnovu ishoda validacije podataka, posebno ozbiljnosti identifikovanih grešaka (npr. razlikovanje sistemskih akcija za 'upozorenja' naspram 'kritičnih grešaka'). ○Evidenciju akcija obrade.

●(M) Notifikacije i upozorenja za tokove posla obrade podataka: Automatske notifikacije i upozorenja korisnicima u vezi sa neriješenim zadacima, rokovima, eskalacijama i značajnim događajima unutar konfigurisanih tokova posla obrade podataka. 4.4. Procjena i upravljanje rizicima

●(M) Profiliranje rizika: Alati unutar COTS rješenja za kreiranje i održavanje profila rizika za nadzirane subjekte na osnovu podnijetih podataka, nadzornih nalaza i drugih relevantnih informacija, sa konfigurabilnim parametrima. Okvir za procjenu rizika treba da bude dovoljno fleksibilan da modelira različite vrste rizika relevantne za tržišta kapitala, kao što su tržišni rizik, kreditni rizik, rizik likvidnosti, operativni rizik i rizik ponašanja.

●(M) Konfigurabilno bodovanje rizika: Sposobnost SCMN-a da definiše i primijeni konfigurabilne metodologije i parametre za bodovanje rizika kako bi procijenio nivoe rizika nadziranih subjekata i finansijskih instrumenata.

●(D) Praćenje rizika i kontrolne table: Kontrolne table i alati, koristeći ugrađene analitičke sposobnosti sistema (ili željeno fleksibilno BI okruženje ako je implementirano), za tekuće praćenje identifikovanih rizika i ključnih indikatora rizika (KRI), koje može konfigurisati SCMN. 4.5. Analitika podataka i poslovna inteligencija

●(O) Unaprijed izgrađene kontrolne table i vizualizacija sa unaprijed postavljenim KPI-jevima i KRI-jevima: COTS sistem bi poželjno trebao da uključuje robusne, unaprijed

izgrađene alate i kontrolne table za korisnike SCMN-a, sa sveobuhvatnim setom interaktivnih vizualizacija i unaprijed postavljenih ključnih pokazatelja performansi (KPI) i ključnih indikatora rizika (KRI).

●(M) Ugrađeni napredni alati za samouslužne upite i izvještavanje: COTS sistem mora pružiti moćne, ali intuitivne ugrađene alate koji omogućavaju samouslužno istraživanje i analizu podataka od strane korisnika SCMN-a. Ovo uključuje sposobnost fleksibilnog i nezavisnog kreiranja prilagođenih analitičkih izvještaja i ad-hoc upita koristeći sopstvene funkcionalnosti sistema, bez potrebe za eksternim alatima ili IT intervencijom za standardne analitičke potrebe.

●(D) Fleksibilno okruženje za poslovnu inteligenciju (BI) za naprednu vizualizaciju i izvještavanje: Sistem bi poželjno trebao da pruži okruženje koje podržava, ili se besprekorno integriše sa, naprednim alatima za poslovnu inteligenciju (BI) i vizualizaciju podataka koji su po sposobnostima uporedivi sa vodećim BI platformama na tržištu (npr. Power BI, Tableau ili slično). Ovo okruženje je namijenjeno specijalizovanim korisnicima (npr. analitičarima podataka unutar SCMN-a) za izgradnju visoko interaktivnih i sofisticiranih kontrolnih tabli i izvještaja, potencijalno koristeći složene skupove podataka i napredne tehnike vizualizacije. Ovo bi dopunilo ugrađenu samouslužnu analitiku sistema omogućavanjem specijalizovanijih ili složenijih analitičkih prezentacija kada je to potrebno.

●(D) Sistem ranog upozoravanja (EWS): Funkcionalnost, konfigurabilna unutar COTS rješenja, za razvoj i implementaciju EWS-a na osnovu unaprijed definisanih pravila i analitičkih modela kako bi se označili potencijalni problemi ili anomalije koje zahtijevaju nadzornu pažnju.

●(D) Alati za statističku analizu: Integracija ili obezbjeđivanje alata za vršenje statističke analize nadzornih podataka. 4.6. Praćenje usklađenosti

●(M) Mehanizam pravila za provjere usklađenosti: Konfigurabilni mehanizam pravila unutar COTS rješenja za automatsku provjeru usklađenosti nadziranih subjekata sa regulatornim zahtjevima na osnovu podnijetih podataka i drugih informacija. Pravilima treba da upravlja osoblje SCMN-a.

●(M) Praćenje regulatornih promjena: Mehanizam za praćenje promjena u regulativi i olakšavanje ažuriranja povezanih pravila i nadzornih procesa unutar sistema putem konfiguracije.

●(M) Nadzor i upravljanje kršenjima podnesaka: Funkcionalnost za evidentiranje, praćenje i upravljanje identifikovanim kršenjima regulative ili nadzornih podnesaka, sa lako preglednim rokovima po kombinacijama podnesaka. 4.7. Upravljanje korisnicima i kontrola pristupa

●(M) Enterprise-grade upravljanje identitetom i pristupom (IAM): Sistem mora uključivati ili se besprekorno integrisati sa enterprise-grade IAM rješenjem. Ovo rješenje će obezbijediti robusno i centralizovano upravljanje identitetima korisnika, jaku autentifikaciju (uključujući dvofaktorsku autentifikaciju (2FA) kako je detaljno navedeno u nastavku), granularne politike autorizacije (podržavajući RBAC model detaljno opisan u nastavku), i upravljanje životnim ciklusom identiteta (npr. dodjeljivanje, oduzimanje pristupa, pregledi pristupa) na svim komponentama sistema, uključujući portal za subjekte.

●(M) Bezbjedna autentifikacija sa samouslužnim 2FA (TOTP/HOTP): IAM rješenje mora podržavati jake mehanizme autentifikacije, sa obaveznim zahtjevom za dvofaktorsku autentifikaciju (2FA) za sve korisnike. Serverski mehanizam za 2FA mora podržavati standardne TOTP (Time-based One-Time Password, u skladu sa RFC 6238) i HOTP (HMAC-based One-Time Password, u skladu sa RFC 4226) algoritme za generisanje i

validaciju jednokratnih lozinki. Sistem mora pružiti samouslužni mehanizam za korisnike da se prijave, upravljaju (npr. re-sinhronizuju, uklone) i testiraju svoje 2FA autentifikatore. Sistem mora nativno podržavati upotrebu uobičajenih OTP aplikacija koje su u skladu sa standardima (npr. FreeOTP, Google Authenticator, Microsoft Authenticator i druge slične aplikacije koje podržavaju TOTP/HOTP standarde) bez zahtjeva za vlasničkim hardverskim tokenima ili specifičnim aplikacijama dobavljača.
●(M) Sposobnost jedinstvene prijave (SSO): EWP portal treba da pruži SSO sposobnost za sve ponuđene module sa mogućnošću integracije novih samostalnih modula putem standardizovanih protokola za pristup i bezbjednost integrisanih sa IAM (dodavanje novih modula treba da bude putem low-code (konfiguracija), no-code mehanizama).
●(M) Kontrola pristupa zasnovana na ulogama (RBAC): Sveobuhvatan RBAC mehanizam, koji mogu konfigurisati administratori SCMN-a kao dio IAM okvira, kako bi se osiguralo da korisnici mogu pristupiti samo podacima i funkcionalnostima relevantnim za njihove uloge i odgovornosti.
●(M) Upravljanje korisničkim nalozima: Centralizovana administracija korisničkih naloga, uloga i dozvola putem IAM rješenja.
●(M) Razdvajanje dužnosti: Dizajn sistema, podržan IAM i RBAC konfiguracijama, treba da sprovodi principe razdvajanja dužnosti.
●(D) Protokoli za integraciju IAM: Jaka prednost za IAM rješenja koja podržavaju standardne protokole (npr. SAML 2.0, OAuth 2.0/OpenID Connect) kako bi se olakšala potencijalna integracija sa postojećim ili budućim korporativnim provajderima identiteta SCMN-a. 4.8. Revizorski tragovi i evidentiranje
●(M) Sveobuhvatni revizorski tragovi: Detaljni i nepromjenljivi revizorski tragovi za sve sistemske aktivnosti, uključujući pristup podacima, modifikacije podataka, akcije korisnika (povezane sa IAM identitetima), promjene konfiguracije sistema i promjene definicija izvještaja ili pravila validacije.
●(M) Upravljanje i pregled logova: Bezbjedno evidentiranje sistemskih događaja i alati za ovlašćeno osoblje za pregled i analizu logova. 4.9. Integracija sistema
●(M) API sposobnosti: Robusni aplikacioni programski interfejsi (API) (npr. RESTful API), obezbijeđeni kao dio COTS rješenja, kako bi se omogućila integracija sa drugim internim sistemima SCMN-a (npr. računovodstvo, upravljanje dokumentima) i relevantnim eksternim sistemima (npr. registar preduzeća, druga regulatorna tijela, međunarodne organizacije) na bezbjedan način.
●(M) Dokazana integracija sa regulatornim gateway-ima EU: Sistem mora pružiti standardne ili konfigurabilne module ('HUB konektore') za bezbjedan i pouzdan prenos regulatornih izvještaja tijelima EU. Dobavljač mora pružiti dokaze o postojećim takvim integracijama kod drugih regulatornih tijela. Ova sposobnost mora pokrivati, najmanje, prenos podataka na: ○ESMA-ine platforme za izvještavanje podataka (ESEF). ○EBA-in centralni data hub (EUCLID).
●(M) Sposobnosti izvoza podataka: Sposobnost bezbjednog izvoza podataka u različitim formatima za upotrebu u drugim sistemima ili za eksterno izvještavanje, podložno odgovarajućoj autorizaciji i konfiguraciji. 4.10. Komunikacione i portalske funkcije
●(M) Bezbjedan portal za subjekte: Namjenski i bezbjedan web-baziran portal, kao dio COTS rješenja, za nadzirane subjekte da: ○Podnose regulatorne podatke i prateću dokumentaciju. ○Primaju obavještenja i komunikacije od SCMN-a. ○Prate status svojih podnesaka i zahtjeva. ○Pristupaju relevantnim regulatornim informacijama i smjernicama koje objavljuje SCMN. ●(M) Sandbox sposobnost podnošenja: Portal mora uključivati namjensko 'sandbox' ili testno okruženje gdje nadzirani subjekti mogu vršiti probne podneske regulatornih podataka (npr. za nove ili revidirane predloške

izvještavanja, XBRL taksonomije) u odnosu na definicije izvještaja koje su prošle interno testiranje i simulaciju SCMN-a (prema odjeljku 4.2). Ovaj sandbox treba da omogući subjektima da validiraju svoje podatke u odnosu na važeća pravila i taksonomije bez da se podnesak smatra zvaničnim, pružajući povratne informacije o kvalitetu podataka i usklađenosti formata prije formalnog podnošenja u proizvodno okruženje.

●(M) Bezbjedno slanje poruka: Bezbjedne interne mogućnosti slanja poruka unutar sistema i za komunikaciju sa nadziranim subjektima putem portala kroz konfigurabilni tok posla obrade.

●(D) Modul za javno objavljivanje: Modul za olakšavanje pripreme i objavljivanja ovlašćenih informacija na javnoj web stranici SCMN-a. 5. Tehnički zahtjevi Sistem mora ispunjavati visoke tehničke standarde kako bi se osigurala pouzdanost, bezbjednost, performanse i održivost, u skladu sa vodećim COTS rješenjem. 5.1. Arhitektura sistema

●(M) Moderna arhitektura: Predloženi sistem treba da bude zasnovan na modernoj, robusnoj i skalabilnoj arhitekturi (npr. N-tier, orijentisana na mikroservise ili drugi dokazani arhitektonski obrasci koji promovišu modularnost i fleksibilnost). Prednost će se dati rješenjima izgrađenim na dobro definisanoj, od strane dobavljača podržanoj COTS platformskoj arhitekturi koja osigurava stabilnost i jasan put nadogradnje.

●(M) Opcije implementacije: Dobavljači treba da navedu dostupne modele implementacije za svoje COTS rješenje (npr. on-premise, privatni cloud, javni cloud, hibridni). SCMN će ocjenjivati predloge na osnovu bezbjednosti, suvereniteta podataka, troškova i operativnih razmatranja. Ako se predloži cloud rješenje, ono mora biti u skladu sa crnogorskim propisima o rezidentnosti i zaštiti podataka.

●(M) Modularnost i proširivost: Dizajn COTS sistema treba da bude modularan kako bi omogućio buduća poboljšanja i dodavanje novih funkcionalnosti (npr. putem novih modula ili nadogradnji) uz minimalne smetnje. 5.2. Tehnološki stek

●(M) Dokazane i održive tehnologije: COTS sistem treba da koristi dobro uspostavljene, dokazane i održive tehnologije. Prednost će se dati rješenjima koja koriste tehnologije sa jakom podrškom zajednice ili dobavljača i jasnim budućim planom razvoja.

●(D) Otvoreni standardi: Gdje je primjenljivo, prednost će se dati COTS rješenjima koja koriste otvorene standarde kako bi se olakšala interoperabilnost i izbjeglo vezivanje za jednog dobavljača.

●(M) Tehnologija baze podataka: Predložena tehnologija baze podataka koja podupire COTS rješenje mora biti robusna, skalabilna, bezbjedna i sposobna da podnese očekivane obime podataka i transakciona opterećenja u standardnim ANSI SQL RDBMS sistemima. 5.3. Performanse i skalabilnost Sistem mora biti arhitektiran za visoke performanse i skalabilnost kako bi se osiguralo responzivno iskustvo za sve korisnike i kako bi se nosio sa budućim rastom. Dobavljači moraju opisati svoj pristup testiranju performansi i pružiti dokaze o sposobnosti rješenja da ispuni sljedeće minimalne zahtjeve:

●(M) Istovremeno opterećenje korisnika: Sistem mora podržavati, bez pada performansi, najmanje 100 istovremenih internih korisnika SCMN-a i 500 istovremenih eksternih korisnika portala koji obavljaju tipične aktivnosti (npr. unos podataka, pregled izvještaja, interakcija sa kontrolnom tablom).

●(M) Vremena odziva korisničkog interfejsa: Ključne interaktivne funkcije moraju biti visoko responzivne. Na primjer: ○Učitavanje ključnih interaktivnih kontrolnih tabli: ispod 5 sekundi. ○Otvaranje velikih, složenih izvještaja za pregled: ispod 5 sekundi. ○Navigacija od stranice do stranice unutar aplikacije: ispod 2 sekunde.

●(M) Propusnost obrade podataka: Sistem mora efikasno obrađivati podneske podataka. ○Validacija tipičnog velikog regulatornog podneska (npr. XML fajl od 5MB sa nekoliko stotina pravila validacije): ispod 10 sekundi.

●(M) Rukovanje obimom podataka: Sistem mora biti dizajniran da efikasno upravlja i obrađuje velike obime podataka, sa dokazanom skalabilnošću da primi projektovani rast obima podataka i broja korisnika od najmanje 20% godišnje u narednih 5-10 godina bez potrebe za velikim arhitektonskim promjenama.
●(M) Skalabilnost: Arhitektura mora omogućavati vertikalno (dodavanje resursa serveru) i/ili horizontalno (dodavanje više servera) skaliranje resursa kako bi se na predvidljiv i isplativ način zadovoljile rastuće potrebe. 5.4. Bezbjednosni zahtjevi
●(M) Enkripcija podataka: Podaci moraju biti enkriptovani i u mirovanju (u bazi podataka i skladištu fajlova) i u tranzitu (tokom komunikacije između komponenti sistema, korisnika i eksternih subjekata) koristeći jake algoritme enkripcije.
●(M) Autentifikacija i autorizacija: Robusni mehanizmi autentifikacije i autorizacije kojima se upravlja putem enterprise-grade IAM rješenja (prema odjeljku 4.7).
●(M) Usklađenost sa bezbjednosnim standardima: COTS sistem treba da bude razvijen prateći prakse bezbjednog kodiranja (npr. ublažavanje OWASP Top 10) i treba da podrži SCMN u usklađivanju sa relevantnim nacionalnim i međunarodnim standardima informacione bezbjednosti (npr. principi ISO 27001).
●(M) Upravljanje ranjivostima: Dobavljač mora imati jasan proces za identifikaciju i rješavanje bezbjednosnih ranjivosti u svom COTS sistemu i njegovim komponentama, uključujući blagovremeno obezbjeđivanje bezbjednosnih zakrpa.
●(M) Razmatranja o detekciji/prevenciji upada: Sistem treba da bude kompatibilan sa standardnom mrežnom bezbjednosnom infrastrukturom, uključujući firewall-e i sisteme za detekciju/prevenciju upada.
●(M) Bezbjedan životni ciklus razvoja: Dobavljač treba da opiše svoje prakse bezbjednog životnog ciklusa razvoja softvera za svoj COTS proizvod. 5.5. Migracija podataka
●(M) Plan i alati za migraciju podataka: Dobavljač mora pružiti jasan metod, plan i alate (po mogućnosti uključujući standardne alate iz COTS rješenja) za migraciju istorijskih i trenutnih podataka iz postojećih sistema SCMN-a (koje će SCMN specificirati) u novi sistem. Ovo uključuje mapiranje, transformaciju, validaciju i usaglašavanje podataka.
●(M) Podrška tokom migracije: Dobavljač će biti odgovoran za podršku SCMN-u tokom cijelog procesa migracije podataka kako bi se osigurao integritet i potpunost podataka. 5.6. Dostupnost, backup i oporavak od katastrofe
●(M) Rješenje za backup i oporavak: Mora se obezbijediti sveobuhvatno rješenje za backup i oporavak za sistem i njegove podatke, koje omogućava redovne automatske backup-e i blagovremenu obnovu u slučaju kvara.
●(D) Podrška za oporavak od katastrofe (DR): Sistem treba da podržava implementaciju u DR okruženju. Dobavljači treba da opišu mehanizme i procedure za prebacivanje na DR lokaciju i povratak. (SCMN će specificirati svoje DR sposobnosti i zahtjeve) RTO i RPO su definisani na 24h. 5.7. Neproizvodna okruženja
●(M) Obezbjeđivanje testnog okruženja: Dobavljač mora obezbijediti, implementirati, konfigurisati i podržavati najmanje jedno namjensko neproizvodno okruženje (nazvano "Testno okruženje") koje je, koliko je to moguće, funkcionalno ekvivalentno proizvodnom okruženju. Ovo okruženje je ključno za SCMN da: ○Sprovodi temeljno testiranje svih ažuriranja sistema, zakrpa i novih verzija COTS rješenja prije implementacije u proizvodnju. ○Testira nove konfiguracije, prilagođavanja tokova posla i promjene pravila validacije, nakon njihovog internog testiranja i simulacije prema odjeljku 4.2.. ○Validira procese i rezultate migracije podataka. ○Sprovodi sesije obuke korisnika i omogući korisnicima da se upoznaju sa funkcionalnostima sistema. ○Obavlja druge aktivnosti osiguranja kvaliteta i pred-proizvodne validacije bez uticaja na živi operativni sistem.

●(M)Omogući korisnicima SCMN-a da dizajniraju, razvijaju i testiraju nove predloške izvještaja i analitičke modele koristeći ugrađene alate sistema (kako je simulirano interno prema odjeljku 4.2. 6. Implementacija i upravljanje projektom
●(M) Faze projekta: Predlog mora sadržati jasan plan implementacije projekta sa definisanim fazama (npr. početak, dizajn i konfiguracija, testiranje, implementacija, puštanje u rad, podrška nakon puštanja u rad) za COTS rješenje.
●(M) Metodologija projekta: Dobavljač treba da opiše svoju standardnu metodologiju implementacije za predloženo COTS rješenje, detaljno navodeći kako će biti prilagođena okruženju SCMN-a i osigurati blagovremenu i uspješnu isporuku projekta.
●(M) Tim za upravljanje projektom: Dobavljač mora dodijeliti namjenskog menadžera projekta i pružiti detalje o predloženoj strukturi projektnog tima, uključujući uloge, odgovornosti i iskustvo ključnog osoblja, posebno sa implementacijom predloženog COTS rješenja.
●(M) Redovno izvještavanje i komunikacija: Jasan plan za redovno izvještavanje o napretku projekta, sastanke i komunikaciju između dobavljača i SCMN-a.
●(M) Testiranje i osiguranje kvaliteta: Detaljna strategija testiranja, uključujući planove za jedinično testiranje, testiranje integracije sistema, testiranje prihvatanja od strane korisnika (UAT) u namjenskom testnom okruženju i testiranje performansi konfigurisanog COTS rješenja. SCMN će biti aktivno uključen u UAT.
●(M) Upravljanje rizicima: Dobavljač treba da opiše svoj pristup identifikaciji, upravljanju i ublažavanju projektnih rizika povezanih sa implementacijom COTS rješenja.
7. Obuka i prenos znanja
●(M) Sveobuhvatan program obuke: Dobavljač mora pružiti sveobuhvatan program obuke prilagođen različitim korisničkim grupama unutar SCMN-a, fokusirajući se na funkcionalnosti i konfiguracione sposobnosti COTS rješenja: ○Krajnji korisnici: Obuka o svim relevantnim funkcionalnostima, unosu podataka, generisanju izvještaja i samouslužnom dizajnu pomoću ugrađenih alata, korišćenju tokova posla (tokovi obrade podataka), internim procedurama testiranja/simulacije izvještaja i interakciji sa portalom. ○Administratori sistema: Dubinska obuka o konfiguraciji sistema (uključujući tokove posla obrade podataka, pravila validacije, upravljanje životnim ciklusom definicija izvještaja), upravljanju korisnicima putem IAM rješenja (uključujući podešavanje i podršku za 2FA), administraciji bezbjednosti, praćenju, procedurama za backup/oporavak, upravljanju okruženjem (uključujući osvježavanje testnog okruženja) i osnovnom rješavanju problema COTS rješenja. ○Tehničko osoblje/Super-korisnici: Napredna obuka o arhitekturi sistema, strukturi baze podataka (ako je dostupna za izvještavanje), mogućnostima prilagođavanja (ako postoje unutar COTS okvira), alatima za razvoj izvještaja i integracionim tačkama. Ako se predloži željeno napredno BI okruženje, bila bi potrebna i relevantna obuka za specijalizovane korisnike o tim alatima.
●(M) Materijali za obuku: Obezbjeđivanje visokokvalitetnih materijala za obuku (priručnici, vodiči, prezentacije) na engleskom i/ili crnogorskom jeziku, uključujući standardnu COTS dokumentaciju i vodiče za konfiguraciju specifične za SCMN.
●(M) Format obuke: Obuka može biti kombinacija sesija u stilu učionice, praktičnih radionica (koristeći testno okruženje) i programa "obuka za trenere", prema potrebi.
●(M) Prenos znanja: Plan za efikasan prenos znanja na osoblje SCMN-a kako bi se osigurala samoodrživost u radu sistema, konfiguraciji (gdje je primjenljivo, npr. dizajn izvještaja, pravila toka obrade podataka, životni ciklus definicija izvještaja unutar COTS rješenja) i osnovnom održavanju.
●(M) Podrška za obuku nakon implementacije: Dostupnost ad-hoc ili osvježavajućih sesija obuke po potrebi nakon implementacije. 8. Podrška i održavanje •(M) Podrška

nakon implementacije: Dobavljač mora pružiti jasan opis usluga podrške nakon implementacije koje se nude za COTS rješenje. •(M) Ugovori o nivou usluge (SLA): Predloženi SLA-ovi moraju jasno definisati: oRadno vrijeme podrške i kanale za kontakt. oGarantovana vremena odziva za različite nivoe ozbiljnosti problema i to najmanje Kritična greška 4 sata, Ozbiljna greška 16 sati, Mala greška 40 sati (Kritična greška: Korisnik ne može više koristiti Softver zbog greške na nekoj od osnovnih funkcionalnosti Softvera, što ima kritičan uticaj na izvršenje aktivnosti. Takav incident ili zahtjev zahtijeva hitnu intervenciju i otklanjanje iste. Primjeri grešaka ove vrste su: problemi sa podacima ili njihovo uništenje, gubitak podataka. Nema zamjenskog rješenja za incident ili zahtjev, te je za otklanjanje istog potrebna promjena organizacije aplikacije ili velike promjene u aplikaciji. Ozbiljna greška: Korisnik može koristiti Softver, ali je njegova upotreba znatno ograničena. Ozbiljan incident ili zahtjev može biti izbjegnut trenutnim zamjenskim rješenjem. Primjer istog je: prekid ili zastoj, poruke koje korisnika vode pogrešnim putem, greške koje su nastale kao posljedica greške u Softverskom rješenju, ali se dešavaju slučajno ili pod uticajem rijetkih i izuzetnih događaja ili slučajnosti. Mala greška: Korisnik može koristiti Softver, ali je njegova upotreba ograničena, mada je takvog opsega koji nije kritičan u cjelosti. Za primjetne incidente ili zahtjeve postoje odgovarajući zamjenski načini koji ne utiču na mogućnost rješenja. Primjeri istih su: incidenti ili zahtjevi koje čine upotrebu određenih procedura nemogućim, interfejsi koji rade neispravno, smanjena primjenljivost ili kapacitet sistema.). oGarantovana vremena rješavanja ili obezbjeđivanja privremenog rješenja za različite nivoe ozbiljnosti problema i to najmanje Kritična greška 1 radni dan , Ozbiljna greška 2 radna dana, Mala greška 5 radnih dana. oProcedure za eskalaciju problema.

•(M) Tekuće održavanje: Detalji o uslugama održavanja za COTS rješenje, uključujući: oObezbjeđivanje ispravki grešaka, zakrpa i servisnih paketa. oRedovna ažuriranja kako bi se osiguralo da sistem ostane kompatibilan sa osnovnim tehnologijama (npr. operativni sistemi, baze podataka) i usklađen sa planom razvoja proizvoda. o U održavanje treba da bude uključeno makar 10h mjesečno sa akumuliranjem do 6 mjeseci. oZakazani prozori za održavanje i procedure.

•(M) Nadogradnje sistema: Politika i proces za obezbjeđivanje i implementaciju manjih i većih nadogradnji sistema, u skladu sa planom razvoja COTS proizvoda, uključujući nove funkcije i funkcionalnosti.

•(M) Prilagođavanje evoluirajućim regulatornim zahtjevima: Dobavljač mora opisati svoju sposobnost i proces za prilagođavanje COTS sistema promjenama u regulatornim okvirima, standardima izvještavanja (npr. nove taksonomije od nacionalnih ili međunarodnih tijela poput ESMA-e) i pravilima validacije na blagovremen način. Ovo uključuje kako će takve promjene biti isporučene (npr. putem ažuriranja proizvoda, konfiguracionih paketa) i cjenovno određene, kao i u kojoj mjeri SCMN može samostalno konfigurisati takve promjene koristeći sistemske alate.

• (M) "Hypercare" podrška nakon puštanja u rad: "Nakon uspješnog puštanja sistema u rad, dobavljač mora obezbijediti namjenski period 'hypercare' podrške od najmanje 12 nedjelja. Tokom ovog perioda, dobavljač će pružiti povišen nivo podrške, uključujući potencijalno resurse na licu mjesta, brža vremena odziva od standardnih SLA-ova i namjenske članove projektnog tima kako bi se osigurala glatka tranzicija za korisnike SCMN-a, brzo rješavanje bilo kakvih nepredviđenih problema i stabilizacija novog operativnog okruženja. 9. Cloud infrastruktura i tehnički zahtjevi 9.1. Pregled Ovaj odjeljak detaljno opisuje obavezne tehničke i arhitektonske zahtjeve za cloud infrastrukturu na kojoj se predloženo softversko rješenje mora implementirati. Dobavljač je odgovoran za obezbjeđivanje, konfigurisanje i održavanje okruženja koje u potpunosti

ispunjava ove specifikacije. Arhitektura je dizajnirana da osigura najviše nivoe bezbjednosti, skalabilnosti, upravljanja i operativne izvrsnosti, pridržavajući se priznatih industrijskih okvira za usvajanje clouda. Zahtjevi za Cloud usluge: Ukoliko dobavljač predloži rješenje hostovano u cloudu (npr. SaaS, PaaS), sljedeći zahtjevi su obavezni i moraju biti adresirani u predlogu:

•(M) Rezidentnost i obrada podataka: Da bi se uskladilo sa propisima o suverenitetu podataka, svi podaci SCMN-a—uključujući primarne podatke, metapodatke, logove i sve backup-e—moraju boraviti i biti obrađivani isključivo unutar geografskih granica [npr. Evropske unije (EU)]. Dobavljač mora specificirati predložene cloud regione.

•(M) Segregacija okruženja: U bilo kom multi-tenant cloud okruženju, dobavljač mora opisati tehničku arhitekturu i robusne kontrole koje se koriste za osiguranje logičke i, gdje je primjenljivo, fizičke segregacije i kriptografske izolacije podataka, obrade i mrežnog okruženja SCMN-a od svih drugih tenanata.

• (M) Cloud usklađenost i revizije: Predloženi cloud servis provajder i aplikacioni servis dobavljača moraju biti usklađeni sa priznatim međunarodnim bezbjednosnim standardima. Dobavljač mora pružiti dokaze o usklađenosti, kao što su trenutni sertifikati ili izvještaji o reviziji trećih strana, za standarde uključujući, ali ne ograničavajući se na, ISO 27001, ISO 27017 (Cloud bezbjednost).

•(M) Izlazna strategija: Dobavljač mora pružiti sveobuhvatan plan izlaska i povezane alate. U slučaju raskida ugovora, dobavljač mora podržati potpun i blagovremen izvoz svih podataka SCMN-a (uključujući sve podneske, korisničke podatke, konfiguracije, revizorske tragove i metapodatke) u otvorenom, nevlasničkom i mašinski čitljivom formatu (npr. XML, JSON, CSV fajlovi u strukturiranoj hijerarhiji). Dobavljač mora opisati ovaj proces, uključujući očekivane vremenske okvire i sve povezane troškove. Dobavljač se obavezuje da kompletan izvorni kod softverskog rješenja bude deponovan kod ovlašćene escrow agencije, uz pravo SCMN-a da, u slučaju prestanka poslovanja Dobavljača, stečaja ili nemogućnosti ispunjenja ugovornih obaveza, preuzme izvorni kod radi nesmetanog korišćenja i održavanja sistema. 9.2. Opšti arhitektonski principi Infrastruktura mora biti dizajnirana prema sljedećim osnovnim principima:

●Platforma-kao-servis (PaaS) na prvom mjestu: Arhitektura će prioritetno koristiti upravljane PaaS servise u odnosu na Infrastrukturu-kao-servis (IaaS) kako bi se smanjilo administrativno opterećenje i iskoristile nativne cloud skalabilnosti i bezbjednosne funkcije. ●Bezbjednost-po-dizajnu: Bezbjednost će biti osnovna komponenta arhitekture, sa više slojeva zaštite i proaktivnim praćenjem prijetnji ugrađenim u cijelo okruženje.

●Skalabilnost i elastičnost: Sistem mora biti u stanju da automatski ili na zahtjev skalira resurse kako bi efikasno prilagodio promjenljiva radna opterećenja i obime podataka.

●Visoka dostupnost: Arhitektura mora biti potpuno otporna bez ijedne tačke kvara, osiguravajući kontinuitet poslovanja za sve kritične nadzorne funkcije. 9.3. Cloud upravljanje i organizacija

●Logička hijerarhija: Mora se uspostaviti logička hijerarhija resursa kako bi se organizovala okruženja (npr. proizvodno, staging, razvojno) za efikasno upravljanje i razdvajanje dužnosti. ●Označavanje resursa: Mora se implementirati sveobuhvatna politika označavanja za sve cloud resurse kako bi se omogućilo efikasno upravljanje troškovima, izvještavanje i praćenje resursa.

●Upravljanje zasnovano na politikama: Okruženje mora koristiti mehanizam za sprovođenje politika kako bi se automatski primjenjivala i revidirala bezbjednosna, usklađenosna i konfiguraciona pravila na svim resursima. Ovo uključuje ograničavanje implementacija na odobrene geografske regione i sprovođenje upotrebe enkripcije

podataka. 9.4. Mrežna arhitektura (Hub-and-Spoke model) Rješenje mora biti implementirano unutar "hub-and-spoke" virtuelne mrežne topologije kako bi se osigurala mrežna izolacija, centralizovana bezbjednost i skalabilnost.

●Centralna Hub mreža: Namjenska virtuelna mreža koja djeluje kao centralna tačka za povezivanje i dijeljene servise. Mora sadržati: ○Upravljani, cloud-nativni Next-Generation Firewall (NGFW). ○Bezbjedan gateway za povezivanje sa on-premise mrežom Komisije. ○Bezbjedan servis za daljinski pristup (npr. bastion host) za administratore.

●Radne Spoke mreže: Dvije ili više izolovanih virtuelnih mreža ("spokes") će se koristiti za implementaciju komponenti sistema i biće povezane sa centralnim hub-om. Ovo mora uključivati, najmanje: ○DMZ/Perimeter Spoke: Za hostovanje eksterno okrenutih komponenti dostupnih sa interneta putem Layer-7 load balancera. ○Interni/Infrastrukturni Spoke: Za hostovanje osnovne aplikacione logike, baza podataka i drugih internih backend komponenti, bez direktnog pristupa internetu.

●Tok i inspekcija saobraćaja: Sav saobraćaj između spoke mreža, kao i sav saobraćaj ka i sa interneta i on-premise mreže, mora biti rutiran i pregledan od strane centralnog firewall-a u hub mreži. Ovo će se sprovoditi putem prilagođenih mrežnih politika rutiranja. 9.5. Mrežni bezbjednosni servisi

●Upravljani Next-Generation Firewall (NGFW): Stateful, upravljani firewall servis sa integracijom obavještajnih podataka o prijetnjama, sposoban da filtrira saobraćaj na osnovu mrežnih i aplikacionih pravila (npr. po IP adresi, portu i FQDN).

●Web Application Firewall (WAF): Upravljani WAF mora štititi sve web-okrenute aplikacije od uobičajenih web ranjivosti i eksploatacija, kao što su one u OWASP Top 10.

●DDoS zaštita: Virtuelne mreže moraju biti zaštićene enterprise-grade servisom za ublažavanje distribuiranih napada uskraćivanjem usluge (DDoS).

●Bezbjedan administrativni pristup: Rješenje mora pružiti bezbjedan metod za administrativni pristup (npr. RDP/SSH) koji ne uključuje izlaganje portova za upravljanje direktno javnom internetu, koristeći upravljani bastion ili jump-host servis. 9.6. Povezivanje ●Site-to-Site (S2S) VPN: Mora se uspostaviti bezbjedan, enkriptovan VPN tunel između cloud okruženja i on-premise mreže Komisije koristeći IKEv2 protokole.

●Point-to-Site (P2S) VPN: Mora biti dostupan bezbjedan VPN rješenje za ovlašćene udaljene korisnike, sa autentifikacijom integrisanom u centralni provajder identiteta Komisije. 9.7. Računarska i aplikaciona platforma

●Serverless kontejnerska platforma: Primarni model implementacije za mikroservise aplikacije mora biti serverless platforma za orkestraciju kontejnera. Ova platforma mora podržavati: ○Implementaciju u privatnu, izolovanu virtuelnu mrežu. ○I potrošačke (serverless) i namjenske računarske profile za fleksibilno skaliranje. ○Nativnu integraciju sa centralizovanim servisima za evidentiranje. ○Sposobnost montiranja perzistentnog skladišta sa upravljanog file servisa.

●Virtuelne mašine: Za sve komponente koje nisu pogodne za kontejnerizaciju, mogu se koristiti virtuelne mašine. Ove VM moraju koristiti operativni sistem sa podrškom za automatsko, minimalno remetilačko bezbjednosno krpljenje ("hotpatching"). 9.8. Servisi za skladištenje i baze podataka

●Upravljani relacioni servis baze podataka (PaaS): Osnovna baza podataka sistema mora biti potpuno upravljani, visoko dostupni relacioni servis baze podataka (PaaS). Mora sadržati: ○Implementaciju unutar privatne virtuelne mreže bez javne krajnje tačke. ○Integraciju sa centralnim provajderom identiteta Komisije za autentifikaciju. ○Ugrađenu visoku dostupnost i automatske, zonski redundantne backup-e. ○Napredne sposobnosti zaštite od prijetnji. ○Sprovođenje TLS 1.2 ili više za sve konekcije.

●Upravljani servis za dijeljenje fajlova: Rješenje mora uključivati potpuno upravljani servis za skladištenje fajlova dostupan putem standardnih mrežnih protokola (npr. SMB). Mora podržavati različite nivoe performansi i bezbjedan pristup iz privatnih virtuelnih mreža. 9.9. Bezbjednost, usklađenost i identitet
●Cloud bezbjednosni položaj i zaštita radnog opterećenja: Okruženje mora biti zaštićeno jedinstvenom platformom za upravljanje bezbjednošću. Ova platforma mora pružati: ○Kontinuiranu procjenu bezbjednosti u odnosu na industrijske benčmarke (npr. CIS, NIST, ISO 27001). ○Detekciju prijetnji za računarske, skladišne i workloads baza podataka. ○Prioritizovana bezbjednosna upozorenja i preporuke za sanaciju koje se mogu primijeniti. ●Upravljanje identitetom i pristupom (IAM): Sav pristup mora biti upravljan od strane centralnog provajdera identiteta, sprovodeći princip najmanjih privilegija koristeći kontrolu pristupa zasnovanu na ulogama (RBAC).
●Višefaktorska autentifikacija (MFA): MFA mora biti sprovedena za sve korisnike sa administrativnim ili privilegovanim pristupom.
●Enkripcija podataka: Svi podaci moraju biti enkriptovani i u mirovanju i u tranzitu koristeći jake, industrijski standardne kriptografske algoritme. 9.10. Praćenje, evidentiranje i revizija ●Centralizovano praćenje i evidentiranje: Mora se implementirati centralizovana platforma za prikupljanje, skladištenje i analizu logova i metrika performansi sa svih aplikacionih i infrastrukturnih komponenti.
●Analitika i kontrolne table: Platforma mora pružiti moćan jezik za upite za dubinsku analizu i podržavati kreiranje real-time kontrolnih tabli za operativnu vidljivost.
●Upozoravanje: Mora se konfigurisati mehanizam za upozoravanje kako bi se proaktivno obavještavali administratori o problemima sa performansama, bezbjednosnim događajima i operativnim anomalijama.
●Revizorski tragovi: Sistem mora održavati sveobuhvatne i nepromjenljive revizorske tragove svih korisničkih aktivnosti i administrativnih akcija. 9.11. Backup i oporavak od katastrofe
●Upravljani servis za backup: Mora se konfigurisati centralizovani, upravljani servis za backup kako bi se automatski pravile rezervne kopije svih kritičnih komponenti, uključujući virtuelne mašine, baze podataka i dijeljene fajlove.
●Testiranje: Dobavljač mora sprovoditi i dokumentovati periodične testove obnove backup-a kako bi se osigurao integritet podataka i mogućnost oporavka. 10. Rječnik / Definicije ●2FA: Dvofaktorska autentifikacija
●API: Aplikacioni programski interfejs
●BI: Poslovna inteligencija
●COTS: Komercijalno gotovo rješenje
●CSV: Vrijednosti odvojene zarezom
●DR: Oporavak od katastrofe
●ESEF: Jedinstveni evropski elektronski format
●ESMA: Evropska agencija za hartije od vrijednosti i tržišta
●EWS: Sistem ranog upozoravanja
●HOTP: Jednokratna lozinka zasnovana na HMAC-u (u skladu sa RFC 4226)
●IAM: Upravljanje identitetom i pristupom
●KRI: Ključni indikator rizika
●MFA: Višefaktorska autentifikacija (uključuje 2FA)
●OCR: Optičko prepoznavanje znakova
●OIDC: OpenID Connect
●OWASP: Open Web Application Security Project
●RBAC: Kontrola pristupa zasnovana na ulogama

- RegTech: Regulatorna tehnologija
- RPO: Ciljna tačka oporavka
- RTO: Ciljno vrijeme oporavka
- SAML: Jezik za označavanje bezbjednosnih tvrdnji
- SCMN: Komisija za tržište kapitala Crne Gore
- SLA: Ugovor o nivou usluge
- SupTech: Nadzorna tehnologija
- Sistem: Softversko rješenje za nadzor koje se nabavlja
- TOTP: Jednokratna lozinka zasnovana na vremenu (u skladu sa RFC 6238)
- UAT: Testiranje prihvatanja od strane korisnika
- XBRL: Proširivi jezik za poslovno izvještavanje
- XML: Proširivi jezik za označavanje.

Član 2

Rok izvršenja ugovora je 6 mjeseci od dana potpisivanja ugovora, uključujući faze analize, dizajna, implementacije, testiranja i obuke.

Mjesto izvršenja ugovora: Na teritoriji Crne Gore.

Član 3

Ukupna vrijednost usluga, prema prihvaćenoj ponudi broj: 140776 od 23.09.2025. godine, iznosi **149.900,00 eura bez uračunatog PDV-a.**

PDV: 00,00 €

Rok plaćanja je: 30 dana od dana obostrano potpisanog zapisnika o prijemu svake od ugovorenih faza i ispostavljene fakture.

Način plaćanja je: virmanski.

Član 4

Izvršilac se obavezuje:

- da rukovodi izvršenjem svih usluga;
- da obezbijedi kompletnu dokumentaciju po kojoj se izvode usluge;
- da snosi troškove naknade korišćenja patenata i odgovoran je za povredu zaštićenih prava intelektualne svojine trećih lica,
- da u slučaju problema utvrdi nivo problema sa Naručiocem, i u skladu sa istim uskladi vrijeme odziva i restauraciju,

Garantni rok za isporučeno softversko rješenje je 12 mjeseca od dana primopredaje sistema.

Garantni rok obuhvata otklanjanje svih grešaka (bug-ova) i tehničku podršku.

GARANCIJA ZA DOBRO IZVRŠENJE UGOVORA
Član 5

Dobavljač se obavezuje da Naručiocu u trenutku potpisivanja ovog Ugovora preda neopozive, bezuslovne i naplative na prvi poziv garanciju za dobro izvršenje ugovora, za slučaj povrede ugovorenih obaveza u iznosu od 10 % od vrijednosti ugovora.

Garancija za dobro izvršenje ugovora treba da važi deset dana duže od roka trajanja ugovora.

Navedenu garanciju Naručilac može aktivirati u svakom momentu kada nastupi neki od razloga za raskid ovog Ugovora.

Član 6

Ugovorne strane su saglasne da do raskida ovog Ugovora može doći ako Izvršilac ne bude izvršavao svoje obaveze u rokovima i na način predviđen Ugovorom.

Naručilac je obavezan da u slučaju uočavanja propusta u obavljanju posla pisanim putem pozove Izvršioca i da putem Zapisnika zajednički konstatuju uzrok i obim uočenih propusta.

Kontrole kvaliteta usluge se vrši preko ovlašćenih lica Naručioca, sačinjavanjem i potpisivanjem Izvještaja o realizovanim aktivnostima.

Član 7

Za sve što nije definisano ovim Ugovorom primjenjivaće se odredbe Zakona o obligacionim odnosima.

Član 8

Ukoliko u toku trajanja ovog ugovora dođe do bilo kakvih promjena u nazivu ili drugim statusnim promjenama ugovornih strana, tada će sva prava i obaveze ugovorne strane kod koje dođe do takve promjene, preći na njenog pravnog sljedbenika.

Član 9

Izvršilac se obavezuje da u toku trajanja ovog Ugovora, kao i po isteku istog, ne iznose bilo kakve službene ili povjerljive informacije u vezi ovog Ugovora, poslova i aktivnosti Naručioca, bez prethodne pisane saglasnosti Naručioca.

Član 10

Ugovorne strane su saglasne da eventualne sporove povodom ovog ugovora rješavaju sporazumom. U protivnom, sve sporove koji nastanu u vezi sa ovim Ugovorom rješavaće Privredni sud u Podgorici.

Član 11

Ugovor o javnoj nabavci koji je zaključen uz kršenje antikorupcijskih pravila u skladu sa odredbama člana 38 Zakona o javnim nabavkama, ništav je.

Član 12

Ovaj ugovor je zaključen i potpisan od ovlašćenih zakonskih zastupnika strana ugovora i sačinjen je u 6 (šest) istovjetnih primjeraka, od kojih su 3 (tri) primjerka za NARUČIOCA a 3 (tri) primjerka za IZVRŠIOCA.

NARUČILAC
Željko Drinčić,
Predsjednik Komisije

IZVRŠILAC
Dragan Oremuš,
direktor

COMPLIANT RISK TECHNOLOGY LLC
VATID: HR30872422309
Croatia EU

CRNA GORA
KOMISIJA ZA KONTROLU POSTUPAKA JAVNIH NABAVKI
Primljeno: 29.10.2025
Org.jed.:
01/9-1042/10-25