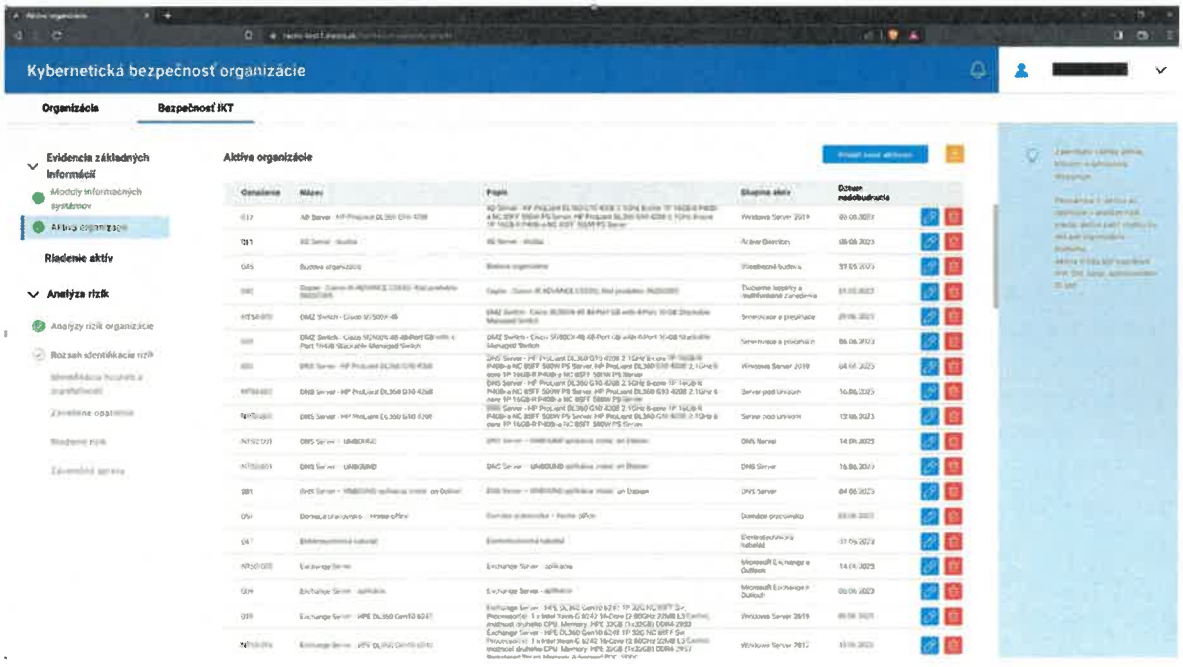
Z hľadiska bezpečnosti IS bude disponovať aj:

- personalizáciou užívateľských účtov,
- naplnenými číselníkmi,
- monitoringom prístupov k aplikácii,
- funkciou importu údajov,
- funkciou pre zálohy a obnovu databáz,
- prehľadmi a štatistikami,
- správou zo servisu a užívateľským helpdeskom,
- konfiguráciou emailových klientov na zasielanie upozornení mimo aplikácie

Informácie o produkte: CyberSec+ a modul KBO ISIT software SK:

- Tenký klient (TK) *CyberSec+* :
  - Web nadstavba pre modul KBO (kybernetická bezpečnosť organizácie).
  - Aktuálna verzia softvéru je 1.0.2
  - Vlastník majetkových a predajných práv, výrobca : Inezis Identity Solutions, s.r.o., Sekurisova 16, Bratislava – mestská časť Dúbravka 841 02
  - Slovenský produkt.



- Tlstý/Tučný/Hrubý klient (HK):
  - Identifikácia softvérovej aplikácie : ISIT SOFTWARE SK (jazykové a právne prostredie pre SR)
  - *modul KBO* (kybernetická bezpečnosť organizácie).
  - Aktuálna verzia softvéru je 3.19
  - Vlastník majetkových a predajných práv, výrobca : ISIT Slovakia s.r.o., Klincová 37 82108 Bratislava

Príloha č. 1 - Špecifikácia Diela a návrh riešenia Zhotoviteľa

Modul A: Nasadenie informačného systému pre identifikáciu a riadenie rizík

Spoločnosť NESS Slovensko, a.s. ponúka dodanie a implementáciu hotového „slovenského" riešenia pre riadenie kybernetickej bezpečnosti organizácie.

Riešenie riadenia KBO s CyberSec+ (Web nadstavba pre modul KBO) umožňuje zabezpečiť legislatívny súlad s požiadavkami zákona č. 69/2018 Z. z ., Vyhlášky č. 362/2018 Z. z., zákona č. 95/2019 Z. z., ako aj so štandardami ISO/IEC 2700x.

IS Riadenia rizík umožní koncovému zákazníkovi realizovať:

- správa aktív – vedenie zoznamu aktív subjektu, vrátane ich vlastníkov
- správa zraniteľností – vedenie zoznamu rozpoznaných zraniteľností, vrátane ich vlastníkov
- správa hrozieb – vedenie zoznamu rozpoznaných hrozieb
- správa opatrení – vedenie zoznamu opatrení potrebných na potlačenie zraniteľností
- správa vzťahov – evidencia rozpoznaných vzťahov medzi aktívami a zraniteľnosťami
- správa rizík – identifikácia a ohodnotenie rizík na základe pravdepodobností hrozieb, uplatňovaných opatrení a dopadov na subjekt
- semikvantitatívnu metódu hodnotenia významnosti rizík
- číselné ohodnotenie pravdepodobnosti hrozieb a účinnosti opatrení

Mimo požadovaných funkčných vlastností, zákazník získa aj podmoduly:

- Evidencia základných informácií o prevádzkovateľovi základnej služby
- Riadenie tretích strán – zahrňuje evidenciu tretích strán, evidenciu uzavretých zmlúv a NDA, špecifikáciu a rozsah bezpečnostných opatrení prijatých treťou stranou a iné.
- Personálna bezpečnosť: zahrňuje evidenciu zamestnancov organizácie, evidenciu zamestnancov tretích strán pristupujúcich k informačným systémom organizácie, evidenciu zodpovedností zamestnanca a iné.
- Manažérska konzolu pre relácie aktív - podpora pre modifikáciu a pridávanie používateľom definované relácie medzi aktívom, hrozbou, jej zraniteľnosťami a nápravnými opatreniami
- Manažment bezpečnostných incidentov s výstupmi na dozorné orgány - zahrňuje evidenciu a riadenie incidentov kybernetickej bezpečnosti, evidenciu riešení, nápravných opatrení a výsledkov opatrení kybernetického bezpečnostného incidentu, generovanie hlásenia závažného kybernetického incidentu podľa šablóny NBÚ (SK-CERT).
- Audit opatrení a matica RASCI
- Fyzická a objektová bezpečnosť

IS Riadenia rizík bude pre užívateľov dostupný:

- v slovenskej lokalizácií
- vo forme tučného klienta ako aj tenkého klienta cez webový prehliadač bez špeciálnych nárokov. Pričom podmoduly IS Riadenia rizík budú súčasťou tučného klienta.
- so schopnosťou generovania zostáv vo formáte PDF
- s ohľadom na citlivosť údajov, prístup k systému a dátam bude riadený.

- Slovenský produkt.

Súčasťou dodávky je časovo neobmedzená licencia informačného systému ISIT Software SK, modul KBO pre identifikáciu a riadenie rizík pre počet používateľov podľa zadania, vrátane implementácie na serveroch verejného obstarávateľa a zaškolenia používateľov.

Podpora výrobcu po dobu 36 mesiacov.

Požadované prostredie :

Strana Klient: stanica s OS Windows 10 a novší pre nastavenie a podpora prehliadačov Microsoft Edge, Chrome,...

Strana Server: Windows Server Standard 2019 a novší s IIS/Linux s PHP, .Net, MS SQL Express, Keycloak, Docker desktop resp. podľa aktuálne verzie produktu v čase.

Opis funkcionality:

a) Legislatívne kritériá
   - Legislatívny súlad s požiadavkami zákona č. 69/2018 Z. z ., Vyhlášky č. 362/2018 Z. z., zákona č. 95/2019 Z. z., ISO/IEC 2700x so základným balíkom opatrení (114) a rozšíreným balíkom opatrení (850)
   - Povinnosť dodržiavania súladu s platnou legislatívou (Legislatíva SK, Medzinárodné normy) zabezpečená formou pravidelného maintenance prostredníctvom aktualizácií

b) Obsahové kritériá
- Platforma na správu, riadenie a analýzy procesov v oblasti kybernetickej bezpečnosti s customizáciou v prostredí objednávateľa
- Samostatné podmoduly pre :
  - Evidenciu základných informácií o prevádzkovateľovi základnej služby
  - Riadenie tretích strán:
    - evidencia tretích strán,

- evidencia uzavretých zmlúv a NDA,
- špecifikácia a rozsah bezpečnostných opatrení prijatých treťou stranou,
- riadenie prístupov zamestnancov tretích strán k informačným systémom a/alebo k ich častiam,
- evidencia zmlúv s tretími stranami

- Personálnu bezpečnosť:
  - evidencia zamestnancov organizácie,
  - evidencia zamestnancov tretích strán pristupujúcich k informačným systémom organizácie,
  - evidencia absolvovaných školení zo strany zamestnancov,
  - evidencia prístupov zamestnancov organizácie/tretích strán ku komponentom informačných systémov organizácie,
  - evidencia prístupov, kompetencií / oprávnení a úloh zamestnancov vo vzťahu k informačným systémom organizácie,
  - evidencia zodpovedností zamestnanca
- Evidenciu a riadenie aktív
  - evidencia aktív organizácie,
  - evidencia vlastníkov aktív organizácie,
  - vrátane podpory funkcie importu informačných aktív zo súboru formátu .xlsx, .csv, .xml
- Manažment rizík:
  - vedenie zoznamu hrozieb,
  - vedenie zoznamu zraniteľností vo väzbe na príslušné aktíva a hrozby resp. druhy aktív,
  - identifikácia a ohodnotenie rizík, určenie vektora dopadov,
  - automatizovaný proces analýzy rizík podľa zvoleného bezpečnostného modelu súladného s konkrétnou legislatívou:
    - zákonom č. 69/2018 Z. z., a Vyhláškou NBÚ č. 362/2018 Z. z.;
    - zákonom č. 95/2019 Z. z., a Vyhláškou UPVII č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy;
    - ISO/IEC 2700x so základným balíkom opatrení (114) alebo rozšíreným balíkom opatrení (850) + kombináciou best practices
  - v procese analýze rizík sú použité prvky semikvantitatívnej (zmiešanej) metódy s implementovanými fázami:
  - - Stanovenie jednotného indexu rizika so stanovením 4 úrovní závažnosti rizika a stanovením jednotlivých rozpätí pre tieto úrovne,
  - - Identifikácia relevantných zraniteľností a hrozieb
  - - Posúdenie rizika so stanovením 4 úrovní pre

- a) určenie hodnoty pravdepodobnosti jednotlivých hrozieb v súvislosti s daným aktívom,
- b) určenie hodnoty dopadu jednotlivých hrozieb v súvislosti s daným aktívom,
- c) výpočet úrovne závažnosti výsledných rizík (vyjadrený číselne),
- d) klasifikácia úrovní závažnosti rizík.;

- Metodika analýzy rizík vychádza z Metodiky NBÚ pre analýzu rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

- automatizovaný proces analýzy rizík obsahuje jednak automatizované pridelenie hrozieb, zraniteľností a ochranných opatrení ku každému aktívu/skupine aktív, katalóg rizík s prehľadmi vrátane pridelenia jedinečného ID pre každé generované riziko, identifikáciu následkov/dopadov s prehľadmi hrozieb, zraniteľností, dopadov CIA, hodnôt aktíva, pravdepodobnosti a miery rizika, riadenie rizík s vyhodnotením rizika prijatie zostatkových rizík, viazanosti vlastníka s aktívami a ich opatreniami, monitorovanie rizík. Z AR je možnosť generovať exporty vo formátoch pdf, word – zoznamy prvkov bezpečnosti, prehľad viazanosti k vlastníkom aktív - vlastník, aktívum, opatrenie a jeho realizácia a generovať súborný dokument Záverečná správa obsahujúci minimálne Správu KB, závery z Analýzy rizík, Vyhlásenie o aplikovateľnosti, Legislatívne východiská, použitá metodika a iné;
- proces riadenia rizík obsahuje priradenie osoby zodpovednej za
  - zavedenie nápravného opatrenia,
  - priradenie osoby zodpovednej za prijatie rizika,
  - priradenie osoby zodpovednej za prenos rizika,
  - priradenie osoby zodpovednej za spoločné znášanie rizika,
  - priebežné sledovanie stavu implementovania nápravných opatrení,
- priradenie lehôt na riešenie, prijatie, prenos a zdieľanie rizika

- Manažérsku konzolu pre relácie aktív
  - podpora pre modifikáciu a pridávanie používateľom definované relácie medzi aktívom, hrozbou, jej zraniteľnosťami a nápravnými opatreniami
- Manažment bezpečnostných incidentov s výstupmi na dozorné orgány
  - Evidencia a riadenie incidentov kybernetickej bezpečnosti, Evidencia riešení, nápravných opatrení a výsledkov opatrení kybernetického bezpečnostného incidentu, Generovanie hlásenia závažného kybernetického incidentu podľa šablóny NBÚ (SK-CERT).
- Audit opatrení a matica RASCI
- Fyzickú a objektovú bezpečnosť

- Samostatná funkcionalita Príjem a spracovanie bezpečnostných upozornení NBU na aktuálne hrozby a zraniteľnosti s detekciou aktív v systéme s určením ochranných opatrení a upozornením pre

definované osoby v systéme – bezpečnostné varovania do manažmentu bezpečnostných varovaní nám distribuuje SK CERT NBÚ.

- Produkt disponuje personalizáciou užívateľských účtov, naplnenými číselníkmi, monitoringom prístupov k aplikácii, funkciou importu údajov, funkciou pre zálohy a obnovu databáz, prehľadmi a štatistikami, správou zo servisu a užívateľským helpdeskom, konfiguráciou emailových klientov na zasielanie upozornení mimo aplikácie

c) Systémové kritériá

- Príjem aktuálnych správ a upozornení do informačného servisu aplikácie
- Systém automatických aktualizácií aplikácie; zmeny aplikácie sú riadené formou verziovania
- Systém záloh a obnovy databázy zo zálohy
- Monitoring prístupov k aplikácii
- Funkcie a ovládacie prvky (vrátane vypĺňateľných polí) poskytujú priamo na mieste nápovedu resp. pomocné vysvetlivky pre užívateľa
- Používateľský manuál je v slovenskom jazyku a priamo integrovaný a elektronicky sprístupnený v systéme
- Funkcionalita aplikácie je prispôsobená na priamy príjem dokumentácie, ktorá je určená špeciálne pre danú organizáciu
- Databázy sú napĺňateľné manuálne a aj automatizovane prostredníctvom importov z určených formátov; Import záznamov do číselníkov z viacerých druhov vzorových databáz
- Systémové prvky : Monitoring, Oprávnenia, Nastavenia aplikácie, Importy, Záloha a obnova databázy, Licencovanie, Technická / Zákaznícka pomoc, TeamViewer, Nové vo verziách, Správa dokumentov
- Funkčné a ovládacie prvky : Vyhľadávanie podľa konkrétnych kritérií vrátane filtrov, Tlač, Editačné položky

Bezpečnosť dát aplikácie z hľadiska ich umiestnenia sa plne riadi bezpečnostnou politikou prevádzkovateľa, prevádzkovateľ určí miesto uloženia, resp. prevádzkovania databázy aplikácie

Pre dosiahnutí kvality rizikovej analýzy, je požadovaná súčinnosť zo strany objednávateľa a poskytnutie všetkých požadovaných informácií zo strany dodávateľa vo fáze analýzy, v termíne T+2dni.

Modul B: Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností (BCM)

Modul BCM bude riešiť interné procesy a dokumentáciu pre riadenie kontinuity činnosti. Objednávateľ obdrží v elektronickej a/alebo papierovej podobe Riadiacu dokumentáciu na zabezpečenie kontinuity riadenia kybernetickej bezpečnosti, v súlade so zákonom č. 69/2018 Z. z., a Vyhláškou NBÚ č. 362/2018 Z. z.

Dokumentácia BCM bude definovať scenáre rôznych udalostí, na základe analýz (Riziková zo SW, Rozdielová), ktoré potencionálne môžu mať negatívny vplyv na bežné činnosti organizácie ako sú napríklad:

- náhla nedostupnosť personálu či nepoužiteľnosť pracoviska/budovy,
- nedostupnosť technologickej infraštruktúry či potrebných médií,

- incident či živelná katastrofa.

V rámci kontinuity činností budú stanovené požiadavky na zdroje na základe analýz (Riziková zo SW, Rozdielová), (adekvátne finančné, materiálno-technické a personálne zdroje), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností. V zmysle požiadaviek zákona o kybernetickej bezpečnosti bude určené čo bude:

- hlavným cieľom plánu kontinuity s ohľadom na riadenie incidentov v prípade katastrofy alebo iného rušivého incidentu a ako sa obnovia činnosti v stanovených termínoch,
- strategickým imperatívom procesu riadenia kontinuitu s ohľadom na predchádzanie ďalším stratám.

Súčasťou kontinuity činností bude vypracovanie analýzy funkčných dopadov a kvalifikácia potencionálnych dopadov a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie. Požiadavkou analýzy funkčného dopadu bude určenie:

- cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb,
- cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby.

Kontinuitou budú zavedené postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujúce najmenej:

a) frekvenciu a rozsah zdokumentovania a schvaľovania obnovy záloh,
b) určenie osoby zodpovednej za zálohovanie,
c) časový interval, identifikáciu rozsahu údajov, zadefinovanie dátového média zálohovania a zabezpečenie vedenia dokumentácie o zálohovaní,
d) umiestnenie záloh v zabezpečenom prostredí s riadeným prístupom
e) požiadavku šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,
f) požiadavku výkonu pravidelného preverenia záloh na základe vypracovaného plánu, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.

Modul riadenia kontinuity činností bude obsahovať minimálne:

- plán kontinuity na stanovenie požiadaviek a zdrojov,
- plán reakcie na incidenty,
- politiku a ciele kontinuity,
- analýzu funkčných dopadov,
- stratégiu riadenia kontinuity vrátane evakuačných postupov,
- plány havarijnej obnovy prevádzky,
- plán údržby a kontroly BCMS.

Pre dosiahnutie požadovanej kvality organizačných opatrení (dokumentácie)pre oblasť riadenia kontinuity činnosti, je požadovaná súčinnosť zo strany objednávateľa a poskytnutie všetkých požadovaných informácií zo strany dodávateľa vo fáze analýzy, v termíne T+2dni.

Príloha č. 2 - Doba plnenia Diela, časový harmonogram

Harmonogram realizácie projektu:

Nadobudnutie účinnosti zmluvy – T. Údaje sú uvedené v pracovných dňoch SR

	Aktivita	Začiatok aktivity Mesiac/rok	Koniec aktivity Mesiac/rok
Hlavné aktivity	Analýza a dizajn	T+1	T+19
	Dodávka technológií	T+6	T+19
	Implementácia a testovanie	T+6	T+39
	Nasadenie	T+29	T+50