**ČASŤ B1. OPIS PREDMETU ZÁKAZKY**

1. **Úvodné slovo do problematiky**

Cieľom projektu je do prostredia Úradu pre reguláciu hazardných hier zaviesť optimalizáciu procesov riadenia kybernetickej bezpečnosti, riadenie rizík, kontinuity činností, riadenie incidentov pomocou finančných prostriedkov z dopytovej výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“. Po implementácii projektu bude proces zavedený a ďalej vykonávaný internými zamestnancami, predovšetkým manažérom kybernetickej a informačnej bezpečnosti a ďalším bezpečnostnými zamestnancami. Hlavným výsledkom realizácie projektu bude realizácia a optimalizácia procesov riadenia kybernetickej bezpečnosti, analýza rizík, riadenie rizík, kontinuity činností, riadenie incidentov, spracovanie stratégie informačnej a kybernetickej bezpečnosti a politiky informačnej bezpečnosti (ďalej len „služby riadiacej bezpečnostnej dokumentácie a procesov riadenia informačnej a kybernetickej bezpečnosti“) do prostredia Úradu pre reguláciu hazardných hier. Aktuálne Úrad pre reguláciu hazardných hier nemá implementované riešenia na komplexné opatrenia kybernetickej bezpečnosti povinné v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe. Z externého pohľadu sa zvyšuje frekvencia a závažnosť útokov, z interného pohľadu sa zase neustále zvyšuje závislosť na informačných aktívach a IT systémoch. Zvyšujú sa teda hrozby, zraniteľnosti a následne aj dopady bezpečnostných incidentov a preto je potrebné zvýšiť úroveň a kvalitu poskytovaných IT služieb a aj procesov riadenia kybernetickej bezpečnosti.

Pre projekt zvýšenia úrovne kybernetickej bezpečnosti sú potrebné nasledovné aktivity.

* Klasifikácia informácií a kategorizácia sietí a informačných systémov
* Smernica o bezpečnej prevádzke IS a sietí
* Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP
* Vykonanie analýzy rizík a analýzy dopadov
* Návrh katalógu rizík a spôsobov ich riadenia
* Klientsky modul evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov. Tento modul reprezentuje nástroja na evidenciu procesov pre riadenie kybernetickej bezpečnosti, rizík, zraniteľností a hrozieb.
* Plán ľudských zdrojov
* Nastavenie politík v prostredí úradu
* Vypracovať analýzu funkčnej závislosti všetkých aktív na základnú službu
* Zaviesť metodiku riadenia celého životného cyklu všetkých aktív
* Zaviesť procesy na výkon riadenia aktív a rizík a tak isto implementácia nástroja na riadenie rizík a politík v organizácií URHH.
* Vytvoriť a formalizovať postupy pri zaradení osoby do bezpečnostných rolí, presunu práv, povinností a zodpovedností vo vzťahu ku kybernetickej bezpečnosti na inú osobu a nastaviť úlohy, povinnosti a zodpovednosti pri týchto postupoch
* Vypracovať plán rozvoja bezpečnostného povedomia a pravidelného vzdelávania zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov a tento plán vykonávať v praxi vo forme úvodného školenia, preškolenia pri zmene pracovnej pozície alebo pravidelného ročného školenia formou e-learningu a o absolvovaní týchto školení uchovávať záznam.
* Vytvoriť a formalizovať pravidlá a postupy na riešenie prípadov porušenia bezpečnostnej politiky zo strany používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov
* Vytvoriť a formalizovať postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu s používateľom, administrátorom, s osobou zastávajúcou niektorú z bezpečnostných rolí umožňujúcich presun práv, povinností a zodpovedností na inú novú osobu.
* Vytvoriť a formalizovať postupy na obmedzenie alebo odňatie prístupových oprávnení a privilégií v prípade porušenia bezpečnostných politík vybranými pozíciami v spoločnosti.
* Vypracovať analýzu dopadov definovaných havarijných scenárov na základnú službu a jej komponenty.
* Definovať jednotlivé požiadavky na RTO, RTO a iné a aplikovať ich do postupov a technologických procesov zálohovania a testovania obnovy.
* Zaviesť požiadavky vyplývajúce z plánov obnovy aj do dodávateľských zmlúv.

1. **Detailný popis potrieb je nasledovný**

V tejto kapitole sa bude budeme venovať jednotlivým aktivitám, dokumentom a riešeniam, ktoré je potrebné dodať na URHH, na nápravu nálezov po kybernetickom audite.

* 1. **Klasifikácia informácií a kategorizácia sietí a informačných systémov**

Je požadované vytvoriť Smernicu pre výkon identifikácie a inventarizácie aktív a následne spôsobu ich klasifikácie a kategorizácie IS a sietí.

Na klasifikácii sa budú podieľať aj interní zamestnanci, cieľom projektu je aj transfer know-how, aby si bola organizácia schopná klasifikáciu následne realizovať aj vlastnými silami.

* 1. **Smernica o bezpečnej prevádzke IS a sietí**

Organizácia zabezpečuje ochranu informácií v sieťach a v podporných zariadeniach, ktoré ich v sieťach spracúvajú. Siete sú v organizácií primerane riadené a spravované, čím sa zabezpečuje ochrana informácií

v systémoch a aplikáciách. Bude pokrývať najmä oblasti:

- bezpečná správa a prevádzka IS a sietí,

- riadenie zmien,

- riadenie kapacít,

- riadenie záplat a aktualizácii,

- zálohovanie dát,

- posudzovanie technických zraniteľnosti,

- správa používateľov a riadenie prístupov,

- bezpečnostné požiadavky pre prístupové práva a účty privilegovaných používateľov.

* 1. **Vykonanie analýzy rizík a analýzy dopadov**

Analýza rizík je výstupom komplexnej a hĺbkovej analýzy rizík IS . Vykonaná analýza rizík IS je aktuálna pre danú etapu projektu. Do úvahy boli brané nasledovné normy, zákony a štandardy:

 Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti

 STN ISO/IEC 27001:2014,

 STN ISO/IEC 27002:2014,

 STN ISO/IEC 27005:2012,

Hlavný dokument Analýzy rizík obsahuje manažérske zhrnutie, metodiku analýzy rizík, opis analyzovanej časti, katalóg aktív a hlavné opatrenia, ktoré sú identifikované analýzou rizík.

Analýza rizík je základnou súčasťou Bezpečnostného projektu a pozostáva z viacerých navzájom prepojených častí, a to:

1. Klasifikácia aktív v projekte,

2. Zoznamu analyzovaných aktív a pôsobiacich hrozieb na tieto aktíva,

3. Vyhodnotenie rizík,

4. Návrhu bezpečnostných opatrení,

5. Zhrnutia výsledkov analýzy rizík.

Výstupom bude vykonaná Analýza rizík podľa jednotnej smernice (metodiky) pre dátovo-procesné aktíva (biznis agendy) a IKT zdroje, ktoré tieto agendy podporujú.

Na Analýzu rizík sa budú podieľať aj interní zamestnanci, cieľom projektu je aj transfer know-how, aby si bola organizácia schopná tieto analýzy opakovane realizovať aj vlastnými silami.

* 1. **Návrh katalógu rizík a spôsobov ich riadenia**

Návrh katalógu rizík a spôsobu ich udržiavania, aktualizácie a riadenia (mitigácie), ktorý bude obsahovať identifikované riziká z analýzy rizík a spôsoby (možnosti) ich riadenia (mitigácie), vrátane zavedenia formalizovaného a opakovaného procesu riadenia rizík a ich schválenia vedením Úrad pre reguláciu hazardných hier alebo Bezpečnostným výborom ak tento bude zriadený.

* 1. **Klientsky modul evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov.**

Tento modul reprezentuje nástroja na evidenciu procesov pre riadenie kybernetickej bezpečnosti, rizík, zraniteľností a hrozieb. Nastroj je požadované implementovať v prostredí zadávateľa. Detailné požiadavky na nástroj sú popísane v ďalších častiach tohto dokumentu.

* 1. **Plán ľudských zdrojov**

Výstupom aktivity bude časový plán implementácie, alokácia zdrojov. Na aktivite sa budú podieľať aj interní zamestnanci, cieľom projektu je aj transfer know-how

* 1. **Nastavenie politík v prostredí úradu**

Výstupom bude nasledovné:

• Vytvorenie a zobrazenie Mapy topológie v reálnom čase v rámci hybridného prostredia

• Tvorba a správa zásad segmentácie

• Funkcia optimalizácie a čistenia politík

* 1. **Vypracovať analýzu funkčnej závislosti všetkých aktív na základnú službu**

Požadované je analyzovať stupeň závažnosti ohrozenia ZS vplyvom výpadku Informačného Aktíva asociovaného so základnou službou

Definovať inštalačný štandard pre informačné aktíva v sieťach a vyžadovať ich aplikovanie pri inštalácií v rámci životného cyklu informačného aktíva.

Určiť úlohy, povinnosti a zodpovednosti za riadenie kybernetickej bezpečnosti, riadenie aktív, riadenie rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie.

Rozšíriť zoznam všetkých informačných aktív v spoločnosti a zaviesť jeho centrálne riadenie napr. oddelením informatiky. Obsahom bude priradenia biznis vlastníka a klasifikácii.

* 1. **Zaviesť metodiku riadenia celého životného cyklu všetkých aktív**

Požiadavka je definovanie Metodika životného cyklu informačného aktíva. Táto metodika bude neskôr zadefinovaná v nástroji „Klientsky modul evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov.“

Typy opatrení v kontexte životného cyklu informačného aktíva:

 existujúce opatrenia (z angl. Existing controls) – opatrenia inherentne zabudované už v čase návrhu

resp. implementácie systému,

 rozšírené (tiež „vylepšené“) opatrenia (z angl. Enhanced controls) – aplikované na implementovaný

systém s cieľom ošetrenia rizika identifikovaného už v rámci bežnej prevádzky systému; typicky ich

navrhuje manažér kybernetickej a informačnej bezpečnosti,

 dodatočné opatrenia (z angl. Additional, Complementary controls) - odporúča ich typicky audítor

v správe auditu s cieľom ošetrenia rizika identifikovaného v rámci výkonu auditu kybernetickej

bezpečnosti.

* 1. **Zaviesť procesy na výkon riadenia aktív a rizík a tak isto implementácia nástroja na riadenie rizík a politík v organizácií URHH.**

Postupy aplikovania metodiky životného cyklu aktíva. Tieto budú definované a spravované v rámci „Klientskeho modulu evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík a incidentov.“

* 1. **Vytvoriť a formalizovať postupy pri zaradení osoby do bezpečnostných rolí, presunu práv, povinností a zodpovedností vo vzťahu ku kybernetickej bezpečnosti na inú osobu a nastaviť úlohy, povinnosti a zodpovednosti pri týchto postupoch**

V rámci tejto požiadavky je nutné vypracovať RACI matice pre kľúčové role informačnej a kybernetickej bezpečnosti, zohľadniť závislosti (Oddelenie exekutívy, výkonu a kontroly), zastupiteľnosť a prenositeľnosť rolí.

* 1. **Vypracovať plán rozvoja bezpečnostného povedomia a pravidelného vzdelávania zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov a tento plán vykonávať v praxi vo forme úvodného školenia, preškolenia pri zmene pracovnej pozície alebo pravidelného ročného školenia formou e-learningu a o absolvovaní týchto školení uchovávať záznam.**

V rámci tejto požiadavky je nutné navrhnutie systémového plánu vzdelávania formou vstupný skolení ako aj pravidelných školení s dôrazom na cieľovú skupinu. Navrhnúť spôsob vyhodnocovania procesu rozvoja budovania bezpečnostného povedomia zamestnancov a tretích strán

* 1. **Vytvoriť a formalizovať pravidlá a postupy na riešenie prípadov porušenia bezpečnostnej politiky zo strany používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov**

V rámci tejto požiadavky je nutné zadefinovať disciplinárny proces nad rámec pracovného poriadku pre prípady porušenia kybernetickej bezpečnosti

* 1. **Vytvoriť a formalizovať postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu s používateľom, administrátorom, s osobou zastávajúcou niektorú z bezpečnostných rolí umožňujúcich presun práv, povinností a zodpovedností na inú novú osobu.**

V rámci tejto požiadavky je nutné vytvorenie a zavedenie procesu skončenia pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu s používateľom, administrátorom, s osobou zastávajúcou niektorú z bezpečnostných rolí

* 1. **Vytvoriť a formalizovať postupy na obmedzenie alebo odňatie prístupových oprávnení a privilégií v prípade porušenia bezpečnostných politík vybranými pozíciami v spoločnosti.**

V rámci tejto požiadavky je nutné vytvorenie a zavedenie procesu na obmedzenie alebo odňatie prístupových oprávnení a privilégií v prípade porušenia bezpečnostných politík vybranými pozíciami v spoločnosti.

* 1. **Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP**

Smernica pre výkon AR/BIA, vrátane definovania základných parametrov (hrozby, dopadové kritéria, spôsob identifikácie a klasifikácie rizík, spôsob definovania RTO a RPO a pod.).

Vypracovanie BIA na základnú službu a jej komponenty.

Definovanie atribútov RTO, RPO a transponovať do požiadaviek BCP a politiky zálohovania

Personalizovať role v BCP

Definovať a riadiť požiadavky na dodávateľov vyplývajúcich z BIA.

* 1. **Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP**

Zavedenie BCMS musí vychádzať z medzinárodných štandardov a v súlade s požiadavkami platnej legislatívy predovšetkým ZoKB a zákona o ITVS.

* + 1. **Kontext organizácie**

V rámci tejto kategórie definujeme nasledovné požiadavky a výstupy.

* Popis organizácie a jej kontextu z pohľadu BCMS - Opis spoločnosti a identifikácia interných a externých závislostí z pohľadu BCMS
* Zadefinovanie potrieb a očakávaní zainteresovaných strán - Identifikácia a spôsob identifikácie zainteresovaných strán spoločnosti a identifikácia ich požiadaviek závislostí z pohľadu BCMS.
* Právne požiadavky - Identifikácia zákonných a regulačných požiadaviek a definovanie spôsobu identifikácie právnych požiadaviek, zabezpečenie udržiavania a dokumentovania závislostí z pohľadu BCMS.
* Určenie rozsahu systému manažérstva kontinuity podnikania - Stanovenie hraníc aplikovateľnosti BCMS v spoločnosti, geografická, technologická, organizačná.
* Rozsah pôsobnosti systému manažérstva kontinuity podnikania - Určenie častí, ktoré budú zaradené do BCMS. Výber produktov a služieb zahrnutých do procesu BCMS

Definovanie a spôsob dokumentovania výnimiek z BCMS, ktoré však nesmú ovplyvniť schopnosť organizácie zaistiť kontinuitu podnikania v priamej väzbe na analýzu obchodného dopadu.

* + 1. **Riadenie**
* Ciele BCMS - Definovanie SMART cieľov BCMS a definovanie spôsobu naplnenia cieľov. Definovanie merateľných kritérií (KPI)
* Stanovenie politiky kontinuity podnikania - Stanoviť Politiku kontinuity podnikania, ktorá musí obsahovať rámec pre stanovenie cieľov kontinuity podnikania, musí obsahovať záväzok plniť príslušné požiadavky a záväzok k neustálemu zlepšovaniu BCMS. Zaistenie integrácie požiadaviek BCMS do podnikových procesov. Definovanie potrebných zdrojov vrátane definovania kľúčových rolí.
* Publikovanie politiky kontinuity podnikania - Politika kontinuity podnikania musí byť dostupná ako dokumentovaná informácia a komunikovaná vo vnútri organizácie. Musí byť k dispozícii zainteresovaným stranám
* Role, zodpovednosti a právomoci - Definovať role a zodpovednosti a právomoci formou RACI matice. Definovanie zodpovednosti a spôsobu za predkladanie správ o BCMS vedeniu spoločnosti.
  + 1. **Plánovanie**
* Opatrenia zamerané na riziká a príležitosti - Zaviesť proces, ako organizácia plánuje opatrenia pre riešenia rizík a príležitostí pri procese plánovania BCMS. Definovanie Opatrení, ktoré zabránia ohrozeniu BCMS. Spôsob Integrácie a implementácie opatrení do procesov BCMS. Zavedenie hodnotia účinnosti opatrení
* Ciele kontinuity podnikania a plány na ich dosiahnutie - Definovanie Cieľov kontinuity podnikania ktoré musia byť:
  + Konzistentné s politikou kontinuity podnikania
  + Byť merateľné
  + Zohľadniť aplikovateľné požiadavky
  + Byť monitorované
  + Byť komunikované
  + Byť aktualizované
* Určenie spôsobu dosiahnutia cieľov kontinuity podnikania - Jednotlivé ciele BCMS musí určiť:
  + Čo sa bude robiť
  + Aké zdroje budú použité
  + Kto bude zodpovedný
  + Kedy to bude dokončené
  + Ako budú hodnotené výsledky
* Plánovanie zmien systému manažérstva kontinuity podnikania - Definovanie spôsobu zmien s dôrazom na
  + Účel zmien a ich dôsledky
  + Integritu BCMS
  + Dostupnosť zdrojov k zmene
    1. **Podpora**
* Zdroje - Definovanie zdrojov potrebných na vytvorenie, implementáciu, udržiavanie a neustále zlepšovanie BCMS
* Kompetencie a povedomie - Definovanie kompetencie osôb, ktoré sú zahrnuté do BCMS.
* Vyškolenie osôb, ktoré sú zahrnuté do BCMS.
* Dokumentované informácie – minimálny rozsah - Vypracovanie dokumentácie minimálne v rozsahu požiadaviek kriteriálnej normy:
  + Zoznam zákonných, regulačných a iných požiadaviek (bod 4.2.2) - obsahuje zoznam všetkého, čo musíte splniť.
  + Rozsah BCMS a vysvetlenie výnimiek (článok 4.3) - definuje, kde bude váš BCMS implementovaný.
  + Politika kontinuity podnikania (článok 5.2) - definuje hlavné zodpovednosti a zámer vedenia.
  + Ciele kontinuity činnosti (článok 6.2) - definuje merateľné ciele, ktoré sa majú dosiahnuť pomocou kontinuity činnosti.
  + Kompetencie personálu (článok 7.2) - definuje potrebné znalosti a zručnosti.
  + Plány a postupy kontinuity činnosti (doložka 8.4) - zahŕňa plány a postupy pre reakcie, komunikáciu, obnovu (vrátane plánov obnovy po havárii), činnosti obnovy a návratu.
  + Dokumentovaná komunikácia so zainteresovanými stranami (článok 8.4.3.1) - môžu to byť e -maily, ale aj oficiálna komunikácia zo zdrojov, ako sú vládne agentúry a ďalšie.
  + Záznamy dôležitých informácií o narušení, prijatých opatreniach a prijatých rozhodnutiach (článok 8.4.3.1) - tieto záznamy sa spravidla robia prostredníctvom zápisnice alebo vyplnením kontrolných zoznamov vykonaných činností.
  + Údaje a výsledky monitorovania a merania (bod 9.1.1) - toto je hodnotenie, či váš BCMS splnil ciele.
  + Program vnútorného auditu (doložka 9.2)
  + Výsledky interného auditu (článok 9.2) - spravidla ide o správu o internom audite.
  + Výsledky preskúmania manažmentom (doložka 9.3) - spravidla má formu zápisnice alebo zdokumentovaných rozhodnutí.
  + Povaha nezhôd a prijaté opatrenia (článok 10.1) - toto je opis nezhôd a ich príčiny.
  + Výsledky nápravných opatrení (článok 10.1) - toto je opis toho, čo bolo urobené s cieľom odstrániť príčinu nezhody.
    1. **Prevádzka**
* Analýza dopadu na podnikanie (BIA) a posudzovanie rizík - Vypracovanie metodiky pre analýzu dopadu (BIA) na podnikanie a posudzovanie rizík.

Definovanie spôsobu a periodicity preskúmavania analýzy dopadu

Analýza dopadov na podnikanie musí:

* + Definovať typy dopadu a kritériá relevantné pre kontext organizácie.
  + Identifikovať činnosti, ktoré podporujú poskytovanie produktov a služieb.
  + Používať typy dopadov a kritéria pre posudzovanie v čase
  + Identifikovať časový rámec (MTPD maximálna prípustná doba narušenia), v ktorom by sa dopady neobnovujúcich činností stali neprijateľné
  + Stanoviť prioritný časový rámec pre obnovenie narušených činností na minimálnu kapacitu „RTO cieľová doba obnovy“.
  + Použiť analýzu na určenie prioritných činností.
  + Rozhodnúť ktoré zdroje sú potrebné na podporu prioritných činností
  + Určiť závislosti, vrátanie partnerov a dodávateľov a nezávislých prioritných činností
* Proces posudzovania rizík - Definovanie spôsobu organizácia vykonávať posudzovania rizík
* Stratégie a riešenie kontinuity podnikania - Identifikovať a vybrať stratégie pre zaistenie kontinuity podnikania, ktoré určujú možnosti PRED, POČAS a PO narušení.
* 5.4 Identifikácia stratégií a riešení - Definovanie Stratégia s dôrazom na požiadavky:
  + Zabezpečené základné požiadavky na obnovu prioritných činností v stanovenom čase
  + Ochrana prioritných činnosti
  + Znižovať pravdepodobnosť narušenia
  + Skracovať dobu narušenia
  + Obmedziť dopad narušenia na produkty a služby organizácie
  + Zaistiť dostupnosť primeraných zdrojov
* Štruktúra reakcie - Nastavenie štruktúry tímov zodpovedných za reakciu na narušenie so schopnosťou :
  + Posúdiť povahu a rozsah narušenia a jeho potenciálny dopad
  + Stanoviť hranicu dopadu, ktorá odôvodní reakcie
  + Aktivovať vhodnú reakciu
  + Naplánovať opatrenia
  + Stanoviť priority
  + Sledovať účinky narušenia a reakcie
  + Aktivovať riešenia pre kontinuitu podnikania
  + Komunikovať s relevantnými zainteresovanými stranami

Pre každý tím musia byť určení pracovníci a ich náhradníci s definovanou zodpovednosťou – definované role.

Musia byť definované zdokumentované postupy vrátane činností a postupov.

* Varovanie a komunikácia - Nastaviť a zdokumentovať postupy pre:
  + Internú a externú komunikáciu so zainteresovanými stranami
  + Prijímanie, dokumentovanie a reagovanie na dokumentáciu od zainteresovaných strán
  + Zaistenie dostupnosti komunikačných prostriedkov behom varovania
  + Uľahčenie štruktúrovanej komunikácie s núdzovými pohotovostnými službami
  + Poskytnutie podrobností o reakcii organizácie v médiách
  + Zaznamenávanie detailov narušenia, prijatých opatrení a účinných rozhodnutí
* Plán kontinuity podnikania - Vypracovať metodiku pre postupy kontinuity podnikania, ktoré pomáhajú tímom reagovať na narušenie a pomáhajú organizácii s reakciou a zotavením v rozsahu:
  + Podrobnosti o opatreniach, ktoré je nutné urobiť tak, aby prioritné činnosti pokračovali alebo boli obnovené vo vopred stanovených časových intervaloch a sledovali dopad narušenia
  + Odkaz na vopred definovanú prahovú hodnotu a postup pre aktiváciu reakcie.
  + Postup umožňujúci dodávku produktov a služieb o dohodnutej kapacite.

Podrobnosti o riadení bezprostredných následkov narušenia a uložení povinností s ohľadom na prospech jednotlivcov, prevenciu ďalšej straty.

Každý plán musí zahrňovať:

* + Účel, rozsah a ciele,
  + Role a zodpovednosti tímu,
  + Účel, rozsah a ciele,
  + Role a zodpovednosti tímu,
  + Opatrenia na implementovanie riešení,
  + Podporné informácie pre aktiváciu opatrení
  + Interné a externé vzájomné súvislosti
  + Požiadavky na zdroje
  + Požiadavky na podávanie správ
  + Proces odstúpenia.
* Obnova - Zdokumentovanie postupu pre obnovu a navrátenie podnikateľských aktivít z dočasných opatrení prijatých v priebehu a po narušení
* Program nácviku - Implementovať program nácviku a testovania pre overenie efektívnosti stratégií a riešení pre zachovanie kontinuity podnikania

Testy musia byť :

* + sú v súlade s cieľmi kontinuity podnikania
  + sú založené na vhodných scenároch a dobre naplánované a definované
  + podporujú spoluprácu a kompetencie daných rolí
  + v čase overujú stratégie a riešenia
  + obsahujú správu z nácviku
  + Správa obsahuje výsledky a odporučenia pre zlepšenie
  + Musia byť sú preskúmavané
  + sú realizované i v prípade významných zmien v organizácii mimo plán
    1. **Hodnotenie výkonnosti**
* Monitorovanie, meranie, analýza a vyhodnotenie - Zaviesť systém monitorovania a merania s definovaním zodpovednosti a intervaly na meranie a monitorovanie.

Zaviesť proces interného audit na prvky BCMS

* + 1. **Zlepšovanie**
* Nezhody a nápravné opatrenia - Nastavenie procesu na vysporiadanie sa s nezhodou to, aby boli prijaté opatrenia pre elimináciu príčin nezhody

1. **Požiadavky na zavedenie** **nástroja na evidencie a procesov pre riadenie kybernetickej bezpečnosti, rizík, zraniteľností a hrozieb**

Oblasť komplexného riadenia bezpečnosti, procesov, dokumentácie a riadenia rizík bude zabezpečená implementáciou systému pre riadenie kybernetickej bezpečnosti, rizík, zraniteľností a hrozieb zraniteľností a hrozieb.

Obstarávateľ požaduje implementáciu, ktorá bude v prostredí obstarávateľa.

1. **Funkčné požiadavky na parametre služby:**

* Lokálna implementácia v rámci datacentier obstarávateľa.
* Systém musí byť možné nasadiť vo virtualizovanom prostredí.
* Riešenie je dodané ako jednotné softvérové riešenie s viacerými modulmi.
* Inštalácia a konfigurácia aplikačného programového vybavenia
* Implementácia procesných nastavení podľa špecifikácií vypracovaných v rámci analýzy
* Interné testovanie s testovacími dátami vyhotovenými zhotoviteľom,
* Vyhotovenie dokumentácie,
* Implementácia rozhraní s externými informačnými systémami,
* Dizajn wokflow-u, implementácia bezpečnostných politík
* Návrh a implementácia operačných postupov pre rutinné operácie správy s využitím funkcionality delenia práce pre jednotlivé tými v rámci organizácie
* Mapovanie požiadaviek technického návrhu na funkčné celky infraštruktúry
* Implementácia bezpečnostných politík do konfigurácií
* Zohľadnenie backup politík a vytvorenie backup plánu, pre Log Data na zabezpečenie konzistencie a retencie
* Prevádzková dokumentácia, udržiavanie a obnova (BCM a DR)
* Komplexná technická dokumentácia na všetkých vrstvách dodaného riešenia
* Know-how transfer
* Implementácia a parametrizácia riešenia, migrácia existujúcich dokumentov, smerníc a predpisov obstarávateľa.
* Integráciu s LDAP zadávateľa a definovanie rolí v rámci organizácie
* Zabezpečenie jednotného projektového riadenia

1. **Prerekvizity riešenia:**

Zadávateľ

* Zadávateľ poskytne virtuálny priestor a prístupy – všetky aktivity spojené s inštaláciou zabezpečuje dodávateľ.
* Systému musí byť nasadený a udržiavaný v dvoch verziách – testovacia verzia, produkčná verzia.

Požadovaný rozsah služieb v rámci implementácie:

* + Vstupná analýza a špecifikácia (analýza existujúcich dát, záznamov, procesov a dokumentácie)
  + Na základe analýzy definovanie požiadaviek, problémov, procesov, návrhy riešenia, a plánovanie
  + Implementácia systému
  + Parametrizácia a prípadné do vývoje
  + Vkladanie testovacích dát
  + Základné školenia kľúčových zamestnancov a testovacích zamestnancov
  + Nastavenie Work-flow procesov
  + Nastavenie prepojení na externé systémy
  + Školenia
  + Školenie pre správcov systému
  + školenie pre manažérov
  + školenia pre interných audítorov
  + Školenia pre Manažérov kybernetickej
  + školenia k dokumentácii
  + školenia všetkých zamestnancov
  + Testovanie;
  + testovanie funkcionality minimálne 1 mesiac
  + Plnenie produkčných dát, to znamená napríklad zoznam aktív a existujúcich hrozieb, zraniteľnosti a rizík
  + Nasadenie do prevádzky;
  + Aktívny dohľad nad produkčnou prevádzkou
  + Support: Monitoring, údržba, na 12 mesiacov. (Súčasťou riešenia je aj podpora výrobcu v rozsahu 1 rokov). To znamená asistencia v prípade technických problémov s riešením.

1. **Požiadavky na systém:**

|  |
| --- |
| 1. **Systém** |
| * Systém musí poskytovať riadenie kybernetickej bezpečnosti ako celku a v súlade so Zákonom o kybernetickej bezpečnosti. |
| * Jazyk systému aj sprievodnej dokumentácie – slovenský alebo česky |
| * v prípade potreby a rozhodnutia URHH a Manažéra KB musí byť systém schopný zastrešiť všetky evidenčné a procesné oblasti riadenia KB nezávisle od iných systémov a bez potreby integrácie na iné systémy. |
| * systém nesmie byť zložený s viacerých samostatných špecifických systémov – požadované je jednotné riešenie a jednotná technológia v rámci všetkých definovaných funkcionalít. |
| * systém musí umožňovať pracovať aj s databázami, ktoré nie potrebné priebežne platiť. Databáza bude dodaná Zadávateľom. |
| * nástroj musí umožňovať úpravy existujúcich modulov a rolí/oprávnení podľa požiadaviek Zadávateľa. |
| * Integrovaný zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a požiadavky vyhlášky č. 362/2018 Z.z. Obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. To znamená, že systém mapuje opatrenia, aktíva, hrozby, rizika voči zákonu o kybernetickej bezpečnosti č. 69/2018 Z.z. |
| * možnosť pracovať v systéme aj s inými bezpečnostnými štandardmi (napr. ISO 27001, ako separátny modul) |
| * požadovaná integrácia s AD (min. LDAP), primárne na zdieľanie účtov. |
| * možnosť definovať vlastné workflow procesy na úrovni celého systému |
| * ku každému prvku (napr. akZtíva, systémové aktívum, hrozba a pod.) možnosť definovať neobmedzené množstvo užívateľských parametrov minimálne na úrovni textových polí alebo číselníkov (v rámci interných kapacít bez potreby súčinnosti dodávateľa) |
| * systém musí umožňovať nastavenie pre každú rolu vo forme read only (pridelený zamestnanec môže nahliadať ale nemôže nič pridávať, upravovať ani mazať) |
| * možnosť nastaviť eskalačné procedúry pre jednotlivé činnosti (napr. plány v prípade neplnenia) |
| * možnosť prepojiť so service deskom, alebo CMDB databázou |
| * možnosť využívať API rozhranie |
| * riadenie prístupov v systéme musí pracovať princípom Need to know |
| * kompletná evidencia všetkých zmien zrealizovaných užívateľom alebo správcom s možnosťou zobraziť históriu zmien bez potreby generovať samostatné výstupy. |
| * integrovaná OLAP kocka minimálne na úrovni pohľadov na informačné aktíva, systémové aktíva, hrozby, zraniteľnosti, opatrenia, riziká, nezhody a ich vzájomné súvislosti v danom okamihu. |
| * Na základe prístupových práv možnosť užívateľsky vyexportovať akékoľvek zoznamy do excelu, wordu, pdf. |
| * možnosť vytvoriť a automatizovane udržiavať Prehlásenie o aplikovateľnosti |
| * každý užívateľ musí mať svoje jedinečné prihlasovacie údaje. |
| * automatizované pripomienkovanie a upozorňovanie zamestnancov v prípade ak majú zrealizovať nejakú aktivitu súvisiacu s procesmi KB. (napr. povinnosť aktualizovať analýzu rizík, povinnosť prehodnotiť informačné aktíva, povinnosť oboznámiť sa s dokumentom a pod.) |
| * notifikácia aktivít minimálne na úrovni mailov. |
| 1. **Org. štruktúra** |
| * Org. štruktúru mať možnosť integrovať s AD a pravidelne aktualizovať |
| * integrácia s AD v rozsahu štruktúry „vedenie, odbor, oddelenie“ |
| * integrácia s AD v rozsahu zamestnanec, pracovná pozícia, zaradenie v Org. štruktúre, nadriadený zamestnanec, nástup a ukončenie pracovného pomeru |
| * možnosť evidencie viacerých objektov (budov) a ich rozdelenie v rámci Org. štruktúry |
| * možnosť vytvárať vlastné role |
| * možnosť užívateľsky vytvárať skupiny zamestnancov podľa potreby a následne s danými skupinami pracovať v rámci celého systému |
| * v prípade zmien v Org. štruktúre automaticky upozorniť kompetentné osoby |
| 1. **Informačné aktíva** |
| * Vysvetlenie: Primárne aktíva - informácie, dáta, know-how apod. Systémové aktíva - informačné systémy, hw, sw, siete, sieťové prvky, dodávatelia a pod. |
|  |
| * vytvorenie a správu katalógu primárnych aktív a systémových aktív, ich väzieb, možnosť ich hodnotenia, nastavenie hierarchie, priraďovanie kompetentných osôb (vrátane externého subjektu ako tretej strany). možnosť dopĺňať ďalšie sledované parametre bez potreby do vývoja |
| * možnosť priradiť k primárnemu aktívu neobmedzené množstvo systémových aktív |
| * možnosť definovať vlastné metriky hodnotení dôvernosti, integrity a dostupnosti |
| * možnosť definovať garantov aktív na úrovni zamestnanca, role alebo oddelenia |
| * pre každé informačné aktívum musí mať možnosť definovať úroveň dôvernosti, integrity a dostupnosti v vzťahu ku každému priradenému systémovému aktívu samostatnú. Tento vzťah musí priamo vstupovať do analýzy rizík. |
| 1. **Systémové aktíva** |
| * možnosť definovať popis, vlastné kategórie aktív, definovať ich logické (IT) umiestnenie, alebo fyzické umiestnenie |
| * možnosť nastaviť, či hodnota systémového aktíva bude preberaná z pripojených primárnych aktív, alebo bude automatizovane vypočítavaná, alebo bude manuálne fixne definovaná. |
| * systémové aktíva musí byť možné hromadne naimportovať |
| * ku každému systémovému aktívu musí byť možné priradiť opatrenia, ktoré sú na danom systémovom aktíve implementované. |
| 1. **Riadenie rizík** |
| * Vytvorenie a správa katalógu hrozieb, zraniteľností a opatrení, priraďovanie kompetentných osôb alebo externých subjektov. |
| * možnosť užívateľsky definovať vlastné riziká, vlastné hrozby, zraniteľnosti, opatrenia. Vytváranie vlastných registrov. |
| * spracovanie Business impact analýzy (BIA) minimálne na úrovni informačných aktív a súvisiacich systémov |
| * možnosť definovať viac analýz súčasne vrátane metodík analýz (minimálne 2 – automatizovaná podľa aktuálnych zmien a systémová napr. na úrovni jedného roka) |
| * automatizovaná analýza rizík na základe priebežných záznamov (incidenty, zistenia z auditov, zistenia z kontrol a podobne) |
| * v prípade automatizovaných výpočtov rizík KB si URHH definuje vlastné vstupy, parametre, hodnoty, váhy a vzorce, ktoré budú vstupovať do automatizované výpočtu. |
| * Dodávateľ povinný na vyžiadanie poskytnúť podrobne rozpísané metodiky výpočtov analýz rizík, všetky položky, ktoré do výpočtov vstupujú, ich hodnoty a váhy a vzorce pre výpočet rizík. |
| * riadenie rizík musí byť možné až do detailu konkrétneho aktíva, alebo systému v danom čase, vrátane s históriou výšky rizika na danom aktíve, alebo systéme. |
| * ku každému riziku musí byť možné priradiť súvisiace informačné aktíva, systémové aktíva, opatrenia, zraniteľnosti, hrozby |
| * ku každému riziku musí byť možné definovať plány zvládania rizika |
| * jedno riziko môže mať viac plánov ako aj jeden plán môže zastrešovať viac rizík |
| * pri realizácii plánov musí byť nastavený WF proces vrátane eskalačných procesov. |
| * každý plán musí obsahovať minimálne popis aktivity, WF procesy, zodpovedné osoby, finančnú alebo kapacitnú náročnosť, termíny realizácie, a definovať osoby kto schváli že daný plán bol splnený, eskalačné procesy pre prípad, že sa plány nesplnili. |
| 1. **Zraniteľnosti** |
| * URHH si definuje vlastný katalóg zraniteľností |
| * možnosť vytvárať skupiny zraniteľností |
| * možnosť napojenia systému na monitorovacie systémy, alebo systémy riadenia zraniteľností. Možnosti budúcich integrácii. |
| * možnosť sledovať úroveň jednotlivých zraniteľností (v %, alebo inom číselnom vyjadrení) na základe reálneho vývoja bezpečnosti v prostredí URHH |
| * každá zraniteľnosť musí mať pridelenú zodpovednú osobu, ktorá v prípade zneužitia zraniteľnosti je systémom okamžite informovaná |
| * možnosť definovať hodnoty zraniteľnosti fixne, alebo operatívne sa meniace podľa reálneho vývoja bezpečnosti v prostredí URHH |
| 1. **Hrozby** |
| * URHH si definuje vlastný katalóg hrozieb |
| * možnosť vytvárať skupiny hrozieb |
| * možnosť sledovať úroveň jednotlivých hrozieb (v %, alebo inom číselnom vyjadrení) na základe reálneho vývoja bezpečnosti v prostredí URHH |
| * každá hrozba musí mať pridelenú zodpovednú osobu, ktorá v prípade uskutočnenia hrozby je systémom okamžite informovaná |
| * možnosť definovať hodnoty hrozieb fixne, alebo operatívne sa meniace podľa reálneho vývoja bezpečnosti v prostredí URHH |
| 1. **Opatrenia** |
| * URHH si definuje vlastný katalóg opatrení |
| * možnosť vytvárať skupiny opatrení |
| * možnosť sledovať úroveň jednotlivých opatrení (v %, alebo inom číselnom vyjadrení) na základe reálneho vývoja bezpečnosti v prostredí URHH |
| * každé opatrenie musí mať pridelenú zodpovednú osobu, ktorá v prípade zlyhania opatrenia je systémom okamžite informovaná |
| * možnosť definovať hodnoty opatrení fixne, alebo operatívne sa meniace podľa reálneho vývoja bezpečnosti v prostredí URHH |
| 1. **Ciele** |
| * Možnosť definovať ciele KB |
| * ciele KB musia byť priamo prepojené s rizikami KB |
| * každý plán musí obsahovať minimálne popis aktivity, WF procesy, zodpovedné osoby, finančnú alebo kapacitnú náročnosť, termíny realizácie, a definovať osoby kto schváli že daný plán bol splnený, eskalačné procesy pre prípad, že sa plány nesplnili. |
| * možnosť prideliť jeden plán k viacerým cieľom |
| * možnosť sledovať plnenie plánov napr. v % vyjadrení |
| 1. **Audity, kontroly, testy** |
| * Kompletná agenda auditov od plánovania cez realizáciu a vyhodnocovanie auditov |
| * riadenie auditov v zmysle zákona č. 69/2018 o kybernetickej bezpečnosti. Nástroj umožní dokumentovanie auditných záznamov a správ |
| * možnosť plánovať a riadiť audity |
| * možnosť definovať vlastné kategórie auditov, kontrol, testov. Ako je napríklad testovanie voči známym zraniteľnostiam. |
| * možnosť definovať vlastné kategórie zistení auditov, kontrol, testov a ich váhu |
| * v rámci každého auditu možnosť definovať interného, alebo externého audítora, oddelenie na ktorom prebehne audit, presný dátum a čas kedy prebehne audit, predmet auditu, článok normy/vyhlášky/ zákona |
| * v rámci jednotlivých zistení možnosť definovať väzby na aktíva, systémové aktíva, hrozby, zraniteľnosti. |
| * zabezpečenie kompletnej evidencie interných/externých auditov/kontrol, auditných plánov, auditných zistení, plány pre zvládanie auditných zistení vrátane možnosti notifikácie osôb, ktoré majú získať informácie o audite, zabezpečenie evidencie kontrol, vyhodnocovanie. |
| * každý plán musí obsahovať minimálne popis aktivity, WF procesy, zodpovedné osoby, finančnú alebo kapacitnú náročnosť, termíny realizácie, a definovať osoby kto schváli že daný plán bol splnený, eskalačné procesy pre prípad, že sa plány nesplnili. |
| * možnosť automatizovane prepočítavať riziká na základe identifikovaných zistení v prostredí zadávateľa. |
| 1. **Dokumentácia** |
| * Komplexná a kompletná správa bezpečnostnej dokumentácie na úrovni smerníc, politík, vyhlášok, záznamov, manuálov a pod. |
| * možnosť riadiť prístupy k dokumentácii podľa vopred definovaných pravidiel, schválených URHH |
| * možnosť definovať práva pre každý dokument individuálne, ale aj pre skupiny dokumentov |
| * možnosť vložiť dokument a riadiť v systéme celý životný cyklus od odoslania na pripomienkovanie, cez úpravy, schválenie, oboznamovanie až po ukončenie platnosti dokumentu a jeho vyradenie. |
| * možnosť vygenerovať dokumentáciu na základe informácií zo systému a riadiť v systéme celý životný cyklus od odoslania na pripomienkovaní, cez úpravy, schválenie, oboznamovanie až po ukončenie platnosti dokumentu a jeho vyradenie. |
| * kompletná evidencia všetkých zmien v každom vygenerovanom dokumente na úrovni zobrazenia pôvodného znenia a nového znenia, |
| * evidencia všetkých popisov zmien v každom nevygenerovanom dokumente |
| * kompletná evidencia všetkých zmien v dokumente a autorov zmien |
| * Riadenie verzií dokumentácie a archívne uloženie všetkých predchádzajúcich verzií dokumentu |
| * pripomienkovanie návrhov dokumentácie (vrátane možnosti zabezpečenia notifikácie určených osôb na pripomienkovanie, notifikácie cieľovej skupiny užívateľov, že dokument bol aktualizovaný), |
| * v rámci pripomienkovania kompletná evidencia všetkých pripomienok v dokumente s väzbou na text, ku ktorému je pripomienka daná, čas a dátum pripomienky, autora pripomienka a aj výsledok ako bola daná pripomienka spracovaná. |
| * pripomienkovanie návrhov dokumentácie (vrátane možnosti zabezpečenia notifikácie určených osôb na pripomienkovanie, notifikácie cieľovej skupiny užívateľov, že dokument bol aktualizovaný), |
| * automatizovaný proces oboznamovania sa s dokumentom a potvrdení o oboznamovaní |
| * systém musí mať definovaný proces, prostredníctvom ktorého je možné vygenerovať prezenčnú listinu, vyškoliť zamestnancov osobne a následne danú prezenčnú listinu zapracovať do systému. |
| * nastavenie workflow a eskalačných procesov pre pripomienkovanie, schvaľovanie a oboznamovanie sa s predpismi, |
| * požadovaná možnosť tvorby a generovania dokumentácie podľa interného dizajn manuálu. |
| * nastavenie neobmedzeného počtu workflow procesov pre jednotlivé typy dokumentov alebo záznamov. Tvorba, alebo úprava workflow procesov musí byť možná aj bez spoluúčasti dodávateľa – t.j. internými zamestnancami URHH |
| * nastavenie dátumu platnosti dokumentu (od-do), dátumu vydania dokumentu, |
| * nastavenie klasifikačného stupňa citlivosti informácií dokumentu, |
| 1. **Externé subjekty** |
| * Riadenie dodávateľov/externých subjektov s vplyvom na kybernetickú bezpečnosť, priraďovanie ich rolí, hodnotenie subjektu z pohľadu dostupnosti, dôvernosti a integrity. možnosť priradenia externého subjektu k jednotlivým aktivitám, procesom, plánom v rámci celého systému na úrovni kompetentnej osoby externého subjektu. |
| * možnosť definovať externé subjekty ako integrovanú súčasť systému s prepojením na informačné aktíva, systémy, opatrenia, hrozby, zraniteľnosti, audity a pod. |
| * možnosť definovať tretie strany až na úroveň konkrétneho zamestnanca |
| * možnosť riadiť role zamestnancov externých subjektov rovnako ako interných zamestnancov |
| * možnosť definovať kompetencie a povinnosti zamestnancov externých subjektov rovnako ako interných zamestnancov. |
| 1. **Incidenty / udalosti** |
| * Možnosť evidovať podrobne všetky bezpečnostné incidenty a udalosti a ich súvislosti |
| * možnosť definovať vlastné kategórie incidentov a udalostí a definovať k nim workflow proces |
| * v rámci každého incidentu / udalosti možnosť definovať miesto, čas, zodpovedné osoby, úroveň škody |
| * možnosť integrácie s existujúcou evidenciou, alebo inými bezpečnostnými systémami |
| * v rámci jednotlivých incidentov / udalostí možnosť definovať väzby na aktíva, systémové aktíva, hrozby, zraniteľnosti. |
| * možnosť definovať pre každý incident viac plánov na zvládanie incidentu |
| * každý plán musí obsahovať minimálne popis aktivity, WF procesy, zodpovedné osoby, finančnú alebo kapacitnú náročnosť, termíny realizácie, a definovať osoby ktoré schvália že daný plán bol splnený, eskalačné procesy pre prípad, že sa plány nesplnili. |
| * možnosť automatizovane prepočítavať riziká na základe jednotlivých incidentov / udalostí |
| * možnosť vyhodnocovať incidenty za určité obdobie a identifikovať koreňové príčiny incidentov / udalostí |
| 1. **Výstupy** |
| * Možnosť definovať vlastné výstupy vo forme tabuliek alebo grafov (XLS, PDF,XML) |
| * možnosť zobrazovať výsledky tabuliek a grafov k definovanému času, alebo určiť interval aktualizácie dát. |
| * možnosť automatizovane zasielať vybrané výstupy určenými osobám v určených intervaloch |
| * možnosť riadiť prístupy (edit, read only) k jednotlivým výstupom |
| * možnosť prepojenia na externé manažérske systémy |
| * možnosť užívateľsky definovať aké výstupy sa majú zobrazovať na úvodnej obrazovke systému po prihlásení užívateľa. |
| 1. **Logovanie** |
| * logovanie všetkých užívateľských aj systémových aktivít v systéme |
| * možnosť prepojenia na externé monitorovacie systémy |

Minimálne 3 referencie nasadenia systému a jeho využívania minimálne 1 rok v ostrej prevádzke vo vyššie požadovanej funkcionalite v rozsahu pre 100 a viac užívateľov.

1. **Licencovanie**

Požadujeme licenciu ktorá bude zodpovedať požiadavkám:

* + minimálne pre 100 aktívnych používateľov ktorí budú aktívne pracovať v systéme
  + minimálne 350 pasívnych užívateľov, ktorí budú pracovať v systéme len v prípade že ich systém vyzve aby zrealizovali nejakú aktivitu.

1. **Ostatné požiadavky**

* Vypracovanie interných smerníc a prevádzkovej dokumentácie riadenia IB a KyB
* Stratégia kybernetickej bezpečnosti

Určiť SMART ciele na dosiahnutie súladu s požiadavkami ZoKB.

Určiť spôsob na dosiahnutie SMART cieľov kybernetickej bezpečnosti vo forme organizačných, personálnych, fyzických a technologických opatrení (napr. ISO 27002:2022) na implementovanie požiadaviek zákona č. 69/2018 Z. z.

Určiť úlohy, povinnosti a zodpovednosti za riadenie kybernetickej bezpečnosti, riadenie aktív, riadenie rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie.

Zaviesť rámec riadenia bezpečnostnej dokumentácie pre celú organizáciu, v rozsahu podľa Príloha č. 2 k vyhláške č. 362/2018 Z. z. B: Štruktúra bezpečnostnej politiky kybernetickej bezpečnosti a personalizovať jednotlivé oblasti.

Vypracovať stratégiu kybernetickej bezpečnosti, ktorá bude adresne popisovať všetkých 8 požiadaviek definovaných v Prílohe č. 1 A vyhlášky 362/2018 Z. z. a tomuto dokumentu prideliť vlastníka, ktorý bude zodpovedať za jej následné udržiavanie, aktualizáciu a uplatňovanie v praxi.

Vypracovať politiky adresujúce všetkých 8 povinných oblastí podľa Prílohy 1 B vyhlášky 362/2018 Z. z. a personalizovať role pre implementáciu a aktualizovanie bezpečnostných politík.

Zadokumentovať rozsah a spôsob plnenia všetkých bezpečnostných opatrení požadovaných zákonom č. 69/2018 Z. z., vyhláškou NBÚ č. 362/2018 Z. z . Pre vyhodnotenie efektívnosti procesov nastaviť jednotlivé KPI.