**Příloha č. 2 výzvy**

**Technická specifikace**

## Předmět veřejné zakázky

Předmětem plnění Veřejné zakázky bude **dodávka softwarových prostředků** pro realizaci systému **řízení informačních rizik** a zvládání bezpečnostních událostí dle **technické specifikace a požadavků na funkcionalitu nástroje** uvedené dále v této příloze.

Předmětem plnění Veřejné zakázky bude dodávka softwarových prostředků a poskytnutí všech potřebných softwarových licencí. Dále pak instalace a implementace systému **řízení informačních rizik** a zvládání bezpečnostních událostíve shodě s požadavky:

* zákona 181/2014 Sb., Zákona o kybernetické bezpečnosti (dále též **ZoKB**)
* vyhlášky Vyhláška č. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti (dále též **VoKB**).
* normy **ISO 27001**, resp. normy řízení rizik informační bezpečnosti **ISO/IEC 27005** a
* směrnice Evropského parlamentu a Rady (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (dále též **NIS2**),

vše v aktuálně platné verzi.

**Využití zdrojů zadavatele:**

Dodávané řešení musí být provozovatelné a bude provozováno na infrastruktuře Zadavatele. Zadavatel umožní vytvoření struktury virtuálních serverů dle potřeb dodávaného řešení na virtualizační platformě **VMware vSphere 8**, včetně funkce VMware HA. Zadavatel dále poskytne licence operačního systému **Microsoft Windows Server 2022 DataCenter** dle požadavků navrženého řešení.

Všechny ostatní licence, nutné pro legální provoz dodávaného řešení na infrastruktuře Zadavatele musí být součástí dodávky.

**Požadované licence**

1. **Softwarový nástroj pro řízení informačních rizik - typ a rozsah**

Rozsah a počet poskytnutých licencí musí pokrýt bezpečnostní role dle zákona 181/2014 Sb., Zákona o kybernetické bezpečnosti, a dále všechny administrátorské role pro správu celého systému či jeho dílčích částí a další role nezbytné pro jeho užití v organizaci. Požadované minimální licenční zajištění je následující:

* minimálně 2x licence pro administrátory celého systému jako celku,
* minimálně 2x licence pro bezpečnostní management řízení rizik a aktiv (např. Manažer kybernetické bezpečnosti a Auditora kybernetické bezpečnosti),
* minimálně 10x licencí pro řízení rizik v celém životním cyklu (od hodnocení až po systém jejich zvládání) pro určený soubor aktiv (též tzv. funkční celek),
* multilicence – licenčně neomezené pro nahlížení a úpravy vedení evidence a hodnocení rizik aktiv kybernetických informačních systémů dle ZoKB (tj. v úrovni dostupnosti, důvěrnosti a integrity), včetně řízení jejich vazeb, pro kontrolní účely a schvalování (např. pro garanty aktiv nebo garanty podnikových procesů,
* multilicenci - licenčně neomezený přístup ke grafickému prostředí popisu struktury podnikových procesů a vazeb na podpůrná aktiva ve smyslu ZoKB, včetně vazeb na vizualizace a hlášení bezpečnostních událostí a incidentů z primárních dohledových systémů organizace.

Tento výčet licencí je obecný a postihuje bezpečnostní role v oblasti **řízení informačních rizik** a zvládání bezpečnostních událostí tak, jak to vnímá Zadavatel. Struktura licencí je věcí Uchazeče, nesmí však omezit uvedený rozsah užití a administrace.

1. **Databázový software - typ a rozsah**

Předmětem dodávky systému řízení informačních rizik jsou rovněž licence databázového systému (např. Microsoft SQL Server) v aktuální verzi. Typ a počet licencí musí odpovídat potřebám poskytovaného řešení.

**Realizace**

Realizace systému **řízení informačních rizik** a zvládání bezpečnostních událostíbude provedena na prostředcích Zadavatele v datovém centru lokality Pardubice.

**Práce**

Součástí plnění předmětu Veřejné zakázky jsou i tyto práce:

* 1. všechny **práce** spojené s realizací díla, zejména pak:
* vypracování vstupního prováděcího plánu projektu (dále jen **Implementační plán projektu**), vč. akceptačních procedur (nutných k provedení akceptace díla) a akceptačních protokolů,
* provedení veškerých úkonů a činností nutných k tomu, aby software mohlo plnit sjednaný či obvyklý účel, zejména:
  + **instalaci** dodávaného SW vybavení na prostředky zadavatele (viz. **Využití zdrojů zadavatele)** ve struktuře schválené v Implementačním plánu projektu,
  + **implementaci** a **vstupní** **nastavení** dodávaného řešení. Vstupním nastavením se rozumí základní nastavení všech procesů realizovaných dodávaným systémem, zejména procesů spojených s:
    - prováděním rizikových analýz a hodnocením rizik,
    - vedením agend všech podpůrných aktiv (ve smyslu zákona o kybernetické bezpečnosti ZoKB),
    - nastavením vizualizačních schémat a pohledů,
    - plánováním a zvládáním řešení bezpečnostních událostí a
    - procesy provádění auditů stavu kybernetické bezpečnosti
    - reportováním

tak, aby systém řízení informačních rizik a zvládání bezpečnostních událostí vytvořil jeden konzistentní funkční celek.

* nastavení jednotných **metodik** a **pracovních** **postupů**.
  1. Specifické činnosti
* zpracování rizikové analýzy a dekompozice podpůrných a primárních aktiv v rozsahu základní analýzy dle ZoKB, včetně vizualizace vazeb
* zpracování podkladů pro interní audit kybernetické bezpečnosti
* zavedení procesů ZoKB a interního auditu do SW nástroje
  1. všechny typy **školení** potřebné pro práci s dodávaným řešením, zahrnuje zejména:
* školení systémových administrátorů, klíčových uživatelů a pracovníků v manažerských pozicích v počtu dle nastavených a obsazených rolí - odhad: do 10 osob

Cíl školení: schopnost samostatné administrace, nastavování systému a zavádění další služeb/aktiv pracovníky Zadavatele

* 1. kompletní **dokumentaci** v elektronické podobě, nezbytné pro použití dodávaného softwarového řešení, která zahrnuje minimálně tuto dokumentaci:
* **Uživatelský manuál** - popisem uživatelských funkcí dodávaného softwarového nástroje
* Dokumentaci pro **administraci** dodávaného řešení
* **Implementační plán projektu**:
* analytická část – návrh realizace Díla a časový harmonogram,
* plán školení administrátorů a dalších uživatelů dle specifických rolí
* finální popis implementace dodávaného řešení (skutečné provedení),
* akceptační procedury,
* akceptační protokoly.
* **Exit plán** – plán o řízeném ukončení spolupráce,

**Technická specifikace a požadavky na funkcionalitu nástroje**

**pro řízení informačních rizik a zvládání bezpečnostních událostí**

Uvedené požadavky jsou, pokud není uvedeno jinak, minimální.

Označení **dodávané řešení, řešení, systém** jsou rovnocenné.

Všechny požadované funkce musí být dodány v rámci dodávky a být přístupné bez dalších nákladů, a to včetně požadavků (funkcí) formulovaných jako „Možnost, schopnost, …“.

|  |  |  |
| --- | --- | --- |
| **Požadovaná funkcionalita**  Minimální nepodkročitelné požadavky | | **Splnění**  Ano/Ne |
| **A** | **Základní požadavky** |  |
| 1 | Dodávané řešení musí zahrnovat podporu pro: |  |
|  | komplexní řízení rizik v kybernetickém prostoru organizace |  |
|  | řízení vazeb aktiv a procesů, vč. vizualizace struktury aktiv a vazeb |  |
|  | automatizovaná podpora pro řízení událostí a incidentů, vč. systému notifikací |  |
|  | podpora tvorby plánu zvládání rizik |  |
|  | řízení auditních procesů |  |
|  | podpora pro řízení podnikových procesů (BCM, business continuity management) |  |
|  | řízení business impact analýzy (BIA) |  |
|  | řízení dokumentace dle přílohy č. 5 VoKB |  |
|  |  |  |
| 2 | Dodávané řešení musí zahrnovat podporu pro řízení podpůrných aktiv v rozsahu vyžadovaném zákonem zákon 181/2014Sb. Zákon o kybernetické bezpečnosti (technická aktiva, lidské zdroje, dodavatelé) |  |
| 3 | Dodávané řešení musí být ve shodě se zákonnými normami či předpisy, **v aktuálním znění**, zejména pak: |  |
|  | zákon 181/2014Sb. Zákon o kybernetické bezpečnosti |  |
|  | vyhláška 82/2018Sb. Vyhláška o kybernetické bezpečnosti |  |
|  | dokument NÚKIB - POMŮCKA K AUDITU BEZPEČNOSTNÍCH OPATŘENÍ PODLE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI v aktuální verzi |  |
|  | norma ISO/IEC 27001 (ISMS) |  |
|  | GDPR |  |
| 3 | Shoda s výše uvedenými se zákonnými normami a předpisy musí být zajištěna po celou dobu užití dodávaného řešení s podporou servisní smlouvy (viz. Příloha č. 4 - Smlouva o poskytování servisních služeb). |  |
| 4 | Systém musí být připraven na implementaci normy NIS2 |  |
| 5 | Systém musí podporovat češtinu, a to jak v části popisné (obsah jednotlivých polí), tak v části funkční (menu, funkce, popisy) |  |
|  |  |  |
| **B** | **Obecné požadavky** |  |
| 1 | Systém musí mít implementováno řízení rolí a přístupů. |  |
| 2 | Systém musí umět diverzifikovat přístupy dle organizačního členění a dle přidělených funkčních oblastí (maticová struktura přístupu do systému) |  |
| 3 | Systém musí být napojen na systém řízení přístupů AD/LDAP Zadavatele. |  |
| 4 | Musí být schopen pracovat s identitami i samostatně, bez tohoto napojení na systémy AD/LDAP |  |
| 5 | Systém řízení rizik musí ve všech oblastech umět hierarchickou strukturu řízení organizace včetně případných podřízených nebo přímo řízených organizací |  |
| 6 | Systém zabezpečení opatření musí být schopen vizualizovat události a incidenty v kontextu organizačního členění |  |
| 7 | Systém musí umět reportovat za jakoukoli řízenou oblast (lokalitu), a to jak dle kategorie rizika, organizační jednotky, tak dle hodnocení rizika |  |
| 8 | Systém musí udržovat celou historii změn jednotlivých položek, včetně vazeb. |  |
| 9 | Systém musí umožnit časové workflow úkolů, hlídat upozorňovat na určené milníky řešení či důležité termíny, a ukázat postup aktivit v kalendářovém pohledu |  |
| 10 | Součástí dodávaného řešení je integrovaný systém správy dokumentů, které jsou vytvářeny či generovány systémem, tj. systém disponuje vlastní správou dokumentů |  |
| 11 | Systém musí podporovat řízení celého životního cyklu bezpečnostní dokumentace. |  |
| 11 | Systém umožní připojovat dokumentaci k libovolnému základnímu prvku řízení rizik |  |
| 12 | Umožní připojovat foto a video dokumentaci k zjištěným bezpečnostním událostem a incidentům |  |
| 13 | Systém musí podporovat tvorbu dokumentace pro auditní řízení. |  |
| 14 | Systém musí mít možnost importu a exportu informací z a do systému MS Excel |  |
|  |  |  |
| **C** | **Řízení aktiv** |  |
| 1 | Systém musí vést registr aktiv dle kybernetického zákona a ve shodě s registrem ICT aktiv organizace |  |
| 2 | Základní evidenční údaje o aktivech dle politik a požadavků organizace a údaje o aktivech z hlediska kybernetického zákona (dostupnost, důvěrnost, integrita) |  |
| 3 | Systém musí vést záznamy vazeb aktiv na rizika |  |
| 4 | Systém musí vést záznamy vazeb aktiv na zjištěné bezpečnostní události a incidenty |  |
| 5 | Systém musí umožnit provádění reportingu o aktivech a přiřazených záznamech (rizika, incidenty atd.) |  |
| 6 | Systém musí umožnit vedení popisu o organizační struktuře organizace a jednoduše realizovat případné změny v této struktuře |  |
| 7 | Systém musí vést záznamy o vazbách aktiv na organizační strukturu (zodpovědného pracovníka (administrátor aj.)) |  |
| 8 | Systém musí umožnit rozpad organizační struktury podle fyzického členění organizace i podle business procesů organizace |  |
|  |  |  |
|  |  |  |
| **D** | **Řízení vazeb aktiv** |  |
| 1 | Systém řízení vazeb aktiv musí umět zobrazovat hierarchickou strukturu aktiv dle požadavků zadavatele (pohled přes číselníky) |  |
| 2 | Systém musí umožňovat definovat vazby mezi primárními (data, procesy) a podpůrnými aktivy (technická aktiva, dodavatelé a zaměstnanci, prostory) |  |
|  |  |  |
| **E** | **Vizualizační vrstva a připojení fyzických aktiv** |  |
| 1 | Systém řízení vazeb aktiv musí ve všech oblastech umět vizualizovat strukturu aktiv a to ve fyzické struktuře v logice podnikových procesů organizace |  |
| 2 | Systém musí umožňovat připojovat k těmto aktivům i stavy aktiv v aktuálním IT prostředí, zejména pak události, incidenty, logy a stavy fyzické bezpečnosti a vizualizovat to |  |
| 3 | Systém musí být schopen vizualizovat stavy jednotlivých aktiv z pohledu Business continuity managementu a řízení dodavatelských řetězců |  |
| 4 | Systém vizualizace musí změny ve struktuře aktiv a jejich vazeb promítal automaticky do vizualizačních výstupů |  |
|  |  |  |
| **F** | **Řízení informačních rizik** |  |
| 1 | Systém musí podporovat minimálně tyto procesy: |  |
|  | Vedení registru rizik |  |
|  | Hodnocení rizika |  |
|  | Snižování (minimalizace) rizika |  |
|  | Plán zvládání bezpečnostních událostí (resp. plán nápravných opatření) |  |
|  | Vedení historie rizika |  |
|  | Řízení zbytkových rizik (Promítnutí protiopatření do hodnocení rizika) |  |
|  | Systemizace rizik dle uživatelem definovaných kategorií |  |
| 2 | Systém musí podporovat vedení registru zranitelností s možností uživatelské modifikace |  |
| 3 | Systém musí podporovat vedení registru hrozeb s možností uživatelské modifikace |  |
| 4 | Systém musí poskytovat centrální portál (dashboard), který zobrazuje konzistentně základní informace o rizicích |  |
| 5 | Možnost automatického generování záznamů o rizicích a plánech zvládání pro účely auditu, včetně vazby na hodnotu rizika |  |
| 6 | Možnost slučování rizik do skupin dle požadavků uživatelů systému |  |
| 7 | Možnost jednotného přiřazování a vedení plánů nápravných opatření pro jednotlivá rizika i skupiny rizik |  |
| 8 | Sledování rizik dle struktury aktiv po jednotlivých aktivech vzestupně a sestupně |  |
| 9 | Možnost definovat omezený rozsah přístupu pro obecného uživatele systému řízení rizik (např. pro účely hodnocení rizik) |  |
| 10 | Schopnost provázání rizik na: |  |
|  | Incidenty |  |
|  | Audity |  |
|  | Aktiva |  |
|  | Organizační strukturu |  |
|  | Základní ekonomické informace |  |
|  | Definované procesy |  |
|  | Jednorázové aktivity |  |
|  |  |  |
| 11 | Systém musí vytvářet auditní stopu rizika, tj. vést záznam o vývoji rizika v čase |  |
| 12 | Možnost komentáře k riziku v případě změny hodnocení rizika (doplněk k auditní stopě) |  |
| 13 | Vestavěný základní reporting o rizicích, včetně statistik |  |
|  |  |  |
|  |  |  |
| **G** | **Řízení incidentů** |  |
| 1 | Systém musí umožnit vedení registru incidentů a vazbu incidentu na riziko |  |
| 2 | Systém musí umožnit investigaci incidentů a řízení workflow řešení incidentů |  |
| 3 | Systém musí umožnit vedení plánů opatření k incidentům |  |
| 4 | Systém musí mít implementován alerting a notifikační procesy k incidentům a rizikům |  |
| 5 | Dodávané řešení musí poskytnout možnost reportingu o incidentech, včetně statistik |  |
|  |  |  |
| **H** | **Řízení auditních procesů** |  |
| 1 | Evidence auditů a vedení historie auditů |  |
| 2 | Plánování auditů |  |
| 3 | Vedení odpovědných osob v rámci auditního řízení ve vztahu k jednotlivým oblastem auditu |  |
| 4 | Evidence auditních nálezů |  |
| 5 | Podpora vedení auditních činností |  |
| 6 | Generování auditních zpráv |  |
| 7 | Reporting o auditech včetně statistik |  |
| 9 | Nastavení systému auditu dle podmínek pro audit kybernetické bezpečnosti dle NÚKIB |  |
|  |  |  |
| **I** | **Integrace** |  |
| 1 | Povinná integrace na systém řízení přístupu (AD, LDAP) organizace |  |
| 2 | Povinná integrace se systémem Alvao Helpdesk a Alvao Asset Management |  |
| 3 | Systém musí být otevřený k případné integraci s dalšími bezpečnostními systémy, jako: |  |
|  | Nástroje SIEM |  |
|  | Nástroje EDR/XDR |  |
|  | Dokument management systém (DMS) |  |
|  |  |  |
| **J** | **Statistické a analytické funkce** |  |
| 1 | Systém musí nabízet možnost tvorby samostatných reportů dle požadavků zadavatele, muže být i samostatných systémem typu BI (business inteligence) |  |
| 2 | Systém může být využit i jako samostatný systém typu BI |  |
| 3 | Systém musí umožnit sledovat souvislosti a vazby mezi oblastmi rizikového řízení (statické a dynamické funkce) |  |
| 4 | Systém musí umožnit možnost zavedení systému řízení kvality formou hodnocení KPI dle plnění řízení rizik |  |
| 5 | Systém musí nabízet možnost tvorby uživatelsky definovaných výkazů a reportů |  |
|  |  |  |
|  |  |  |
| **K** | **Podpora pro řízení kontinuity podnikových procesů (BCM) a dodavatelů** |  |
| 1 | Řešení musí zahrnovat podporu pro řízení podnikových procesů a řízení jejich kontinuity a odolnosti |  |
| 2 | Řešení musí podporovat provádění dopadových analýz (BIA analýzy) a hodnotit aktiva z tohoto pohledu. |  |
| 3 | Řešení musí podporovat procesy pro řízení obnovy (disaster recovery procesy, DRP) |  |
| 4 | Řešení musí podporovat životní cyklus řízení dodavatelů v celém životním cyklu, včetně identifikace a hodnocení? |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Zadavatel uvádí, že v rámci budoucího rozvoje může požadovat integraci na využívané systémy detekce bezpečnostních událostí viz. tabulka.

Tento možný rozvoj je zde uveden pouze indikativně a není součástí této poptávky.

|  |  |  |
| --- | --- | --- |
| **L** | **Možnost integrace na systémy detekce bezpečnostních událostí minimálně:** |  |
|  | Zabbix (detekce provozních událostí) |  |
|  | LogManager (sběr a archivace logů) |  |
|  | FlowMon (datové toky) |  |
|  | FortiAnalyzer (perimetr sítě) |  |