**Příloha č. 3 zadávací dokumentace**

# Požadavky na funkcionalitu nástroje pro řízení informačních rizik

Uvedené požadavky technické specifikace a požadavky na **funkcionalitu nástroje pro řízení informačních rizik a zvládání bezpečnostních událostí** 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 264/2025Sb. Zákon o kybernetické bezpečnosti |  |
|  | vyhláška č. 409/2025 Sb., Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností vyhláška |  |
|  | dokument NÚKIB - POMŮCKA K AUDITU BEZPEČNOSTNÍCH OPATŘENÍ PODLE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI v aktuální verzi |  |
|  | s normou ISO/IEC 27001 (ISMS) |  |
|  | s normou ISO/IEC 22301 |  |
|  | GDPR |  |
|  | Zákon 266/2025Sb. zákon o kritické infrastruktuře |  |
|  | CER (Critical Entity Resilience Directive) - Směrnice Evropského parlamentu a Rady EU 2022/2557 o odolnosti kritických subjektů |  |
|  |  |  |
| 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 zadávací dokumentace Příloha č. 4 - Smlouva o poskytování servisních služeb). |  |
| 4 | Systém musí být připraven na implementaci normy CER |  |
| 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 interní 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. |  |
| 12 | Systém umožní připojovat dokumentaci k libovolnému základnímu prvku řízení rizik |  |
| 13 | Umožní připojovat foto a video dokumentaci k zjištěným bezpečnostním událostem a incidentům |  |
| 14 | Systém musí podporovat tvorbu dokumentace pro auditní řízení. |  |
| 15 | 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) |  |
| 3 | Systém musí umožňovat řídit grafické zobrazení vazeb vlastním grafickým rozhraním bez použití dalšího externího systému |  |
|  |  |  |
| **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 tuto skutečnost |  |
| 3 | Systém musí být schopen vizualizovat stavy jednotlivých aktiv z pohledu Business kontinuity 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 bezpečnostních událostí a incidentů** |  |
| 1 | Systém musí umožnit vedení registru bezpečnostních událostí a incidentů a jejich vazbu na riziko a příslušné aktivum |  |
| 2 | Systém musí umožnit investigaci bezpečnostních událostí a incidentů a řízení jejich řešitelského workflow |  |
| 3 | Systém musí umožnit vedení plánů zvládání k bezpečnostním událostem a incidentům |  |
| 4 | Systém musí mít implementován alerting a notifikační procesy k bezpečnostním událostem a incidentům a rizikům |  |
| 5 | Dodávané řešení musí poskytnout možnost reportingu o bezpečnostních událostech a incidentech, včetně statistik |  |
| 6 | Dodávané řešení musí poskytnout možnost tvorby formulářů o povinném hlášení těchto událostí na příslušné orgány státu |  |
|  |  |  |
| **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 | Povinná integrace se systémem SIEM |  |
|  |  |  |
| **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? |  |
|  |  |  |
|  |  |  |
| **L** | **Systém řízení bezpečnostní dokumentace** |  |
| 1 | Řízení dokumentace musí být součástí systému řízení bezpečnosti. |  |
| 2 | Dodávané řešení musí být obsahovat vlastní integrovaný systém DMS. |  |
| 3 | Integrovaný systém DMS musí umožňovat připojení dokumentu k libovolné entitě systému řízení bezpečnosti (rizika, opatření, aktiva, audit, incident). |  |
| 4 | Integrovaný systém DMS musí umožňovat sledování stavu dokumentu. |  |
| 5 | Integrovaný systém DMS musí umožňovat zasílání notifikací při vzniku či změně dokumentu. |  |
|  |  |  |
| **M** | **Podpora pro nezávislé řízení rizik samostatných organizačních subjektů** |  |
| 1 | Dodávané řešení musí podporovat reřim multi-entity/multi-tenant management pro řízení rizik samostatných organizačních subjektů nebo organizací. |  |
| 2 | Software musí umožňovat samostatné vedení agendy rizik pro více organizací/subjektů v rámci jednotného systému. Každá organizace musí mít možnost spravovat svá rizika, plány opatření a reporting nezávisle na ostatních. |  |
| 3 | Systém musí zajistit oddělení dat a plnou datovou izolaci mezi jednotlivými organizacemi; uživatelé jedné organizace nesmí mít přístup k datům jiné organizace, pokud to není výslovně povoleno v rámci nastavení rolí. |  |
| 4 | Systém musí umožňovat centrální dohled a správu všech zapojených organizací z úrovně nadřazeného uživatele (supervizora nebo centrálního administrátora), který bude mít přehled o všech rizicích napříč organizacemi. |  |
| 5 | Software musí obsahovat flexibilní pokročilý systém řízení rolí a oprávnění (role-based access control), který umožní přesně definovat, kdo má přístup k jakým datům, funkcím a reportům, a to jak v rámci jedné organizace, tak mezi organizacemi a supervizorem. |  |
| 3 | Systém musí podporovat koordinované řízení rizik napříč více spolupracujícími subjekty (např. členy sdružení, holdingem, konsorciem apod.), včetně možnosti sdílení vybraných informací podle nastavených pravidel. |  |
| 7 | Systém musí podporovat možnost agregace dat a reportingu, musí být možné zobrazit a exportovat souhrnné přehledy rizik z více organizací současně, včetně konsolidovaných metrik a ukazatelů pro potřeby vedení nebo supervizora. |  |
|  |  |  |
| **N** | **Soulad se Zákonem č. 266/2025 Sb., Zákon o odolnosti subjektů kritické infrastruktury** |  |
| 1 | Zmapování a správa aktiv kritické infrastruktury Software musí umožnit evidenci a kategorizaci aktiv, zařízení, sítí a systémů, které jsou zařazeny jako součást kritické infrastruktury, včetně jejich lokalizace, popisu funkce a závislostí. |  |
| 2 | Systém musí podporovat proces identifikace, analýzy a hodnocení rizik souvisejících s odolností subjektu kritické infrastruktury, včetně identifikace závislostí a meziodvětvových vazeb. |  |
| 3 | Systém musí umožnit plánování, sledování a vyhodnocování opatření směřujících ke zvýšení odolnosti, nejen technických, ale i organizačních, procesních a návazných na strategii |  |
| 4 | Systém musí mít definovaný mechanismus přiřazení práv, rolí a odpovědností (kdo a co spravuje, kdo má dohled) tak, aby bylo zajištěno, že útvary kritické infrastruktury mají jasně určenou odpovědnost za řízení odolnosti |  |
| 5 | Systém musí podporovat evidenci a správu incidentů či výpadků základních služeb, jejich analýzu a nápravná opatření – včetně možnosti zasílat/reportovat podněty státním orgánům dle zákona. |  |
| 6 | Software by měl umožnit export/reporting k tvorbě rámce strategie odolnosti, vyhodnocování plnění opatření, spolupráci s orgány státní správy. |  |
|  |  |  |

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 veřejné zakázky.

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