Příloha č. 3

Smlouvy o zajištěni dodávky a podpory systému pro správu aktiv a rizik

Požadavky na systém řízení aktiv a rizik

Následující kapitoly uvádí základní požadavky Objednatele na informační systém pro správu aktiv a rizik organizace. Cílem informačního systému je řádné řízení a správa aktiv a rizik obecných (finančních, personálních, projektových, BOZP a PO, GDPR, strategických…) a informačních/kybernetických dle platných legislativních a normativních požadavků za podmínek stanovených touto smlouvou.

Normativní a právní východiska systému řízení rizik (informačních):
- norma EN ISO/IEC 27001:2022 Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí;
- zákon č. 181/2014 Sb. o kybernetické bezpečnosti a návazných vyhlášek v platném znění;

Další právní východiska systému řízení rizik:
- zákon č.320/2001 Sb. o finanční kontrole ve veřejné správě;
- zákon č. 262/2006 Sb. Zákoník práce;
- nařízení Evropského parlamentu a Rady (EU) č. 2016/679, ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů;
- nařízení Komise v přenesené pravomoci (EU) 2022/127 ze dne 7. prosince 2021, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2021/2116 o pravidla týkající se platebních agentur a dalších subjektů, finančního řízení, schválení účetní závěrky, jistot a použití eura (oblast rizik upravena především v Příloze č. 1 nařízení, část 1. C – Posouzení rizik);
- usnesení vlády ČR č. 752, k Rámcovému rezortnímu internímu protikorupčnímu programu (RRIPP), z 2. 10. 2013 v návazných aktualizacích;

Uživatelé systému řízení aktiv a rizik (dále jen systému) jsou požadováni v min. rozsahu:
- administrátor / risk manažer (full R/W - Read and write);
- vrcholový risk management (R/O - Read only);
- vlastník rizika/aktiva (R/O - Read only);
- analytik rizika (R/W - Read and write);
- vlastník opatření (R/O - Read only);

1.1.1. Přehled požadavků na funkcionality systému

Zadavatel požaduje zejména tyto základní funkcionality systému:

Číslo	Vlastnost	Splňuje ANO/NE
1.	Evidence a administrace informačních aktiv a vazeb mezi nimi.	ANO
2.	Evidence a administrace informačních/kybernetických rizik organizace včetně katalogu těchto rizik.	ANO
3.	Evidence a administrace obecných rizik organizace, včetně katalogů těchto rizik (referenční seznam rizik).	ANO
4.	Evidence a administrace uživatelů tohoto systému v synchronizaci s MS Active Directory v IS Objednatele.	ANO
5.	Evidence a administrace požadavků Zákona o kybernetické bezpečnosti a normy ISO/IEC 27001 včetně jejich vazeb na informační aktiva, kterých se tyto požadavky týkají.	ANO
6.	Systém musí umět vytvářet nastavitelné datové sestavy/reporty s využitím filtračních nástrojů. Výstup je textový a grafický formát.	ANO
7.	Systém musí umět vytvářet, zachovávat a dostatečně chránit auditní stopu o všech změnách v systému. Evidence a zobrazování historie změn dat a jejich autory.	ANO
8.	Systém musí umět exportovat/importovat data o rizicích do souborů formátu CSV, XML nebo XLS.	ANO
9.	Systém musí používat databázové úložiště Microsoft SQL.	ANO
10.	Systém musí umět v případě potřeby rozšířit počet atributů na jednotlivých kartách hodnocení aktiv a rizik.	ANO
11.	Systém musí umět vytvářet a odesílat nastavitelné uživatelské notifikace např. o založení / změně hodnocení, nastavených termínech aktualizací u rizik a aktiv.	ANO
12.	Obsah notifikací a podmínky jejich generování musí umožnit libovolné nastavování a zapínání/vypínání.	ANO
13.	Evidence a administrace bezpečnostních událostí a incidentů ve vztahu k informačním aktivům.	ANO
14.	Evidence a administrace požadavků BCM (Business Continuity Management) vůči informačním aktivům, včetně jejich vazeb na tato aktiva. Základním nástrojem pro evidenci a administraci požadavků může být např. Karta požadavků BCM.	ANO
15.	Systém umí vytvářet a odesílat nastavitelné uživatelské notifikace na emailovou adresu o provedených změnách v hodnocení aktiv a rizik.	ANO

1.1.2. Požadavky na evidenci a správu aktiv

číslo	Vlastnost	Požadované parametry	Splňuje ANO/NE
1.	Řízení aktiv	Evidence a správa Primárních aktiv (PA)	ANO
2.		Evidence a správa Podpůrných aktiv (PodA)	ANO
3.		Evidence Garantů aktiv	ANO
4.		Hodnocení PA Hodnoty důvěrnosti, integrity a dostupnosti, vypočtená a upravitelná MDA mohou nabývat hodnot 1-4, které jsou barevně odlišeny, např.: 1-zelená, 2-žlutá, 3-oranžová, 4-červená	ANO
5.		Evidence vazeb a hodnocení mezi PA a PodA	ANO
6.	Karta aktiva	ID (generuje systém)	ANO
7.		Název aktiva (text)	ANO
8.		Vlastník aktiva (zdroj, systém se integruje na MS Active Directory)	ANO
9.		Popis aktiva (text)	ANO
10.		Typ/kategorie aktiva (např. rozevírací seznam): - Primární aktivum – informace - Primární aktivum – služba - Podpůrné aktivum – technické - Podpůrné aktivum – organizace - Podpůrné aktivum – dodavatel *Poznámka: Kategorie musí systém umožňovat editovat.*	ANO
11.		Klasifikace aktiva (např. rozevírací seznam): - Veřejné - Interní - Diskrétní	ANO ANO
12.		Hodnotící schéma aktiva (nabývá hodnot 1-4)	ANO
13.		Komentář k aktivu (text)	ANO
14.		Lokalizace/umístění aktiva u PodA (např. text)	ANO
15.		Status Významný dodavatel u PodA a Služeb ANO – NE	ANO

16.		Vazbová položka (vazba aktiva na jiná aktiva)	ANO
17.		Datum založení karty aktiva (datum)	ANO
18.		Datum poslední aktualizace karty aktiva (datum)	ANO
19.		Datum příští revize karty aktiva (datum)	ANO
20.	Hodnotící schéma aktiv	Důvěrnost („Dů“ nabývá hodnot 1-4, barevně odlišeno např. zelená, žlutá, oranžová, červená)	ANO
21.		Dostupnost („Do“ nabývá hodnot 1-4, barevně odlišeno např. zelená, žlutá, oranžová, červená)	ANO
22.		Integrita („Int“ nabývá hodnot 1-4, barevně odlišeno např. zelená, žlutá, oranžová, červená)	ANO
23.		Průběžná MDA (míra důležitosti aktiva) je vypočtená dle převodové tabulky automaticky dle vzorce „Dů x Do x Int“. Pokud je vypočtena systémem automaticky musí být možnost manuální úpravy hodnoty: vzor např.: - 1-15 = 1 (barva zelená) - 16-31 = 2 (barva žlutá) - 32-47 = 3 (barva oranžová) - 48-64 = 4 (barva červená)	ANO
24.		Musí umožnit vložení slovního komentáře autora změny k provedené úpravě finální MDA.	ANO
25.	Přístup k aktivům	Přístup k aktivům je řízen zavedením min. role: Manažer rizik (R/W - Read and write) Vlastník aktiva (R/O - Read only)	ANO
26.	Reporty aktiv	Příjemce reportů je uživatel nebo skupina uživatelů.	ANO
27.		Tvorba reportu ze seznamu registrovaných aktiv musí umožnit nastavit rozsah reportovaného seznamu (přes celé portfolio aktiv či jen přes zvolenou oblast/skupinu aktiv).	ANO
28.		Tvorba reportu ze seznamu Vlastníků aktiv přes celé portfolio aktiv či přes zvolenou skupinu aktiv.	ANO
29.		Tvorba reportu ze seznamu informačních aktiv, na která je vázáno konkrétní informační riziko.	ANO

30.		Tvorba reportu ze seznamu informačních aktiv, na která je vázána konkrétní hrozba nebo zranitelnost.	ANO
31.		Systém musí umožnit vytváření další typy reportů aktiv dle požadavku Zadavatele.	ANO
32.		Systém musí umožňovat rozesílat dané reporty na definované emaily v definovaných intervalech.	ANO

1.1.3. Evidence a správa rizik

Požadovaný systém musí umět evidovat a administrovat rizika v souladu s platnou legislativou, normativou a ostatními požadavky, zejména:

Číslo	Vlastnost	Požadované parametry	Splňuje ANO/NE
1.	Řízení rizik	Systém musí umět rozlišovat dva typy karet: A) kartu rizika pro rizika informační B) kartu rizika pro rizika obecná *Poznámka: Tyto typy se liší obsahem položek a hodnotícím schématem.*	ANO
2.		U obecných rizik se na Kartě zobrazují povinné hodnoty pravděpodobnosti, dopadu a výslednou vypočtenou hodnotu Indexu rizika (IR).	ANO
3.		U informačních rizik zobrazují povinné hodnoty hrozby, zranitelnosti, dopadu a výslednou vypočtenou hodnotu indexu rizika (IR).	ANO
4.		Hodnoty pravděpodobnosti, dopadu a indexu rizika u obecných rizik, resp. hrozby, zranitelnosti, dopadu a indexu rizika u informačních rizik mohou nabývat hodnot 1-4, které jsou barevně odlišeny např.: - 1-zelená - 2-žlutá - 3-oranžová - 4-červená	ANO
5.		Systém musí být schopen vytvářet a evidovat vazby mezi jednotlivými riziky, zejména v případě obecných rizik. Dále musí umět propojit informační rizika s aktivy, ke kterým se tato rizika vztahují (tzv. také na složky organizační struktury.	ANO
6.		Role Vlastníka rizika musí umožňovat min. náhled do Karty rizika a na strukturu vlastněných rizik, v případě rizik informačních včetně vazeb na propojená aktiva.	ANO

7.		Role Analytika rizik musí umožňovat administraci (přepis) Karet rizik.	ANO
8.	Položky karty rizika – riziko OBECNÉ (v závorce typ pole)	ID rizika (generuje systém)	ANO
9.		Název rizika (text)	ANO
10.		Vlastník rizika (zdroj MS Active Directory)	ANO
11.		Analytik rizik (zdroj MS Active Directory)	ANO
12.		Risk management (zdroj MS Active Directory)	ANO
13.		Stav rizika (např. rozevírací seznam)	ANO
14.		Popis rizika (text)	ANO
15.		Dopad rizika (text)	ANO
16.		Datum založení karty rizika (datum)	ANO
17.		Datum poslední aktualizace karty rizika (datum)	ANO
18.		Datum příští revize karty rizika (datum)	ANO
19.		Poznámky k riziku (text)	ANO
20.		Hodnotící schéma obecných rizik (hodnoty 1-4)	ANO
21.		Poznámky k hodnocení rizika (text)	ANO
22.		Datum poslední aktualizace hodnocení rizika (datum)	ANO
23.		Název plánu k ošetření rizika (text)	ANO
24.		Bližší popis plánu (text)	ANO
25.		Datum založení plánu (datum)	ANO
26.		Datum poslední aktualizace plánu (datum)	ANO
27.		Název opatření k ošetření rizika (text)	ANO
28.		ID opatření (generuje systém)	ANO
29.		Vlastník opatření (zdroj MS Active Directory)	ANO
30.		Stav opatření (např. rozevírací seznam)	ANO

31.		Typ opatření (např. rozevírací seznam)	ANO
32.		Popis opatření (text)	ANO
33.		Datum založení/zahájení opatření (datum)	ANO
34.		Datum skutečného zavedení / ukončení opatření (datum)	ANO
35.		Datum poslední aktualizace opatření (datum)	ANO
36.	Položky karty rizika – riziko INFORMAČNÍ (v závorce typ pole)	ID rizika (generuje systém)	ANO
37.		Název rizika (text)	ANO
38.		Vlastník rizika (zdroj MS Active Directory)	ANO
39.		Analytik rizik (zdroj MS Active Directory)	ANO
40.		Risk management (zdroj MS Active Directory)	ANO
41.		Stav rizika (rozevírací seznam)	ANO
42.		Popis rizika (text)	ANO
43.		Dopad rizika (text)	ANO
44.		Datum založení karty rizika (datum)	ANO
45.		Datum poslední aktualizace karty rizika (datum)	ANO
46.		Datum příští revize karty rizika (datum)	ANO
47.		Poznámky k riziku (text)	ANO
48.		Hodnotící schéma informačních rizik	ANO
49.		Hrozba (např. rozevírací seznam)	ANO
50.		Zranitelnost (např. rozevírací seznam)	ANO
51.		Poznámky k hodnocení rizika (text)	ANO
52.		Datum poslední aktualizace hodnocení rizika (datum)	ANO
53.		Název plánu k ošetření rizika (text)	ANO
54.		Bližší popis plánu (text)	ANO

55.		Datum založení plánu (datum)	ANO
56.		Datum poslední aktualizace plánu (datum)	ANO
57.		Název opatření k ošetření rizika (text)	ANO
58.		ID opatření (generuje systém) *Poznámka: Riziko může být ošetřeno více opatřeními.*	ANO
59.		Vlastník opatření (zdroj MS Active Directory)	ANO
60.		Stav opatření (např. rozevírací seznam)	ANO
61.		Typ opatření (např. rozevírací seznam)	ANO
62.		Popis opatření (text)	ANO
63.		Datum plánovaného založení / zahájení opatření (datum)	ANO
64.		Datum plánovaného ukončení / zavedení opatření (datum)	ANO
65.		Datum poslední aktualizace opatření (datum)	ANO
66.	Seznamy hrozeb a zranitelností	Systém musí umět evidovat a administrovat seznamy hrozeb a zranitelností	ANO
67.		Jednotlivé hrozby a zranitelnosti v seznamech musí být editovatelné a musí být opatřeny pořadovým číslem v seznamu, a lze měnit jejich pořadí.	ANO
68.		Seznamy hrozeb a zranitelností se musí zobrazovat např. jako rozevírací seznamy při vyplňování položek hrozba a zranitelnost v kartě informačního rizika.	ANO
69.	Katalogy rizik	Systém musí umět evidovat katalogy/referenční seznamy min. těchto kategorií rizik:	
70.		- Rizika BOZP-PO	ANO
71.		- Rizika Finanční	ANO
72.		- Rizika GDPR	ANO
73.		- Rizika Operativní	ANO
74.		- Rizika Korupce	ANO
75.		- Rizika Podvodů a nesrovnalostí	ANO
76.		- Rizika Projektová	ANO
77.		- Rizika Strategická	ANO
78.		- Rizika Personální	ANO

79.		- Rizika Informační	ANO
80.		Přístupy do katalogů rizik musí být nastaveny takto:	
81.		- Role Garant katalogu (přepis stávajících katalogových rizik a zakládání nových rizik do katalogu)	ANO
82.		- Manager rizik (právo vytvářet kopie katalogových rizik ve složkách organizační struktury nebo aktivech)	ANO
83.		- Všichni uživatelé systému (náhled).	ANO
84.		Systém musí umět vytvářet a evidovat vazby katalogových rizik na jejich kopie v systému („živá“ rizika).	ANO
85.	Hodnotící schéma rizika – riziko OBECNÉ	Pravděpodobnost (P)	ANO
86.		Dopad (D)	ANO
87.		Vypočtený index rizika IR dle vzorce (P x D) a upravený dle převodové tabulky např.: 1-3 = 1 4-8 = 2 9-15 = 3 16 = 4	ANO
88.	Hodnotící schéma rizika – riziko INFORMAČNÍ	Hrozba (H)	ANO
89.		Zranitelnost (Z)	ANO
90.		Dopad (D)	ANO
91.		Vypočtený index rizika IR dle vzorce (H x Z x D) a upravený dle převodové tabulky např.: 1-3 = 1 4-15 = 2 16-36 = 3 37-64 = 4	ANO
92.	Přístupy k rizikům	Přístup k rizikům je řízen zavedením rolí:	
93.		- Vlastník aktiva (náhled)	ANO
94.		- Analytik rizik (přepis)	ANO
95.		- Risk management (náhled)	ANO
96.		- Vlastník opatření (náhled)	ANO

1.1.4. Evidence a správa uživatelů systému

Číslo	Vlastnost	Požadované parametry	Splňuje ANO/NE
1.	Řízení uživatelů	Systém musí umět evidovat a administrovat uživatele systému - Karta uživatele	ANO
2.		Systém musí umět automaticky integrovat/synchronizovat karty uživatelů s MS Active Directory Zadavatele.	ANO
3.		Oprávnění k této integraci má výhradně role Administrátora systému.	ANO
4.	Přístup uživatelů k systému	Systém musí umět rozlišovat minimálně tyto role opravňující k přístupu do systému:	
5.		- Administrátor (právo konfigurovat volitelné parametry systému)	ANO
6.		- Manager rizik (právo přepisu všech dat v systému či v určené oblasti)	ANO
7.		- Vlastník aktiva (přepis v kartě přiděleného aktiva)	ANO
8.		- Vlastník rizika (náhled do karty přiděleného rizika)	ANO
9.		- Analytik rizik (přepis v kartě přiděleného rizika)	ANO
10.		- Vrcholový risk management (náhled do karty přiděleného rizika)	ANO
11.		- Vlastník opatření (náhled do karty rizika s přiděleným opatřením)	ANO
12.	Karta uživatele	Položky karty uživatele musí minimálně obsahovat:	
13.		- Jméno (zdroj MS Active Directory)	ANO
14.		- Příjmení (zdroj MS Active Directory)	ANO
15.		- ID zaměstnance (generuje systém)	ANO
16.		- Služební číslo zaměstnance (zdroj MS Active Directory)	ANO
17.		- Umístění v organizaci – organizační jednotka (zdroj MS Active Directory)	ANO
18.		- Služební email (zdroj)	ANO
19.		- Přiřazené skupiny/grupy	ANO
20.		- Souhrnné notifikace (ano – ne)	ANO
21.		- Komentáře/Poznámky (text)	ANO

22.		- Role (rozevírací seznam)	ANO
23.		- Bezpečnostní přehled (zobrazí oprávnění uživatele)	ANO
24.		- Předání vlastnictví (po aktivaci dojde k přepisu všech nebo vybraných oprávnění na zvoleného jiného uživatele).	ANO