Dokumentace podpory provozu informačního systému

Popis a nastavení systému

**pro**

**projekt DTM**

Verze 0.1

ICZ a.s.

Copyright ICZ a.s.

Žádná část tohoto dokumentu nesmí být kopírována žádným způsobem bez písemného souhlasu majitelů autorských práv. Autorská a jiná díla odvozená z tohoto díla podléhají ochraně autorských práv vlastníků.

Některé názvy produktů a společností citované v tomto díle mohou být ochranné známky příslušných vlastníků.

Obsah

[1 Popis a nastavení systému 4](#_Toc108685403)

[1.1 Verze dokumentu 4](#_Toc108685404)

[1.2 Přehled obrázků 4](#_Toc108685405)

[1.3 Přehled tabulek 4](#_Toc108685406)

[1.4 Související dokumenty 4](#_Toc108685407)

[2 Účel dokumentu 4](#_Toc108685408)

[3 Konvence, názvosloví 4](#_Toc108685409)

[4 Stručná informace o systému hodnocení rizik 5](#_Toc108685410)

[4.4.1 Základní vlastnosti aplikace ICZ Risk\*Guide 5](#_Toc108685411)

[4.4.2 Funkčnost aplikace ICZ Risk\*Guide 6](#_Toc108685412)

[4.4.3 Řízení rizik kybernetické bezpečnosti IT 6](#_Toc108685413)

[5 Architektura technického řešení 7](#_Toc108685414)

[5.1 Popis architektury 7](#_Toc108685415)

[5.1.1 Datová vrstva 7](#_Toc108685416)

[5.1.2 Aplikační vrstva 7](#_Toc108685417)

[5.1.3 Prezentační vrstva 7](#_Toc108685418)

[5.2 Systémové požadavky 7](#_Toc108685419)

[5.2.1 Aplikační server 7](#_Toc108685420)

[5.2.2 Databázový server 7](#_Toc108685421)

[5.2.3 Klientská stanice 7](#_Toc108685422)

[6 Řízení přístupových oprávnění 7](#_Toc108685423)

[6.1 Principy řízení oprávnění a technické předpoklady 7](#_Toc108685424)

[6.1.1 Ověřování uživatelů a jejich členství ve skupinách 8](#_Toc108685425)

[6.1.2 Načítání údajů o uživatelích a organizační struktuře 8](#_Toc108685426)

[6.2 Řízení přístupu na základě členství ve vybraných skupinách 8](#_Toc108685427)

[6.2.1 Jedna skupina definující uživatele s přístupem do aplikace 8](#_Toc108685428)

[6.2.2 Jedna tzv. „výchozí“ skupina uživatelů 9](#_Toc108685429)

[6.2.3 Skupiny pro správce a privilegované uživatele 9](#_Toc108685430)

[6.3 Řízení přístupu k agendovým záznamům 9](#_Toc108685431)

[6.3.1 Skupiny pro řízení přístupu na základě organizačních rolí 10](#_Toc108685432)

[6.3.2 Skupiny pro řízení přístupu na základě pro týmových rolí 10](#_Toc108685433)

[7 Návrh postupů implementaci a podporu provozu 11](#_Toc108685434)

[7.1 Příprava prostředí 11](#_Toc108685435)

[7.2 Správa konfigurací 11](#_Toc108685436)

[7.3 Provozní postupy 11](#_Toc108685437)

[7.4 Migrace 12](#_Toc108685438)

[7.5 Servisní podpora 12](#_Toc108685439)

[8 Požadavky na součinnost objednatele 12](#_Toc108685440)

[8.1 Instalace a provoz systému 12](#_Toc108685441)

[8.2 Agenda hodnocení rizik 12](#_Toc108685442)

# Popis a nastavení systému

## Verze dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze** | **Provedené změny** | **Upravil(a)** | **Datum** |
| 0.1 | Iniciační verze dokumentu | Martin Seget | 13.7.2022 |
|  |  |  |  |
|  |  |  |  |

## Přehled obrázků

Nenalezena položka seznamu obrázků.

## Přehled tabulek

[Tabulka 1 - Skupina pro nastavení práva přístupu do aplikace 7](#_Toc108614366)

[Tabulka 2 - Přehled skupin pro správce a privilegované uživatele 8](#_Toc108614367)

[Tabulka 3 - Přehled skupin pro nastavení oprávnění agendy hodnocení rizik 9](#_Toc108614368)

[Tabulka 4 – Analýza rizik: Přehled skupin pro potenciální členy týmových rolí 10](#_Toc108614369)

[Tabulka 5 – Přehled číselníků pro podporu hodnocení rizik 11](#_Toc108614370)

## Související dokumenty

Žádné

# Účel dokumentu

Dokument popisuje vlastnosti systému pro hodnocení rizik a předpoklady pro jeho nasazení v IT prostředí uživatele.

# Konvence, názvosloví

V textu se nepoužívají žádné konvence na rámec běžných zvyklostí při popisu návrhu informačních systémů tematicky zaměřených na oblast řízení rizik a internách auditů.

# Stručná informace o systému hodnocení rizik

Aplikace ICZ Risk\*Guide je univerzální nástroj pro hodnocení rizik v rámci různých oblastí činnosti organizace. Aplikace podporuje všechny etapy procesu analýzy rizik. Aplikace podporuje základní etapy procesu hodnocení rizik, což jsou identifikace, analýza a vyhodnocení rizik. Na základě vyhodnocení a kvantifikace rizik aplikace umožňuje vybrat bezpečnostní opatření pro snížení rizik a minimalizaci dopadů potenciálních hrozeb na aktiva.

* Univerzální nástroj pro hodnocení rizik různých oblastí činnosti organizace.
* Zrychluje procesy hodnocení rizik (identifikace, analýza a vyhodnocení rizik).
* Dává přehled o aktuálním stavu hodnocení rizik a jejich ošetření.
* Umožňuje vybrat bezpečnostní opatření pro snížení rizik a minimalizovat dopady potenciálních hrozeb na aktiva na akceptovatelnou úroveň.
* Všechna identifikovaná rizika jsou dlouhodobě pod kontrolou.

Analýza rizik kybernetické bezpečnosti IT probíhá v těchto etapách:

* Stanovení kontextu analýzy rizik.
* Stanovení hranice analýzy rizik, výběrem aktiv, která budou do analýzy zahrnuta.
* Identifikace a seskupování aktiv a posuzování jejich hodnoty.
* Identifikace hrozeb.
* Identifikace stávajících opatření na ošetření hrozeb.
* Identifikace zranitelnosti aktiv.
* Identifikace dopadů a následků působení hrozeb na aktiva.
* Analýza hrozeb a zranitelnosti aktiv.
* Průběžné hodnocení rizik.
* Ošetření rizik pomocí nových opatření a akceptace přijatelné míry rizika.

Pro projekt DTM bude aplikace  ICZ Risk\*Guide využívána pro analýzu rizik podle vyhlášky o kybernetické bezpečnosti (vyhláška č. 82/2018 Sb.).  Další rozšiřující moduly (Nápravná opatření, Finanční rizika, Projektová rizika nejsou součástí projektu DTM).

### Základní vlastnosti aplikace ICZ Risk\*Guide

Evidence akcí hodnocení rizik

* Možnost výběru metodiky hodnocení rizik
* Nastavení kvalitativního hodnocení rizik
* Hierarchická evidence a ohodnocení aktiv
* Evidence a hodnocení hrozeb
* Výpočet inherentního a výchozího rizika
* Evidence a přiřazení opatření pro ošetření rizik
* Výpočet zbytkového rizika
* Export nebo import katalogů hrozeb a opatření
* Kontextová nápověda
* Řízení přístupů a práv
* Notifikace
* Audit log, technické informace, administrace

Výstupy

* Prohlášení o aplikovatelnosti, Plán zvládání rizik (kybernetická bezpečnost)
* Grafické znázornění (export pro účely prezentace)

### Funkčnost aplikace ICZ Risk\*Guide

Identifikace a ohodnocení aktiv

Aktivum je vše, co má pro organizaci hodnotu, která může být zmenšena působením hrozby. Aplikace umožňuje vytvořit seznam aktiv a provést jejich ohodnocení. Aktiva stejného typu mohou být dle definovaných kritérií slučována do skupin aktiv. Práce se skupinou aktiv zrychluje a zpřehledňuje proces hodnocení aktiv.

Identifikace a ohodnocení hrozeb

K jednotlivým aktivům nebo skupinám aktiv jsou identifikovány a přiřazeny potencionální hrozby. Přiřazovány jsou pouze hrozby, které se mohou na aktivu přímo uplatnit. Při identifikaci hrozeb jsou použity obecně doporučené seznamy hrozeb, které však nejsou striktní a mohou být upraveny nebo doplněny podle potřeby. Hrozby se mohou uplatnit pouze na relevantní typ aktiv, který je pro každou hrozbu určen v katalogu hrozeb.

Zranitelnost

Zranitelnost je nedostatek či slabina aktiva, která může umožnit působení hrozeb. Míra zranitelnosti je využívána při výpočtu úrovně rizika.

Určení úrovně rizik

Riziko vzniká vzájemným působením hrozby a aktiva. Úroveň rizika je určena hodnotou aktiva, úrovní hrozby a zranitelností aktiva. Je tedy nutné posoudit dopady uplatnění hrozeb na konkrétní aktivum a zvážit reálnou pravděpodobnost výskytu hrozeb z pohledu převažujících hrozeb, zranitelnosti a aktuálně implementovaných opatření. Úroveň výsledného rizika je následně vypočtena na základě následujících veličin:

* hodnota aktiva (dopad hrozby na aktivum),
* úroveň hrozby a
* zranitelnost aktiva pro danou hrozbu.

Výběr opatření pro snížení rizik

Rizika identifikovaná a ohodnocená během procesu hodnocení rizik je nutné zvládat, přičemž jsou používány čtyři základní způsoby zvládání rizik:

* modifikace rizika, tj. aplikace vhodných opatření, která riziko eliminují nebo sníží,
* akceptování rizika s tím, že naplňuje kritéria organizace pro akceptaci rizik,
* sdílení rizika s třetí stranou (pojišťovna, případně jiná třetí strana),
* vyhnutí se riziku (např. ukončením příslušné činnosti – poskytování služby apod.)

### Řízení rizik kybernetické bezpečnosti IT

* V aplikaci byla implementována metodika hodnocení rizik podle mezinárodního standardu ISO/IEC 27005, která se týká bezpečnosti informačních systémů a bezpečnosti informací IT/ISMS. Použitá vodítka vychází z vyhlášky o kybernetické bezpečnosti (vyhláška č. 82/2018 Sb.) a dalších doporučení Národního úřadu pro kybernetickou a informační bezpečnost. Zvolená metodika je po úpravě nebo vytvoření nových katalogů hrozeb a opatření případně i metrik, použitelná i v dalších oblastech.
* Metodika je kvalitativní, využívá stupnice typu nízký – střední – vysoký – kritický alias 1-2-3-4. Úroveň rizika je odhadována na základě třech dílčích ohodnocení – ohodnocení dopadu, ohodnocení hrozby a ohodnocení úrovně opatření (opaku zranitelnosti).

# Architektura technického řešení

## Popis architektury

### Datová vrstva

Transakční relační databáze pro provoz v single a multitenantním upořádání.

### Aplikační vrstva

Aplikace v MS Windows IIS, Windows služby, Message broker Rabbit MQ.

### Prezentační vrstva

Klientská webová aplikace na platformě Angular.

## Systémové požadavky

Řešení může být provozováno ve fyzickém nebo ve virtualizovaném prostředí. Vzhledem k nepříliš vysokému počtu uživatelů (bezpečnostních analytiků a metodiků), který je z pohledu vyžití systému pro hodnocení rizik typicky, není zapotřebí provádět load balancing či jakoukoliv distribuci aplikace nebo jejích komponent na více instancí.

### Aplikační server

Provoz aplikace vyžaduje minimálně OS Windows Server 2016 (IIS) a vyšší. Optimálně Win Server 2019.

RAM: min. 8 GB, doporučeno 12 GB

Procesor: minimálně 4 virtuální procesory, doporučeno 8

### Databázový server

Je vyžadována jedna transakční databáze na databázovém serveru MS SQL 2016 a výše

Diskový prostor pro data minimálně 40 GB a pro logy 20 GB

RAM: min. 12 GB, doporučeno 16 GB

Procesor: minimálně 4 virtuální procesory, doporučeno 8

### Klientská stanice

Konfigurace klientského PC by měla odpovídat standardům pro provoz běžných kancelářských a webových aplikací s podporou prohlížečů Chrome, Edge nebo Firefox.

RAM: Alespoň 1 GB volné paměti, doporučeno 2 GB

Procesor: alespoň Dual Core 2Ghz nebo více

# Řízení přístupových oprávnění

## Principy řízení oprávnění a technické předpoklady

Systém implementuje možnosti řízení oprávnění (autorizaci) k záznamům jednotlivých agend hodnocení rizik jak plošného charakteru, tak až na úroveň jednotlivých záznamů. Obě možnosti lze vzájemně kombinovat a tím reagovat na potřeby zpřístupnění evidovaných záznamů

* jak pro uživatele spravující všechny záznamy dané agendy, tzv. oprávnění na základě organizačních rolí (vedoucí, metodik…)
* tak pro uživatele s odpovědností za vybraný záznam. tzv. oprávnění na základě týmové role pro konkrétní záznam (analytik, řešitel nápravného opatření…)

Předpokladem pro zajištění řízení oprávnění ve výše uvedeném rozsahu jsou

* autentizace uživatele, kdy dochází k ověření uživatele z pohledu oprávněnosti užívat dané uživatelské jméno (login)
* autorizace k provádění konkrétních akcí nebo zobrazení údajů v systému na základě oprávnění přidělených v systému danému loginu nebo skupině jíž je daný login členem

### Ověřování uživatelů a jejich členství ve skupinách

Z technického pohledu je systém schopen provádět autentizaci a zjišťovat členy skupin proti službám

* doméně v Microsoft Active Directory nebo Active Directory Forest
* tenantu Microsoft Azure AD

Pro zrychlení komunikace mezi agendovým systémem a poskytovatelem autentizačních údajů a skupin je používána cache s expirací 5 minut.

### Načítání údajů o uživatelích a organizační struktuře

Údaje o uživatelích se aktualizují na denní bázi do číselníku lkp\_DomainUserDirectory, který zahrnuje následující údaje

* Login name uživatele
* Display name uživatele
* Emailovou adresu uživatele

Údaje o organizační struktuře se aktualizují na denní bázi do číselníku lkp\_DomainUserDirectory, který zahrnuje následující údaje

* Login name uživatele
* Login name nařízeného
* Číslo/kód organizační jednotky

## Řízení přístupu na základě členství ve vybraných skupinách

Identifikátor řídící domény/Azure tenantu: DOMAIN

Používá se jako identifikátor poskytovatele autentizačních služeb a jako prefix prefix loginů/skupin. Např. DOMAIN\RISKGUIDE\_Users

Následující kapitoly definují propojení skupin a aplikačních rolí, které nastavují efektivní přístup uživatelů v daných skupinách k funkcím aplikace určených oprávněními v příslušné aplikační roli (sadě oprávnění). Tyto skupiny typicky odpovídají organizační struktuře. Dá se tedy hovořit o přidělování oprávnění na základě tzv. „organizačních rolí“, kdy uživatel svojí pracovní pozicí v organizaci získává oprávnění s plošným dopadem na funkce a evidované záznamy.

Pro snazší orientaci a jsou kapitoly tematicky členěny podle předpokládaných rolí uživatelů při správě a používání systému. Popsaný způsob řízení vychází z tzv. best practice a není jediný možný.

### Jedna skupina definující uživatele s přístupem do aplikace

Skupina se používá pro přidělení práva *Login* umožňujícího přístup do aplikace. Toto oprávnění se přiděluje pouze tuto skupinou a kontroluje se při každé akci uživatele v aplikaci. Tj. členství ve skupině

|  |  |  |
| --- | --- | --- |
| Aplikační role (sada oprávnění) | Kód aplikační role | Skupina |
| Uživatel aplikace | User | RISKGUIDE\_Users |

Tabulka 1 - Skupina pro nastavení práva přístupu do aplikace

### Jedna tzv. „výchozí“ skupina uživatelů

Ve vybraných případech užití se vyžaduje výběr konkrétního uživatele. Seznam uživatelů, který se má v takovém případě nabídnout v uživatelském rozhraní je vhodné omezit výčtem. Funkce vyžadující výběr uživatele umožňují tento výčet vymezit formou výčtové skupiny.

V některých případech může být jednodušší pro jednotlivé funkce nezadávat výčtové skupiny, ale použít jednu skupinu pro všechny takové funkce. Právě k tomu slouží tzv. výchozí skupina systému, které se použije v případech, kdy není definována příslušná výčtová skupina.

Konfigurace umožňuje tuto výchozí skupinu nezadat. Za takové situace systém nabídne všechny uživatele dané domény/tenantu.

Výchozí skupina uživatelů: RISKGUIDE\_DefaultUsers

Používá se pro výčet uživatelů nabízených v rámci funkcí aplikace zaměřených na obsazení týmových rolí, příjemců notifikací, pokud není konfigurací řečeno jinak. Typicky se jedná o podmnožinu skupiny uživatelů s přístupem do aplikace.

### Skupiny pro správce a privilegované uživatele

Skupiny se používají pro přidělení práv na funkce pro administraci nebo funkce auditu. Doporučované rozdělení kompetencí rolí je následující:

* Oddělené sady oprávnění pro správce „agendových “číselníků a správce přístupových oprávnění. Správce agendových číselníků je typicky odborník na danou agendu a nese za ni odpovědnost. Má tedy přidělena práva na správu číselníků, případně validačních pravidel a notifikačních šablon. Nastavení bezpečnosti je pak doménou bezpečnostního správce.
* Oprávnění pro pasivní dohled na obsah číselníků a nastavení bezpečnosti.
* Konfigurací lze vytvořit aplikační roli tzv. super účet, mající všechny oprávnění na všechny evidované agendové záznamy.
* Sada oprávnění pro přístup ke čtení auditních záznamů (historie) a všech evidovaných agendových záznamů.

|  |  |  |
| --- | --- | --- |
| Aplikační role (sada oprávnění) | Kód aplikační role | Skupina |
| Správce číselníků | LookupAdministrator | RISKGUIDE\_Metodik |
| Správce bezpečnosti | SecurityAdministrator | RISKGUIDE\_Spravce |
| Dohlížitel číselníků a bezpečnosti | OperationalManager | RISKGUIDE\_Spravce |
| Administrátor (super účet) | FullControl | RISKGUIDE\_Admin |
| Auditor | Auditor | RISKGUIDE\_Auditor |

Tabulka 2 - Přehled skupin pro správce a privilegované uživatele

## Řízení přístupu k agendovým záznamům

Uživatelé mají přístup k položkám menu a funkcím na základě sad oprávnění nazývaných aplikační role, které se jim přidělují podle

* členství ve skupinách řídící domény (tzv. globální/agendová oprávnění)
* členství v týmových rolích evidovaných záznamů (hodnocení rizik), přičemž každá role má uvedenu skupinu určující seznam uživatelů, kterým může být daná role přidělena na vybraném záznamu (tzv. týmová oprávnění)

### Skupiny pro řízení přístupu na základě organizačních rolí

Aplikační role a jim příslušná oprávnění vycházejí z metodiky práce s danou agendou a jejími záznamy. Umožňují řídit přístup k aktivním funkcím evidence záznamů (vytváření) a pasivním nebo aktivním funkcím, a to plošně přes všechny záznamy evidované v agendě.

Typické nastavení umožňuje čtecí přístup všech záznamů osobám odpovědným za metodiku nebo kontrolní činnost nad agendou hodnocení rizik. Správce agendy pak disponuje aktivními právy nad všemi záznamy, která využívá typicky v případech personální „nouze“, kdy pro daný zásah není k dispozici pověřená osoba.

#### Analýzy rizik a bezpečnostní opatření

|  |  |  |
| --- | --- | --- |
| Aplikační role (sada oprávnění) | Kód aplikační role | Skupina |
| Zakladatel analýz rizik | RiskAssessmentCreator |  |
| Čtenář agendy hodnocení rizik | RiskAssessmentSuperReader |  |
| Čtenář bezpečnostních opatření | RiskMeasuresReader |  |
| Správce bezpečnostních opatření | RiskMeasuresManager |  |
| Správce agendy hodnocení rizik | RiskAssessmentSuperEditor |  |

Tabulka 3 - Přehled skupin pro nastavení oprávnění agendy hodnocení rizik

### Skupiny pro řízení přístupu na základě pro týmových rolí

Záznamy Analýzy rizik, Metodiky pro analýzy rizik a Nápravného opatření jsou tzv. chráněné záznamy. To umožňuje řídit přístup ke konkrétním záznamům nejen plošně v rámci agendy ale i individuálně pro jednotlivé záznamy (tzv. row security). Tento princip je aplikován a na přehledy a vyhledávání, kdy uživatel „nevidí“ záznamy na které nemá oprávnění.

Pro řízení přístupu uživatelů ke konkrétním záznamům se používají tzv. pracovní týmy. Uživatel, který má mít přístup ke konkrétnímu záznamu musí být evidován v týmu daného záznamu v některé z rolí určených pro daný záznam. Konkrétní oprávnění uživatele jsou pak dána součtem oprávnění rolí, ve kterých je v týmu daného záznamu evidován.

Pro správu záznamů byly na základě metodiky pro hodnocení rizik navrženy níže uvedené týmové role a skupiny řídící domény, jejichž členové mohou být do dané role zadáni. Týmové role jsou nositeli oprávnění. Pro přidělování oprávnění týmovým rolím jsou vytvořeny standardizované sady oprávnění tzv. úrovně, které lze přidělit každé konkrétní týmové roli. Úroveň oprávnění tak „odemyká“ týmové roli konkrétní funkce systému.

Skupinu pro týmovou roli není nutné uvádět, ale pak do dané role bude možné nominovat jakéhokoliv uživatele z výchozí skupiny uživatelů.

#### Analýza rizik

##### Přehled úrovní oprávnění

Čtenář – (RiskAssessment\_Team\_Reader)

Umožňuje roli číst všechny údaje záznamu Risk analýzy (RA). Není možné záznam upravovat, rušit nebo exportovat RA dokumentaci.

Analytik junior – (RiskAssessment\_Team\_Junior)

Umožňuje roli číst a upravovat a rušit všechny údaje záznamu RA. Není možné exportovat RA dokumentaci a obnovovat zrušené RA záznamy.

Analytik senior – (RiskAssessment\_Team\_Senior)

Umožňuje roli číst, rušit a upravovat všechny údaje záznamu RA. Je možné exportovat RA dokumentaci, ale není umožněno obnovovat zrušené RA záznamy.

Správce risk analýzy – (RiskAssessment\_Team\_Master)

Umožňuje roli číst, rušit a upravovat všechny údaje záznamu RA. Je možné exportovat RA dokumentaci i obnovovat zrušené RA záznamy.

##### Týmové role

|  |  |  |
| --- | --- | --- |
| Týmová role (úroveň oprávnění) | Kód týmové role | Skupina nominantů role |
| Garant  - *Správce risk analýzy* | RiskAssessment\_Garant |  |
| Risk analytik  *- Analytik senior* | RiskAssessment\_Analyst |  |
| Risk analytik – zástupce  *- Analytik senior* | RiskAssessment\_AnalystDeputy |  |
| Asistent analytika  *- Analytik junior* | RiskAssessment\_Asistant |  |
| Vlastník aktiva  *- Čtenář záznamu Risk analýzy* | RiskAssessment\_AssetOwner |  |

Tabulka 4 – Analýza rizik: Přehled skupin pro potenciální členy týmových rolí

# Návrh postupů implementaci a podporu provozu

## Příprava prostředí

Konfigurací systému se rozumí sada parametrů a jejich hodnot, které mají vliv na chování systému a mohou být specifické pro jednotlivé instalované instance. Do konfigurace jsou tedy zadávány

## Správa konfigurací

Konfigurací systému se rozumí sada parametrů a jejich hodnot, které mají vliv na chování systému a mohou být specifické pro jednotlivé instalované instance. Do konfigurace jsou tedy zadávány

* parametry nezbytné pro provoz dané instance jako např. konektivita na databázi, konektivita na autentizační služby, emailové služby, atp…
* parametry specifické pro instanci z pohledu jejího užívání, jako nastavení oprávnění, identifikace instance pro uživatele, příjemci notifikací atp…

Konfigurační parametry, resp. jejich uložení je realizováno

* formou konfiguračních souborů (pro služby systému a integrace)
* formou záznamů v databázi-číselníky (pro nastavení vlastností agendy hodnocení rizik, nastavení tenantů)

## Provozní postupy

Pro zahájení provozu systému definovány následující postupy.

* Založení a prvotní nastavení transakční databáze
* Instalace nové instance systému – prvotní instalace a konfigurace aplikace

Pro správu provozu systému jsou definovány a spravovány následující postupy. Jedná se o technické postupy, které se vztahují buď celé instanci nebo vybranému tenantu.

Postupy pro instanci systému

* Start – Uvedení systému do provozu
* Stop – Ukončení provozu systému (vypnutí nebo odstávka)
* Profylaxe – Preventivní pravidelné činnosti zajišťující správný chod systému nebo činnosti vyvolané mimořádnou událostí (mazání logů, kontrolní procedury, konsolidační procedury…)
* Změna konfigurace – Postupy nasazení a uvedení upravené konfigurace do provozu
* Instalace nové verze instance systému – komplexní plánovaná úprava funkčnosti, dat nebo konfigurace
* Patch instance systému – dílčí úprava funkčnosti, dat nebo konfigurace v reakci na mimořádnou událost

Potupy pro tenant v rámci instance

* Změna konfigurace vybraného tenantu(ů)– Postupy nasazení a uvedení upravené konfigurace tenantu do provozu
* Změna konfigurace s dopadem na všechny tenanty– Postupy nasazení a uvedení upravené konfigurace tenantu do provozu

## Migrace

Migrací se rozumí cílená a plánovaná transformace dat nebo konfigurací ze zdrojového systému do instance systému RiskGuide.

V rámci využití RiskGuide pro hodnocení rizik projektu DTM se migrace neuvažuje. Údaje specifické pro analýzy rizik budou součástí jednorázového přenosu výstupů analýz rizik připravených dodavatelem do systému/tenantu uživatele.

## Servisní podpora

Služby zákaznické podpory pod SLA jsou standardně podporovány na korporátní úrovni oddělením ICZ ServiceDesku v režimu 24x7. Na základě konkrétních smluv o podpoře jsou pro toto oddělení připraveny podklady pro podporu projektu, rozdělení kompetencí mezi pracovníky SD, řešitelského týmu a týmu zákazníka včetně dohodnutých eskalačních procedur.

# Požadavky na součinnost objednatele

## Instalace a provoz systému

Součinnost je vyžadována pro zajištění přístupu k integrovaným systémům a službám zahrnujícím

* Poskytovatele autentizačních služeb
* Databázi
* SMTP server

A systémový účet pro provoz služeb systému RiskGuide (aplikační služby, RabbitMQ)

## Agenda hodnocení rizik

Součinnost je vyžadována pro zajištění přístupu uživatelů k agendě hodnocení rizik. Jsou vyžadovány loginy/skupiny uživatelů v rozsahu kapitoly [Řízení přístupových oprávnění](#_Řízení_přístupových_oprávnění).

Součinnost v rámci nastavení číselníků agendy hodnocení rizik není vyžadována. Příslušná nastavení jsou součástí dodávky výsledků analýzy rizik dodavatelem a potřebná součinnost je tak součástí projektu dodávky analýzy rizik a souvisejících metodik.

|  |  |
| --- | --- |
| Kód číselníku | Název číselníku |
| lkp\_ra\_Aspect | Číselník aspektů |
| lkp\_ra\_AssetType | Typ aktiva |
| lkp\_ra\_Area | Číselník oblastí pro analýzy rizik |

Tabulka 5 – Přehled číselníků pro podporu hodnocení rizik