|  |
| --- |
|  |
|  |
|  |
| Specifikace procesu Řízení kvality |
|   |

Obsah

[1 Úvod 4](#_Toc25248695)

[2 Zkratky a pojmy 5](#_Toc25248696)

[3 Vymezení cílů kvality 6](#_Toc25248697)

[3.1 Standardizace procesů správy služeb ČSN ISO/IEC 20000 6](#_Toc25248698)

[3.1.1 Service Desk 6](#_Toc25248699)

[3.1.2 Katalog služeb 6](#_Toc25248700)

[3.1.3 Konfigurační management - Jednotné vedení dokumentace napříč MHMP 6](#_Toc25248701)

[3.2 Opakované a řízené plnění podmínek BCM dle ČSN EN ISO 22301 6](#_Toc25248702)

[3.3 Opakovatelný systém řízení QC 6](#_Toc25248703)

[3.4 Plnění legislativních podmínek provozu 6](#_Toc25248704)

[3.5 Garance uplatnění zásad bezpečnosti 7](#_Toc25248705)

[3.5.1 Integrace dodávaných řešení do jednotného Identity Management Systému v režii MHMP 7](#_Toc25248706)

[3.5.2 Integrace dodávaných řešení do centrálního řešení SIEM 7](#_Toc25248707)

[3.5.3 Bezpečnostní Check List 7](#_Toc25248708)

[3.6 Jednotná metodika pro řízení kvality projektů 8](#_Toc25248709)

[3.7 Metrika kvality 8](#_Toc25248710)

[4 Role a zodpovědnosti systému kvality 10](#_Toc25248711)

[4.1 Řídící výbor kvality 10](#_Toc25248712)

[4.2 RACI matice odpovědností 10](#_Toc25248713)

[4.3 Komunikační matice 11](#_Toc25248714)

[4.4 Eskalační schéma 12](#_Toc25248715)

[5 Popis procesu kvality 13](#_Toc25248716)

[5.1 Stanovení kritérií 14](#_Toc25248717)

[5.1.1 Požadavky vyplývající z procesu BCM dle (ČSN ISO/IEC 22301) 14](#_Toc25248718)

[5.1.2 Splnění podmínek řízení služeb dle ČSN ISO/IEC 20000 14](#_Toc25248719)

[5.1.3 Legislativní požadavky 15](#_Toc25248720)

[5.1.4 Bezpečnostní standardy 15](#_Toc25248721)

[5.2 Hodnocení kvality 16](#_Toc25248722)

[5.2.1 Způsoby a hodnocení rizik projektu 16](#_Toc25248723)

[5.3 Nástroje a postupy pro dosažení cílů kvality 19](#_Toc25248724)

[5.3.1 Registr kvalitativních ukazatelů 19](#_Toc25248725)

[5.3.2 Registr problémů 20](#_Toc25248726)

[5.3.3 Registr opatření a změnových požadavků 20](#_Toc25248727)

[5.3.4 Registr rizik 21](#_Toc25248728)

[5.3.5 Analýza dopadů 22](#_Toc25248729)

[5.4 Pravidelné aktualizace a kontroly ze strany QC 22](#_Toc25248730)

[5.5 Součinnost při řešení rizik ekosystému MHMP 22](#_Toc25248731)

[6 Reporting 24](#_Toc25248732)

[6.1 Projektová úroveň 24](#_Toc25248733)

[6.2 Řídící výbor 24](#_Toc25248734)

[6.3 Ředitel odboru IT 24](#_Toc25248735)

Seznam tabulek

[Tabulka 1: Sledování změn 3](#_Toc530560404)

[Tabulka 2: Zkratky a pojmy uváděné v dokumentu 5](#_Toc530560405)

[Tabulka 3: Metriky kvality 9](#_Toc530560406)

[Tabulka 4: RACI matice odpovědností 11](#_Toc530560407)

Seznam obrázků

[Obrázek 1 – Komunikace rizik 12](#_Toc530560409)

[Obrázek 2 – Eskalační schéma 12](#_Toc530560410)

[Obrázek 3 – Proces kvality 13](#_Toc530560411)

[Obrázek 4 – Proces kvality – vztahy mezi entitami 14](#_Toc530560412)

Sledování změn

|  |  |  |
| --- | --- | --- |
| Datum změny | Provedl | Změna |
| 4.09.2018 | Karel Jičínský | Založení dokumentu |
| 4.10.2018 | Karel Jičínský | Vydáno k revizi zákazníkem |
| 21.11.2018 | Daniel Hejda/ Karel Jičínsků | Úprava hodnocení, formátu, metrik kvality a dopsány některé oblasti cílů kvality |
|  |  |  |

Tabulka 1: Sledování změn

# Úvod

Quality Assurance (dále jen QA) migrace datového centra je koncepčním doplněním souboru procesů, které mají za cíl vyváženě koordinovat migrační, případně rozvojové služby mezi dodavateli a zaměstnanci Magistrátu hlavního města Praha.

Účinný a důsledně naimplementovaný systém jakosti povede k rozvoji kultury organizace MHMP, k rozvoji

jejich zaměstnanců a k úsporám materiálu a energií.

Základní principy systému řízení kvality:

* Zaměření na uživatele služby a naplnění jejich očekávání v oblasti kvality
* Zaměření na vedoucí pracovníky jako podpora pro zajištění prostředků k dosahování cílů kvality
* Zapojení pracovníků napříč strukturou organizace do zlepšování služeb občanům i interním pracovníkům
* Systém řízení kvality zajistí výraznou měrou předcházení případným problémům
* Poskytnutí relevantní zpětné vazby jako nezbytný předpoklad pro správná budoucí rozhodnutí
* Řízení kvality je nezbytná součást řízení vztahů zúčastněných subjektů

# Zkratky a pojmy

|  |  |
| --- | --- |
| Zkratka, pojem | Popis |
| BIA | Business Impact Analysis – analýza dopadů rizik do organizace |
| DR | Data recovery – obnova dat |
| DRP | Disaster recovery plan - Plán obnovy po havárii. Jde o zdokumentovaný proces nebo soubor postupů pro obnovu a ochranu IT infrastruktury |
| Kategorie vad | Slouží pro kategorizaci nálezů v rámci UAT. Jsou tyto kategorie vad:* A – Vada vylučující užívání plnění nebo jeho důležité a ucelené části;
* B – Vada omezující provoz, která způsobuje problémy při využívání a provozování plnění nebo jeho části, ale umožňuje provoz, nemá vliv na kvalitu dat a výsledky zpracování, a jí způsobené problémy lze dočasně řešit organizačními opatřeními;
* C – ostatní Vady.
 |
| Metrika kvality | Vychází z požadavků na kvalitu z pohledu business a technických uživatelů pro dané řešení/službu, které bývají popsány v příslušné analýze. Metrika kvalita musí být měřitelná, tj. je na úrovni akceptačních kritérií. Detailní popis metriky kvality bývá popsán v testovacích scénářích, tj.: co, kdy (postup), jak (metodika, nástroje), kdo (role), s jakým plánovaným výsledem. |
| MHMP | Magistrát hlavního města Praha |
| Nápravné opatření | Jde o opatření, které má zajistit, aby při další *kontrole kvality* byl *výsledem měření kvality* se statusem *vyhověl*. Nejčastěji jde o realizovaný návrh nápravného opatření z poslední *kontroly kvality*, kde status měření byl *vyhověl s výhradou* nebo *nevyhověl*.  |
| Návrh nápravného opatření | Je navrhnut, pokud *výsledek měření kvality* nebyl se statusem *vyhověl*. Nejčastější návrhy jsou: evidence jako rizika (které se pravidelně kontroluje), založení požadavku na změnu, ověření dopadů změnových požadavků realizovaných v minulosti, ověření metodiky pro měření kvality, ověření jiných výstupů či produktů. |
| OAT | Operational Acceptance Testing – Testování provozovatele navazujících a podpůrných služeb |
| QA | Quality Assurance – Quality assurance se týká obecně všech procesů od návrhu, vývoje, nasazení, údržby až po dokumentaci produktu. Cílem této aktivity je dohlédnout, že produkt je vytvářen tak, že jeho jednotlivé části budou mít odpovídající kvalitu, která byla určena. Hlavní proces systému řízení kvality, který zajišťuje trvalé udržování rozsahu parametrů kvality jako podklad pro činnosti QC |
| QC | Quality Control – je operativní proces pravidelného opakování měření a vyhodnocování parametrů kvality určených procesem QA  |
| Quality Assurance | Zajištění a dohled odborného garanta s využitím prvků pro řízení kvality  |
| SIEM | SIEM (Security Information and Event Management) – Systém pro řízení a záznam bezpečnostních a operativních událostí provozované infrastruktury |
| Záznam registru kvality | Kontrola kvality je periodická činnost, kde z každé kontroly/měření se provede záznam, který obsahuje: datum měření, jaké metriky kvality byly měřeny, použitá metoda(y) pro měření kvality, výsledek měření kvality (status), návrh nápravné opatření, kdo měření provedl. |

Tabulka 2: Zkratky a pojmy uváděné v dokumentu

# Vymezení cílů kvality

Na základě provedených vstupních analýz na projektových schůzkách a schůzkách s vedením IT MHMP dle harmonogramu byly definovány níže uvedené cíle pro splnění očekávání a cílů kvality pro migraci aplikačního portfolia do datového centra 04 a 05.

## Standardizace procesů správy služeb ČSN ISO/IEC 20000

V souladu s předchozími projekty je žádoucí posouzení možností procesní integrace a sjednocení postupů, případně aplikačních prvků pro obsluhu procesů v rámci celého životního cyklu primárně pro tyto oblasti:

### Service Desk

Dosavadní praxe několika desítek decentralizovaných řešení oblasti Service Desk neumožňuje zcela optimálně synchronizovat rozvojové aktivity a činnosti spojené s životním cyklem aplikačních celků.

### Katalog služeb

V rámci celoměstské koncepce je definován žádoucí stav poskytování a centralizace služeb IT pro zřizované organizace a městské části a pro tento účel byly zahájeny kroky vedoucí k definování jednotlivých služeb, kdy MHMP bude poskytovatelem.

### Konfigurační management - Jednotné vedení dokumentace napříč MHMP

Jedním z primárních cílů aplikace QA na projekt migrace je využití okamžiku migrace pro zajištění jednotného vzoru vedení aplikační dokumentace napříč všemi agendami MHMP. Jednotný způsob vedení aplikační dokumentace zajistí zvýšenou přehlednost v rámci životního cyklu dodávaných řešení a dále povede k optimalizaci sdílení informací napříč organizační strukturou MHMP.

## Opakované a řízené plnění podmínek BCM dle ČSN EN ISO 22301

Plán obnovy po havárii (DRP) je zdokumentovaný proces nebo soubor postupů pro obnovu a ochranu IT infrastruktury. Tento plán v písemné formě bude dokumentován a bude specifikovat postupy, které má organizace v případě katastrofy následovat. Jde o komplexní prohlášení o důsledných činnostech, které je třeba podniknout před, během a po výskytu ukazatelů ohrožení chodu aplikačních funkcí. Pro dodržení principů kvality je zapotřebí udržovat dokumentace aktuální a pravidelně provádět testování dle nastaveného stupně kritičnosti jednotlivých systémů.

## Opakovatelný systém řízení QC

Výsledkem tohoto cíle je nastavení systému a parametrů kvality, které budou v definovaných intervalech opakovaně ověřovány a měřeny ve standardizované a jednotné podobě tak, aby byla zachována kontinuita měření kvality po celou dobu trvání životního cyklu provozovaných řešení. Parametry budou určeny na základě vyhodnocení BIA (Business Impact Analysis).

## Plnění legislativních podmínek provozu

V rámci QA bude vyhodnocován soulad s plněním legislativních podmínek vyplývajících především z:

1. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
2. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii;
3. Vyhláška č. 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti);
4. Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích;
5. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů);
6. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV;
7. Zákon č. 480/2004 Sb., o některých službách informační společnosti ve znění účinném od 1. července 2017;
8. Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů a o změně některých zákonů.
9. Další relevantní zákony a vyhlášky dle vstupů od technických a věcných garantů jednotlivých aplikací a technologií.

## Garance uplatnění zásad bezpečnosti

Cílem této oblasti kontroly kvality, je naplnění požadavků odboru bezpečnosti a udržení souladu s podmínkami pro bezpečný provoz aplikací a služeb napříč MHMP. V rámci této oblasti bude kontrolována zejména propojitelnost systémů do bezpečnostních aplikací a služeb MHMP a dále pak naplnění podmínek stanovených v rámci nástrojů pro kontrolu bezpečnosti.

### Integrace dodávaných řešení do jednotného Identity Management Systému v režii MHMP

Pro zjednodušení správy uživatelských identit je v prostředí MHMP implementován systém pro řízení identit, který je preferovaným aplikačním řešením, na který je požadována integrace v co nejširším rozsahu používaných aplikačních služeb.

### Integrace dodávaných řešení do centrálního řešení SIEM

MHMP interně disponuje centrálním řešením SIEM a v rámci kvality bude ověřována schopnost integrace provozovaných služeb do tohoto řešení.

### Bezpečnostní Check List

Existující rámce bezpečnostních standardů jsou definovány v rámci „bezpečnostního Check Listu“ pro aplikační řešení a v rámci QA bude vyhodnocováno naplnění uvedených podmínek.

## Jednotná metodika pro řízení kvality projektů

V rámci mnoha paralelně běžících procesů je optimální nastavit jednotný způsob systému měření kvality, který zefektivní proces, tak aby zaměstnanci MHMP při fungování napříč více projekty, obdrželi jednotný způsob a pracovní postupy.

## Metrika kvality

V rámci kontroly metriky kvality jsou posuzovány jednotlivé cíle a jejich naplnění ze strany dodavatele. Oddělení QA/QC stanovilo níže uvedené metriky kvality, které vedou k dosažení cílů a jejich naplnění souladu s požadavky MHMP.

| Cíl kvality | Podřízená oblast kontroly | Metrika kvality |
| --- | --- | --- |
| JEDNOTNÉ VEDENÍ DOKUMENTACE NAPŘÍČ MHMP | Dle šablony Provozní dokumentace | Ověření existence, úplnosti a správnosti dokumentu všemi hodnotiteli |
| OPAKOVANÉ A ŘÍZENÉ PLNĚNÍ PODMÍNEK BCM DLE ČSN EN ISO 22301 | DR plán | Ověření existence, úplnosti a správnosti dokumentu všemi hodnotiteli včetně provedení DR plánu |
| OPAKOVANÉ A ŘÍZENÉ PLNĚNÍ PODMÍNEK BCM DLE ČSN EN ISO 22301 | Interní testování | Ověření existence, úplnosti interních testovacích scénářů s ověřením průběhu testu |
| OPAKOVANÉ A ŘÍZENÉ PLNĚNÍ PODMÍNEK BCM DLE ČSN EN ISO 22301 | Systémové testování | Ověření existence, úplnosti systémových testovacích scénářů s ověřením průběhu testu |
| OPAKOVANÉ A ŘÍZENÉ PLNĚNÍ PODMÍNEK BCM DLE ČSN EN ISO 22301 | Zátěžové testování | Ověření existence, úplnosti zátěžových testovacích scénářů s ověřením průběhu testu |
| OPAKOVANÉ A ŘÍZENÉ PLNĚNÍ PODMÍNEK BCM DLE ČSN EN ISO 22301 | Bezpečnostní testování | Ověření existence, úplnosti bezpečnostních testovacích scénářů s ověřením průběhu testu |
| OPAKOVANÉ A ŘÍZENÉ PLNĚNÍ PODMÍNEK BCM DLE ČSN EN ISO 22301 | Akceptační testování | Ověření existence, úplnosti interních testovacích scénářů s ověřením průběhu testu a akceptace |
| GARANCE UPLATNĚNÍ ZÁSAD BEZPEČNOSTI | Bezpečnostní Check List | Ověření existence, úplnosti a posouzení souladu s bezpečnostním Check Listem jako standardem v prostředí MHMP |
| GARANCE UPLATNĚNÍ ZÁSAD BEZPEČNOSTI | Integrace dodávaných řešení do jednotného Identity Management Systému v režii MHMP | Ověření připravenosti aplikačního řešení pro integraci od IDM |
| GARANCE UPLATNĚNÍ ZÁSAD BEZPEČNOSTI | Integrace dodávaných řešení do centrálního řešení SIEM | Ověření připravenosti aplikačního řešení pro integraci od SIEM |
| PLNĚNÍ LEGISLATIVNÍCH PODMÍNEK PROVOZU | Ověření souladu | Kontrola a ověření existence vyplněného dotazníku na plnění legislativních požadavků |
| STANDARDIZACE PROCESŮ SPRÁVY SLUŽEB ČSN ISO/IEC 20000 | Service Desk | Ověření připravenosti aplikačního řešení pro integraci do Service Desk řešení a procesů |
| STANDARDIZACE PROCESŮ SPRÁVY SLUŽEB ČSN ISO/IEC 20000 | Katalog služeb | Ověření zavedení řešení do Katalogu služeb MHMP |
| STANDARDIZACE PROCESŮ SPRÁVY SLUŽEB ČSN ISO/IEC 20000 | Konfigurační management - jednotné vedení dokumentace napříč MHMP | Ověření zavedení konfiguračního managementu do EA MHMP |

Tabulka 3: Metriky kvality

# Role a zodpovědnosti systému kvality

## Řídící výbor kvality

Je nejvyšším orgánem řízení systému kvality. V pravidelných intervalech vyhodnocuje a naplňuje podmínky vyplývající z výstupů:

* BIA
* Registru kvality
* Registru rizik
* Registru opatření
* Registru změn

Řídící výbor je složen ze zástupců:

* Ředitel IT
* Provozní ředitel
* Manažer kvality
* Projektový manažer MHMP

## RACI matice odpovědností

Pro úspěšné dosažení cílů kvality bude aplikována metoda s použitím RACI matice pro přiřazení a zobrazení odpovědností rolí v úkolu a svěřených oblastech projektů, služeb či procesů v MHMP.

Vysvětlivky:

**R – Responsible** – role odpovědná za splnění úkolu

**A – Accountable** (někdy též Approver) – role odpovědná za celý úkol

**C – Consulted** – role poskytující konzultaci k úkolu

**I – Informed** – role, která má být informována o průběhu plnění či rozhodnutích v úkolu

| ProcesyMigraceRole | Ověřování plnění cílů kvality | Správa registru kvality  | Správa registru rizik | Správa registru opatření | Hodnocení parametrů kvality | Realizace opatření | Přiřazení aktuální organizační struktuře MHMM |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Obchodní manažer | A | I | I | I | I | I | Ředitel odboru INF |
| Manažer kvality | R | R/A | R/A | R/A | R/A | I | Nezávislý externí poradce |
| Manažer bezpečnosti | R | C | C | C | C | C | Oddělení ochrany infrastruktury Magistrátu |
| Manažer změn | R | C | C | C | C | A | Technický garant |
| Projektový manažer | R | I | R | R | R | R | Vyčleněný pracovník odboru INF příp. externista |
| Technický garant | C | R | R | R | R | R | Oddělení správy a provozu aplikací |
| Architekt aplikací a služeb | R | C | C | C | C | I | Oddělení rozvoje IS/ICT příp. vyčleněný pracovník odboru INF/externista |
| Věcný garant | C | C | C | C | C | C | Viz definováno u konkrétní aplikace + vyčleněný pracovník odboru INF příp. externista |
| Dodavatel aplikace nebo služby | C | C | R | R | C | R | Viz definováno u konkrétní aplikace |
| Dodavatel podpůrných služeb infrastruktury | C | C | R | R | C | R | Oddělení správy a provozu HW infrastruktury/dodavatelé správy služeb |
| Dodavatel navazujících služeb | C | C | R | R | C | R | Veřejné registry/dodavatelé navazujících řešení |

Tabulka 4: RACI matice odpovědností

## Komunikační matice

Při zahájení dílčích projektů bude v každém jednotlivém případě sestavena, průběžně doplňována a udržována komunikační matice obsahující všechny dotčené role pro systém řízení kvality.

V případě vzniku rizika bude provedena analýza, vyhodnocení a návrh na ošetření rizika v projektovém týmu, přičemž strategie ošetření rizika bude schválena osobami v rolích na úrovni 1. Pokud by nevznikla shoda, bude provedena eskalace na úroveň 2, tj. řídící výbor. Pokud by řídící výbor nerozhodl všemi svými členy, má člen, který s rozhodnutím nesouhlasil, možnost obrátit se na úroveň 3, což je ředitel IT, který má právo konečného rozhodnutí.

Pokud by vzniklo riziko (nebo i problém) vyhodnocené jako kritické, je projektový tým povinen bez zbytečného odkladu o této skutečnosti informovat řídící výbor a také ředitele IT.



Obrázek 1 – Komunikace rizik

## Eskalační schéma

Pokud bude nutné provést v rámci dílčích projektů eskalaci, provede projektový manažer daného projektu eskalaci na vyšší úroveň, kterou je řídící výbor. Řídící výbor v případě nutnosti bude eskalovat na příslušného dodavatele a v případě nutnosti, pokud nedojde k uspokojivému výsledku eskalace, provede eskalaci na vyšší úroveň Ředitele IT.



Obrázek 2 – Eskalační schéma

# Popis procesu kvality

Proces řízení kvality začíná definováním požadavků na kvalitu, jehož výsledkem je registr parametrů kvality aplikace/služby. Specifikace položek metrik kvality probíhá za přispění všech rolí, které mohou ovlivnit či vyžadovat dosažení cílů kvality.

Po specifikaci metrik kvality se provádí formou měření (u aplikací nejčastěji formou FAT, UAT nebo OAT) pravidelné nebo nepravidelné kontroly kvality. Záznamy o měření se evidují v logu kvality pro danou službu (obsahuje tzv. *záznam kontroly kvality*). Pokud *výsledek měření kvality* je jiný než „vyhověl“, je nutné provést nápravné opatření, aby při dalším měření kvality (při stejných metrikách kvality) byl status „vyhověl“.

Pro účely projektu budou používány tyto registry/logy:

* Management řízení kvality – hlavní registr, kde budou pro každou službu dohledatelné pro dané metriky kvality výsledek z posledního měření kvality.
* Log kontroly kvality – bude evidován pro každou aplikaci/službu a bude obsahovat *záznam kontroly kvality* z jednotlivých měření.
* Registr kvalitativních ukazatelů – bude evidován pro každou aplikaci/službu a bude obsahovat popis metriky kvality nebo odkaz na dokument, kde je daná metrika popsána.
* Registr rizik
	+ Záznamy v registru rizik jsou zaměřeny na evidenci potenciálních rizik, které mohou (zpravidla negativně) působit na definované metriky kvality
* Registr problémů
	+ Záznamy v registru, které představují nechtěný dopad na kvalitu, přičemž již nastaly a je nutné je začít řešit.
* Registr opatření a změnových požadavků
	+ Záznamy v registru, které představují navržená opatření a změny jako reakci na identifikovaná rizika a problémy.
* Analýza dopadů



Obrázek 3 – Proces kvality



Obrázek 4 – Proces kvality – vztahy mezi entitami

## Stanovení kritérií

Níže je uveden seznam předmětných kritérií, která budou ze strany QA hodnocena s cílem dosáhnout co nejlepšího výsledku při dodávce předmětu plnění.

### Požadavky vyplývající z procesu BCM dle (ČSN ISO/IEC 22301)

#### Testovací scénáře

V rámci procesu měření kvality budou měřeny výsledky, provedení a úroveň zpracování testovacích scénářů dle standardu a v předepsaném formátu.

#### Plán obnovy

Bude posuzováno, zda dle parametrů aplikačního řešení a na základě požadovaných parametrů z procesu BIA byla dostatečně zdokumentována a ověřena funkčnost procesu plánu obnovy včetně navržených opatření pro zajištění jeho opakovatelnosti v pravidelných intervalech.

### Splnění podmínek řízení služeb dle ČSN ISO/IEC 20000

V rámci procesů kvality bude analyzováno splnění podmínek pro správu ITSM služeb po celou dobu životního cyklu služeb a jejich integrace do existujících procesů v prostředí MHMP. Metriky kvality se zaměří primárně na ověření existence a integrace procesů:

* Service Desk
* Katalog služeb
* Systém řízení konfigurace (viz provozní dokumentace)

#### Provozní dokumentace – konfigurační management

Slouží pro standardizované vymezení a definici povinného rozsahu dokumentace provozovaných aplikací a služeb. Vychází ze standardů ČSN ISO/IEC 20000 a je v předepsaném formátu včetně metodiky pro vedení dokumentace.

Bude posuzováno, zda byla naplněna podmínka naplnění standardu pro vedení provozní dokumentace, v jaké míře a zda byly odsouhlaseny předané výstupy.

### Legislativní požadavky

Bude posuzováno naplnění legislativních podmínek vyplývajících z požadavků, pokud předmětné řešení těmto zákonům podléhá:

* Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
* Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii;
* Vyhláška č. 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti);
* Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích;
* NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů);
* SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV;
* Zákon č. 480/2004 Sb., o některých službách informační společnosti ve znění účinném od 1. července 2017;
* Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů a o změně některých zákonů.

Hodnocené kritérium může být splněno doložením a certifikací o splnění podmínek vydaných příslušných orgánem k tomu oprávněným.

### Bezpečnostní standardy

V rámci tohoto kritéria bude posuzováno, zda jsou naplněny požadavky vyplývající z „bezpečnostního check listu“ MHMP.

#### SIEM

V rámci tohoto kritéria bude posuzováno, zda jsou naplněny požadavky vyplývající z cílů kvality a zda je předmětné aplikační řešení přizpůsobeno k integraci do řešení SIEM.

#### Identity management system

V rámci tohoto kritéria bude posuzováno, zda jsou naplněny požadavky vyplývající z cílů kvality a zda je předmětné aplikační řešení přizpůsobeno a v jaké míře k integraci do řešení IDM.

## Hodnocení kvality

Pro záznamy v registru kvalitativních parametrů budou použity následující úrovně hodnocení:

* **Nevztahuje se**
	+ Jedná se o výchozí kontrolní hodnotu používanou pro účely zajištění provedení posouzení s výsledkem, že se pro daný případ další posouzení nevyžaduje, neboť se na něj požadované ukazatele nevztahují.
* **Vyhovující**
	+ Měřitelné parametry byly posouzeny, vyhodnoceny a bez výhrad akceptovány.
* **Částečně vyhovující**
	+ Měřitelné parametry byly posouzeny, vyhodnoceny se vznikem záznamu do registru rizik, problémů nebo opatření a jsou doporučeny k provedení dalšího měření po realizaci nápravných opatření nebo reakcí na rizika, ale nevyžadují eskalaci řídícímu výboru kvality.
* **Nevyhovující**
	+ Měřitelné parametry byly posouzeny, vyhodnoceny se vznikem záznamu do registru rizik, problémů nebo opatření a jsou doporučeny k provedení dalšího měření po realizaci nápravných opatření nebo reakcí na rizika, s eskalací a dohledem řídícího výboru kvality. Zpravidla není možné pokračovat v realizaci projektu až do vyřešení rizik a opatření, případně úpravou metrik parametrů kvality.

### Způsoby a hodnocení rizik projektu

V rámci měření kvality a za účelem udržení neustálého zlepšování stavu služby a s ohledem na dlouhodobou udržitelnost vznikl registr rizik. Tento registr rizik bude pravidelně kontrolován týmem QA/QC, přičemž hodnocení rizik podléhá názoru několika osob (dále jen Hodnotitelů), kteří se společně podílejí na určení míry pravděpodobnosti a dopadu, pokud není dopad výsledkem hodnoty prováděného Business Impact Assesmentu (dále také BIA). Níže jsou reflektována hodnotící kritéria, kterými je povinen se řídit každý z hodnotitelů, tak aby byla nalezena vzájemná shoda s nejnižší mírou rozptylu při odhadování hodnoty rizika.

#### Hodnocení rizik

Rizika v registru rizik mohou mít kvalitativní (slovní) i kvantitativní (číselné a lineární) vyjádření, přičemž hodnoty se řídí níže uvedeným číselníkem:

* **Nízké**
	+ Vyplnění hrozby a zranitelnosti se neuplatní nebo míra dopadu na aktivum (cíl kvality) je nízká
* **Střední**
	+ Vyplnění hrozby a zranitelnost se uplatní v omezené míře a dopad na aktivum (cíl kvality) je spíše nepravděpodobný
* **Vysoké**
	+ Vyplnění hrozby a zranitelnost se uplatní a je vysoce pravděpodobné, že k této situaci dojde nebo je dopad velmi vysoký

Funkční vyjádření výpočtu rizika vázaného k aktivu (cíle kvality) je zobecněno do níže uvedeného vzorce:

***Hodnota Rizika = (průměr(Pravděpodobnost každého hodnotitele) \* (BIA Dopad nebo průměr(Dopad každého hodnotitele)***

Do procesu hodnocení jsou zapojeny níže uvedené osoby, pokud některá z osob nebude schopna poskytnout jednoznačné vyjádření o určení kvantu, pak bude tato osoba z hodnocení vyloučena a rozhodné právo má vždy řídící pracovník odpovědný za daný projekt nebo cíl kvality.

**Seznam hodnotitelů**

* Technický garant
* Věcný garant
* Zástupce QA/QC
* Projektový manažer
* Zástupce odboru bezpečnosti

Pro výpočet rizika byla vytvořena níže uvedená matice, která reflektuje výsledný stupeň rizika.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Pravděpodobnost** | **5** | 5 | 10 | 15 | 20 | 25 |
| **4** | 4 | 8 | 12 | 16 | 20 |
| **3** | 3 | 6 | 9 | 12 | 15 |
| **2** | 2 | 4 | 6 | 8 | 10 |
| **1** | 1 | 2 | 3 | 4 | 5 |
|  | **1** | **2** | **3** | **4** | **5** |
| **Dopad** |

Tabulka 5: Matice pro výpočet úrovně rizika

#### Hodnocení pravděpodobnosti

Hodnocení pravděpodobnosti vychází ze subjektivního určení hodnotitelů. Pravděpodobnost musí jednoznačně určit za jaký časový interval a při jaké procentuální pravděpodobnosti dojde nebo může dojít k vyplnění identifikovaného rizika.

Pravděpodobnost je určována na tří stupňové matici, a to dle počtu procent, přičemž hodnotící interval je nastaven na dobu trvání projektu nebo projektové části, která byla stanovena v rámci projektového plánu (to znamená v čase od projektového milníku k dalšímu projektovému milníku)

* **0 – 20% - nepravděpodobné (vyjádření kvantem 1)**, že dojde k naplnění rizika a způsobení dopadu na aktivum (cíl kvality)
* **21 – 40% - spíše nepravděpodobné (vyjádření kvantem 2)**, že dojde k naplnění rizika a způsobení dopadu na aktivum (cíl kvality)
* **41 – 60% - pravděpodobné (vyjádření kvantem 3)**, že dojde k naplnění rizika a způsobení dopadu na aktivum (cíl kvality)
* **61 – 80% - spíše pravděpodobné (vyjádření kvantem 4)**, že dojde k naplnění rizika a způsobení dopadu na aktivum (cíl kvality)
* **81 – 100% - téměř jisté a nebo jisté (vyjádření kvantem 5)**, že dojde k naplnění rizika a způsobení dopadu na aktivum (cíl kvality)

Určení pravděpodobnosti ovlivňuje úroveň hrozeb a zranitelností, které však nejsou vzhledem k této metodice reflektovány, ale nelze je však pominout a je nutné s nimi pracovat a reflektovat je v hodnocení, respektive při určení hodnoty pravděpodobnosti hodnotiteli.

Hodnocení důvěrnosti, dostupnosti a integrity ve vztahu k původci hrozby

|  |  |
| --- | --- |
| Vlastnost hrozby | Původce hrozby |
| Dostupnost *(informace neexistují, nebo nejsou použitelné)* | * + Čas - dostatek času všech klíčových osob podílejících se na jeho vytvoření
	+ Bude to příliš drahé
	+ Požadavek nebyl ukotven ve smlouvě s dodavatelem
	+ Bude se muset aktualizovat v čase včetně všech změn souvisejících projektů
	+ Změnila se specifikace předmětu plnění z důvodu vlivu okolních projektů
	+ Projekt je zpožďován v čase (prodleva proti projektovému plánu)
 |
| Důvěrnost *(s informacemi se seznámil někdo kdo k tomu neměl oprávnění)* | * + Dokumenty jsou zpřístupněny někomu kdo nemá právo na jejich náhled

   |
| Integrita *(informace byly pozměněny či upraveny)* | * + Znalost lidí, kteří vytváří daný plán (souvislosti, atd..)
	+ Je vyplněn správně, dle standardu
	+ Řešení bude to příliš levné
	+ Máme ověřeno, že obsažené informace jsou úplné případně s jakými riziky
	+ Změnila se specifikace předmětu plnění z důvodu vlivu okolních projektů
	+ Projekt je zpožďován v čase (prodleva proti projektovému plánu)
	+ Nedostatečná znalost interních procesů zadavatele
	+ Existuje neznalost dodávaného produktu nebo produktů integrovaných na tento produkt
	+ Existence standardu (dokumentace) pro udržení dokumentačního standardu
	+ Nebudou udržovány po dobu trvání projektu a dále (zastarají)
	+ Dokumenty nejsou zpřístupněny někomu, kdo nemá právo na jejich změnu
 |

Tabulka 6: Původci hrozeb

#### Hodnocení dopadu

Z pohledu plnění cílů kvality a relevantního odhadu dopadu při hodnocení rizik, byla stanovena níže uvedené škála, která pouze typově popisuje odhadovaný dopad, který by mohlo dané riziko mít, pokud dojde k jeho naplnění. Škála je rozdělena do pěti úrovní, které postupují lineárním průběhem. Dopad je uplatněn tak, že jeho nejvyšší hodnota z níže uvedených oblastí je výsledkem dopadu celkového pro dané riziko.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Míra Dopadu | Hodnota dopadu | Dopad na fungování MHMP | Dopad na cíle kvality | Dopad na Bezpečnost |
| Zanedbatelné | **1** | * Nedostupnost aplikací a systémů v řádu 1 – 60 minut
* Nedostupnost do 0 - 1 systému nebo aplikace
* Dojde k maximálnímu ovlivnění do 1% zaměstnanců
 | * Doručení cíle kvality bude opožděno v čase (0 – 7 dní)
* Bude ovlivněn maximálně 1 stanovený cíl kvality
 | * Systémy nebudou dostupné v bezpečnostním monitoringu po dobu ne delší než 1 hodina
 |
| Nízké | **2** | * Nedostupnost aplikací a systémů v řádu 1 – 4 hodin
* Nedostupnost do 2 - 3 systémů nebo aplikací
* Dojde k maximálnímu ovlivnění do 5% zaměstnanců
 | * Doručení cíle kvality bude opožděno v čase (8 – 14 dní)
* Budou ovlivněny maximálně 2 stanovené cíle kvality
 | * Systémy nebudou dostupné v bezpečnostním monitoringu po dobu ne delší než 4 hodiny
 |
| Střední | **3** | * Nedostupnost aplikací a systémů v řádu 5 – 24 hodin
* Nedostupnost do 3 - 5 systémů nebo aplikací
* Dojde k maximálnímu ovlivnění do 10% zaměstnanců
 | * Doručení cíle kvality bude opožděno v čase (15 – 31 dní)
* Budou ovlivněny maximálně 3 stanovené cíle kvality
 | * Systémy nebudou dostupné v bezpečnostním monitoringu po dobu ne delší než 8 hodin
 |
| Vysoké | **4** | * Nedostupnost aplikací a systémů v řádu 25 – 48 hodin
* Nedostupnost 6 - 10 systémů nebo aplikací
* Dojde k maximálnímu ovlivnění do 20% zaměstnanců
 | * Doručení cíle kvality bude opožděno v čase (32 – 65 dní)
* Budou ovlivněny maximálně 4 stanovené cíle kvality
 | * Systémy nebudou dostupné v bezpečnostním monitoringu po dobu ne delší než 24 hodin
 |
| Kritické | **5** | * Nedostupnost aplikací a systémů v řádu 48 a více hodin
* Nedostupnost 10 a více systémů nebo aplikací
* Dojde k maximálnímu ovlivnění více jak 21% zaměstnanců
 | * Doručení cíle kvality bude opožděno v čase (65 a více dní)
* Budou ovlivněny maximálně 5 stanovených cílů kvality
 | * Systémy nebudou dostupné v bezpečnostním monitoringu po dobu delší než 24 hodin
 |

Tabulka 8: Hodnocení dopadu

## Nástroje a postupy pro dosažení cílů kvality

Po posouzení širokého spektra nástrojů a procesů v systémech pro řízení kvality se jeví níže uvedený výběr jako plně postačující a optimální v prostředí MHMP. Uvedené postupy vychází z Best Practice a byly dodavatelem ověřeny v praxi. Pokud budou po prvotních ověřeních zjištěny procesní nedostatky, tak bude celý systém řízení kvality upraven změnou tohoto dokumentu.

### Registr kvalitativních ukazatelů

Slouží k zaznamenání a evidenci parametrů kvality. Obsahuje minimálně tyto parametry:

* Identifikátor záznamu
* Oblast
* Dotčená aplikace / služba
* Název
* Popis
* Metrika kvality
* Kontrola kvality záznam – zápis výsledků provedeného měření kvality (link na provedené měření z registru
* Kontrola kvality datum aktualizace
* Kontrola kvality hodnocení
* Dopad na okolní systémy
* Dotčený cíl kvality
* Věcný obsah
* Datum vzniku zápisu

### Registr problémů

Slouží k zaznamenání a evidenci parametrů kvality. Obsahuje minimálně tyto parametry:

* Identifikace problému
* Týká se….
* Název
* Popis
* Typ
	+ Organizační – problémy s dopady do organizačních procesů
	+ Technické – problémy s vlivem na technologické úrovni
	+ Bezpečnostní – problémy s dopady do standardů bezpečnosti či Best Practice v oblasti kybernetické bezpečnosti
	+ Integrační – problémy s dopadem do integrací mezi aplikacemi
	+ Infrastrukturní – problémy s vlivem do infrastrukturních služeb
	+ Ostatní
* Priorita
	+ Kritický
	+ Vysoký
	+ Střední
	+ Nízký
* Datum vzniku
* Autor: osoba, která záznam založila
* Datum vyřešení
* Revidováno
* Vlastník: kdo bude daný problém zajišťovat. Daná osoba může být i řešitelem
* Příjemce řešení
* Status
* Navržené řešení
* Komentář

### Registr opatření a změnových požadavků

Slouží k zaznamenání a evidenci požadovaných změn vyplývajících z prováděných hodnocení parametrů kvality. Obsahuje minimálně tyto parametry:

* Identifikátor záznamu
* Identifikátor dotčeného parametru kvality
* Název
* Popis
* Priorita
	+ Kritický
	+ Vysoký
	+ Střední
	+ Nízký
* Typ
	+ Organizační – opatření vyžaduje organizační zajištění procesu
	+ Technické – opatření je možné zajistit změnou konfigurace
	+ Bezpečnostní – opatření vyžadující procesní a technickou koordinaci pro splnění podmínek bezpečnosti dle interních směrnic a postupů MHMP, případně dle doporučení z Best Practice
	+ Integrační – opatření přesahuje rámec aplikační vrstvy a přesahuje do jiného řešení třetí strany
	+ Infrastrukturní – opatření vyžaduje změnu infrastrukturní služby či procesu
	+ Ostatní – opatření ostatní bez kategorizace
* Datum vzniku
* Datum vyřešení
* Revidováno
* Přiděleno k řešení
* Příjemce řešení
* Stav řešení
* Datum uzavření
* Detail eskalace
* Komentář

### Registr rizik

Slouží k evidenci a sledování rizik.

Registr rizik bude trvale udržován a vyhodnocován prostřednictvím procesů Kontroly kvality (QC – Quality Control). Registr rizik obsahuje minimálně:

* Identifikátor rizika
* Autor: kdo riziko zaregistroval
* Název
* Popis
* Vazba na původ rizika (Identifikátor aplikace)
* Dopad na aplikaci
* Typ
	+ Organizační – riziko vyplývající z organizačních postupů
	+ Technické – riziko vyplývající z technického prostředí
	+ Bezpečnostní – riziko s vlivem na bezpečnostní směrnice či procesy dle interních směrnic MHMP případně dle Best Practice
	+ Integrační – riziko které vlivem přesahuje rámec dílčí aplikace a zasahuje do aplikací třetích stran
	+ Infrastrukturní – riziko s vlivem do služeb infrastruktury
	+ Ostatní – ostatní rizika bez přesnější specifikace (bude samostatně kategorizováno po projednání dotčených stran
* Datum založení
* Očekávaná doba vzniku rizika (T+ )/datum pro vyřešení
* Vlastník rizika
* Stav rizika
* Akce – návrh jak riziko ošetřit
* Pravděpodobnost: 1 malá, 2- střední, 3 - vysoká
* Dopad: 1 malý, 2- střední, 3 - vysoký
* Kritičnost: porovnání Pravděpodobnosti a Dopadu určeného na základě BIA
* Status rizika: nové, otevřené, pozastaveno, uzavřeno,

### Analýza dopadů

Analýza dopadů (Business Impact Analysis) je řízení kontinuity činností organizace (Business Continuity Management, BCM). Sestává z technik a metod, pomocí kterých se hodnotí, jaké dopady by na organizaci a další zainteresované strany mělo narušení dodávek klíčových produktů nebo služeb organizace a jejich podpůrných kritických činností. BIA stanovuje minimální úrovně zdrojů potřebných pro obnovení kritických činností v definovaných časech a úrovních.

Závěry z analýzy dopadů společně s hodnocením rizik narušení kritických činností organizace jsou základem pro strategie řízení kontinuity činností, které umožňují identifikovat různé varianty a způsoby obnovy kritických činností organizace v požadovaných časech v případě jejich narušení.

Analýza dopadů by měla být přezkoumávána v pravidelných intervalech, alespoň 1x ročně, nebo při podstatných změnách v organizaci a prostředí, v němž organizace působí. Periodicita opakování je definována na základě požadavků vyplývajících z BIA.

## Pravidelné aktualizace a kontroly ze strany QC

Kontrola kvality jako činnost usměrňující události tak, aby bylo v co nejširší možné míře dosaženo souladu s plánem. Vede ke zjišťování odchylek od plánu a cílů. Inicializuje nápravná opatření včetně změnových požadavků. Základním pilířem kontroly je audit registrů rizik, problému, opatření a změnových požadavků s definovaným dopadem do plnění cílů kvality.

Podle nastavených ukazatelů vzešlých ze strany QA bude proces QC (Quality Control) provádět pravidelné kontroly u trvajících kontraktů, dle specifikace kvalitativních parametrů služby v BIA, které mají definovánu udržitelnost v čase, a to zejména s ohledem na plnění předmětných kritérií a jejich aktualizace v čase. K těmto situacím může dojít zejména při:

* Implementaci nového systému s přímou závislostí na daném předmětu plnění;
* Integraci předmětu plnění s novým systémem;
* Upgrade nebo update předmětu plnění;
* Zrušení předmětu plnění nebo jeho náhrada za systém nový.

## Součinnost při řešení rizik ekosystému MHMP

V závislosti na kvalitativních ukazatelích je nutné, aby byl dodavatel vyzván k součinnosti a návrhu protiopatření, které bude aktivně vést ke snížení míry potencionálního rizika. Pokud by dané riziko neznamenalo ohrožení běhu aplikace, projektu nebo služby, pak může být riziko akceptováno a způsob pro eliminaci rizika může být zařazen do roadmapy, a tím se stát jednou z částí budoucího rozvoje daného systému. Každý dodavatel je povinen poskytnout maximální součinnost při návrhu protiopatření.

# Reporting

Nedílnou součástí systému pro řízení kvality je pravidelná informovanost dotčených osob a subjektů o klíčových změnách ve sledovaných parametrech kvality.

Za účelem ověřování účinnosti procesu řízení kvality jsou v prostředí MHMP sledovány následující ukazatele:

* Počet záznamů v registru rizik s rozdělením na jejich závažnost, stav a trendem jejich vývoje
* Počet záznamů v registru problémů s rozdělením na jejich závažnost, stav a trendem jejich vývoje
* Počet záznamů v registru opatření s rozdělením dle stavu a trendem jejich vývoje
* Počet záznamů v registru změnových požadavků s rozdělením dle stavu a trendem jejich vývoje
* Počet záznamů v registru provedených kontrol kvality s identifikací závažnosti nalezených nesouladů
* Stav měřených cílů kvality pro jednotlivé migrované aplikace

## Projektová úroveň

Jako přímý správce záznamů v registrech bude trvale a pravidelně informován PM každého projektu.

## Řídící výbor

Řídící výbor bude informován o celkovém stavu na všech projektech 1x 2 týdny, přičemž o skutečnostech vyhodnocených jako kritické bude informován bez zbytečného odkladu.

## Ředitel odboru IT

Ředitel odboru IT bude informován o celkovém stavu na všech projektech 1x měsíčně, přičemž o skutečnostech vyhodnocených jako kritické bude informován bez zbytečného odkladu.