**«Názov zmeny alebo projektu»**

Koncepčný návrh riešenia (KNR)

**Obsah**

1 Cieľ dokumentu 4

2 Úvod 5

3 Manažérske zhrnutie 6

4 Zoznam realizovaných požiadaviek 6

5 Popis procesov a funkcionality 6

6 Požiadavky na zmeny architektúry a konfigurácie infraštruktúry 6

7 Popis cieľového stavu architektúry 6

8 Popis sieťovej topológie 6

9 Popis šifrovania 7

10 Popis praktík bezpečného vývoja 7

11 Popis logovania 7

12 Popis nasadzovania nových verzií softvéru 7

13 Prevádzkový monitoring 7

14 Popis systémových a privilegovaných účtov 7

15 Popis aplikačného a dátového modelu 8

16 Release management 8

17 Rozhrania 8

18 Migrácia údajov 8

19 Licenčný model, typy SW licencií 8

20 Popis produkčného, predprodukčného, vývojového a testovacieho prostredia 9

21 Klasifikácia údajov 9

22 Riadenie prístupov 9

23 Odporúčaný scenár zálohovania, obnovy a archivácie 9

24 Testovanie 9

25 Štruktúra dokumentácie 10

26 Školenia 10

27 Riziká a obmedzenia 10

28 Harmonogram riešenia 10

29 Nezávislé posúdenie bezpečnosti 10

30 Záver / iné 10

31 Otvorené otázky 10

32 Prílohy 10

Cieľ dokumentu

Tento dokument slúži ako vzor na vypracovanie KNR po formálnej ako aj obsahovej stránke. Motiváciou na jeho vytvorenie je uľahčiť vzájomnú komunikáciu medzi organizačnými jednotkami objednávateľa ako aj komunikáciu medzi objednávateľom a dodávateľom riešenia vo fáze návrhu riešenia, pri akceptácii KNR a aj pri akceptácii riešenia.

**Použitie**

Dokument KNR musí byť v súlade s týmto vzorom. To značí, že všetky kapitoly uvedené v tomto vzore sú povinné a číslovanie a názvy kapitol v KNR musia byť zhodné s číslovaním a názvami v tomto vzore. Každá kapitola začína na novej strane. Obsah kapitol v KNR musí byť v súlade s popisom uvedeným v tomto vzore. Ak sa v tomto vzore uvádzajú podkapitoly v rámci kapitoly, číslovanie podkapitol nemusí byť identické s číslovaním podkapitol v tomto vzore.

Tento dokument je záväzný nielen pri externých dodávkach riešení, ale aj pri interných dodávkach, pri ktorých sa vyžaduje vypracovanie KNR na základe interného predpisu „Riadenie projektov v informačných a komunikačných systémoch“. Pri internej dodávke sa pod dodávateľom rozumie organizačná jednotka, ktorá je zodpovedná za vypracovanie KNR.

Úvod

Táto kapitola môže obsahovať rôzne podkapitoly podľa potreby dodávateľa, ako napríklad predstavenie firmy, zoznam skratiek, zoznam obrázkov, referencia na iné dokumenty, atď.

**Zodpovednosti v dokumente**

Táto podkapitola je povinná a obsahuje nasledujúcu tabuľku s kompetenciami (objednávateľ, dodávateľ) pre každú kapitolu. Ak za danú kapitolu zodpovedá aj objednávateľ aj dodávateľ, uvedie sa aj rozsah, kto je za čo zodpovedný v danej kapitole.

Tabuľka definuje východiskové kompetencie. Po vzájomnej dohode medzi objednávateľom a dodávateľom je možné kompetencie zmeniť.

|  |  |
| --- | --- |
| **Kapitola** | **Zodpovednosť za vypracovanie** |
| Úvod | Zámer riešenia Objednávateľ, ostatné Dodávateľ |
| Manažérske zhrnutie | Dodávateľ |
| Výsledky analýzy a zoznam požiadaviek | Dodávateľ / Objednávateľ |
| Predpoklady riešenia | Dodávateľ |
| Popis procesov a funkcionality | Dodávateľ |
| Požiadavky na zmeny architektúry a konfigurácie infraštruktúry | Dodávateľ |
| Popis cieľového stavu infraštruktúry | Dodávateľ |
| Popis sieťovej topológie | Dodávateľ |
| Popis systémových a privilegovaných účtov | Dodávateľ |
| Popis aplikačného a dátového modelu | Dodávateľ |
| Patch management | Dodávateľ |
| Rozhrania | Dodávateľ |
| Migrácia údajov | Dodávateľ |
| Licenčný model, typy SW licencií | Dodávateľ |
| Popis produkčného, vývojového a testovacieho prostredia | Objednávateľ: xxxxx  Dodávateľ: xxxxxxx |
| Klasifikácia údajov | Objednávateľ: zoznam typov údajov a ich klasifikácia  Dodávateľ: ako riešenie zohľadňuje klasifikáciu údajov |
| Riadenie prístupov | Dodávateľ |
| Odporúčaný scenár zálohovania, obnovy a archivácie | Dodávateľ |
| Testovanie | Dodávateľ |
| Štruktúra dokumentácie | Dodávateľ |
| Školenia | Dodávateľ |
| Riziká a obmedzenia | Dodávateľ |
| Harmonogram riešenia | Dodávateľ |
| SLA dodávateľa voči objednávateľovi | Dodávateľ |
| Záver / iné | Dodávateľ |
| Otvorené otázky | Objednávateľ: xxxx  Dodávateľ: xxxxx |

**Zámer riešenia**

Táto podkapitola je povinná a musí obsahovať stručný popis zámeru riešenia. Objednávateľ dodá dodávateľovi obsah tejto podkapitoly, alebo dodávateľ prevezme zámer riešenia z popisu požiadaviek.

Manažérske zhrnutie

Dodávateľ v tejto kapitole zhrnie navrhované riešenie:

1. aké sú hlavné ciele a prínosy riešenia
2. aké východiská a princípy sa použili pri návrhu riešenia
3. či je riešenie variantné, koľko variantov je navrhnutých
4. ktoré ďalšie systémy a/alebo aplikácie sú ovplyvnené riešením
5. na aké etapy je riešenia rozdelené,
6. iné

Zoznam realizovaných požiadaviek

Kapitola obsahuje požiadavky objednávateľa z biznis špecifikácie, ktoré má riešenie spĺňať.

Rozdiely voči biznis špecifikácii (po dohode oboch strán) musia byť explicitne uvedené v tejto kapitole.

Popis procesov a funkcionality

Táto kapitola obsahuje popis procesov podporovaných navrhovaným riešením, popis funkcionality, popis GUI (obrazoviek). Odporúčame použiť diagramové techniky UML.

Členenie podkapitol je na autorovi KNR – môže zvoliť členenie podľa funkčných / procesných celkov, alebo popis procesov v jednej podkapitole, popis funkčnosti v inej podkapitole, popis obrazoviek / GUI v ďalšej podkapitole, atď.

Požiadavky na zmeny architektúry a konfigurácie infraštruktúry

Táto kapitola obsahuje požiadavky na zmenu architektúry, požiadavky na výpočtový výkon, operačnú pamäť, diskový priestor, požiadavky na operačné systémy a ďalší systémový SW vrátane verzií (napr. webový prehliadač, DB server, atď) pre produkčné prostredie a ak je to relevantné, aj pre testovacie a vývojové prostredie – viď kapitola 14.

Popis cieľového stavu architektúry

Táto kapitola obsahuje popis cieľového stavu architektúry riešenia vrátane schémy nasadenia (UML deployment model) a popisu jednotlivých komponentov riešenia vrátane modelu komponentov (UML component model).

Popis sieťovej topológie

Táto kapitola popisuje komunikačné kanály (zdroj, cieľ, typ prenosového protokolu), požiadavky na sieťový firewalling, požiadavky na host based firewall a pod.

Popis šifrovania

Táto kapitola popisuje komunikáciu medzi klientom a akoukoľvek serverovou komponentou riešenia (napr. tenký klient - samotná aplikácia, tenký klient - podporný vizualizačný/monitorovací nástroj) z pohľadu šifrovania. Rovnako sa tu nachádza popis šifrovanej komunikácie medzi samostatnými nodmi riešenia (napr. komunikácia aplikácia - databáza). Kvalita navrhnutého šifrovania a zdokumentovanie postupov musia byť v súlade so špecifikáciou.

Táto kapitola obsahuje tiež popis systému správy kryptografického materiálu (kľúče, certifikáty certifikáty) počas celého životného cyklu . Systém správy zahŕňa najmä a) bezpečné nakladanie s kryptografickými kľúčmi a certifikátmi, b) generovanie pseudonáhodnýchčísela kľúčov,zriadenie,distribúciu,vkladanie,zmenu, obmedzenie platnosti, vyberanie, ukladanie a likvidáciu kľúčov a zneplatnenie certifikátov, c) umožnenie kontroly a auditu.

Popis praktík bezpečného vývoja

Táto kapitola popisuje použité praktiky z oblasti bezpečného vývoja softvérových produktov, napr. praktiky Software Development Lifecycle, dostupné napr. na https://www.microsoft.com/en-us/securityengineering/sdl a OWASP Secure Coding Practices dostupné na https://www.owasp.org. V rámci vývoja a údržby webových aplikácií ide predovšetkým o požiadavky ASVS (OWASP Application Security Verification Standard) Level 3 verzia v4.

Zároveň kapitola popisuje zoznam testov, ktoré sa vzťahujú k uvedeným praktikám.

Popis logovania

Táto kapitola obsahuje popis logovania, minimálne v nasledovnom rozsahu: aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia citlivých informácií. Dodávateľ popíše spôsob a formát logovania.

Zároveň kapitola obsahuje popis realizácie forwardovania logovaných dát z obchodného systému do logovacieho systému Objednávateľa.

1. Popis nasadzovania nových verzií softvéru

Táto kapitola obsahuje spôsob nasadzovania nových verzií (či už s novými funkčnosťami alebo záplaty) - a to celého systému ako celku a aj jeho jednotlivých modulov/komponentov (ak to systém umožňuje). Popis obsahuje aj používané repozitáre - verejné aj privátne vrátane informácie, či budú prevádzkované dodávateľom alebo EUS.

Popis obsahuje postupy a nástroje aj pri nasadzovaní aplikačnej časti a tiež aj postupy pri nasadzovaní podporného SW vrátane inštalácie aktualizácií, aplikovania bezpečnostných opráv.

1. Prevádzkový monitoring

Táto kapitola obsahuje popis prevádzkového monitoringu. Pokiaľ je prevádzkový monitoring realizovaný dodávateľom, tak popíše rozsah monitorovaných dát a možnosti využitie pre EUS.

Táto kapitola obsahuje popis nastavenia monitoringu dodávaného systému s využitím EUS nástrojov.

Popis systémových a privilegovaných účtov

Táto kapitola popisuje požiadavky na systémové alebo privilegované účty operačných systémov všetkých komponentov riešenia.

Popis aplikačného a dátového modelu

Táto kapitola obsahuje popis aplikačného a dátového modelu. V prípade, že ide o čisto infraštruktúrny projekt alebo zmenu a aplikačný model nie je relevantný, uvedie sa „Ide o čisto infraštruktúrnu zmenu, aplikačný model sa neaplikuje.“ Ak nie je relevantný ani dátový model, uvedie sa „Ide o čisto infraštruktúrnu zmenu, dátový model sa neaplikuje.“

Dátový model nemusí byť len model pre údaje v databáze, ale môže to byť napríklad aj popis dátových štruktúr komunikačného protokolu pri prenose dát a podobne.

Release management

Táto kapitola popisuje akceptované metódy a spôsob aplikovania záplat, upgrade/update pre všetky komponenty ktoré sú súčasťou riešenia. (väzby, poradie, schvaľovanie, testovanie, akceptácia, zodpovednosti)

Rozhrania

Táto kapitola obsahuje popis rozhraní súvisiacich s predmetom dodávky riešenia. Uvedú a popíšu sa všetky rozhrania (zdroj, cieľ, protokol, formát, scheduler, ...)

Migrácia údajov

Táto kapitola obsahuje popis migrácie existujúcich údajov do navrhovaného systému vrátane harmonogramu / fáz migrácie údajov / zodpovedností.

Licenčný model, typy SW licencií

Táto kapitola obsahuje popis licencií - názov, verzia, edicia, jazyková verzia, licenčný model, počet licencií SW produktov dodaných v rámci riešenia.

Ak implementácia riešenia vyžaduje ďalšie licencie (napríklad Windows Server, SQL Server, alebo napríklad riešenie bude mať automatickú výmenu údajov s SAP, čo vyžaduje licencovanie SAP User licenciami používateľov riešenia) musí byť uvedené názov, verzia, edícia, jazyková verzia, licenčný model a počet licencií.

Ak navrhované riešenia má dopad na existujúce licencie (napríklad implementácia riešenia zníži potrebu existujúcich licencií) musí byť uvedený rozsah a popis dopadu.

Ak navrhované riešenie nemá má dopad na existujúce licencie musí byť uvedené „Návrh riešenia nemá dopad na existujúce licencie

Popis produkčného, predprodukčného, vývojového a testovacieho prostredia

Obsahom tejto kapitoly je popis produkčného, predprodukčného, testovacieho a vývojového prostredia a spôsobu ich vytvorenia a samotného nasadenia, ak je to relevantné (napr. kópia produkčného, a pod.).

Dodávateľ uvedie aj svoje požiadavky na prístupy k jednotlivým prostrediam u objednávateľa vrátanie obdobia (napr.: permanentne, počas vývoja, počas migrácie údajov, atď).

Dodávateľ aj objednávateľ sa spolu dohodnú na obsahu tejto kapitoly a objednávateľ dodá dodávateľovi príslušnú časť popisu.

Klasifikácia údajov

Táto kapitola obsahuje klasifikáciu jednotlivých typov údajov z pohľadu bezpečnosti - verejné, interné, dôverné, tajné, prísne tajné, osobné údaje (objednávateľ dodá obsah dodávateľovi), ako aj spôsob, ako riešenie zohľadňuje klasifikáciu údajov (toto je v kompetencii dodávateľa).

Procesné a technické opatrenia pre spracovanie citlivých a dôverných informácií definuje MP Informačná bezpečnosť – aplikácia to musí zohľadňovať (je to obsahom kapitoly 3).

Riadenie prístupov

Táto kapitola obsahuje popis riadenia prístupov a spôsob zabezpečenia.

Odporúčaný scenár zálohovania, obnovy a archivácie

Táto kapitola obsahuje popis zálohovania, obnovy a archivácie spolu so zodpovednosťami. V prípade, že riešenie je formou PaaS, IaaS alebo SaaS, uvedie sa „Riešenie je formou IaaS / PaaS / SaaS. Zálohovanie a obnova je v kompetencii dodávateľa.“ V opačnom prípade (riešenie je prevádzkované v infraštruktúre Eustream) dodávateľ popíše odporúčaný spôsob zálohovania a obnovy a archivácie vzhľadom na prílohu č.2 (SLA voči koncovému zákazníkovi).

Súčasťou popisu údržby sú aj procedúry na zálohovanie aplikácie systému a Podporných komponentov a procedúry na disaster recovery.

Testovanie

Táto kapitola obsahuje

1. popis testovacích scenárov, ktoré budú použité pri funkčných a akceptačných testoch
2. popis spôsobu testovania (počas vývoja, na konci fáz, finálne,...) a určenie zodpovedností
3. popis spôsobu a kritérií akceptácie riešenia

Štruktúra dokumentácie

Táto kapitola obsahuje popis dokumentácie (názvy dodávaných dokumentov a ich stručný popis), ktorá bude ddaná v rámci riešenia.

Školenia

Táto kapitola obsahuje popis školení v rámci dodávky riešenia (Názov, pre koho je určené, trvanie, limity).

Riziká a obmedzenia

Táto kapitola obsahuje popis rizík a obmedzení, ktoré so sebou navrhované riešenia prináša alebo môže priniesť, ich dopad, ako aj popis ich zmiernenia.

Ak sú navrhovaným riešením niektoré riziká zmiernené, treba popísať, ktoré a ako.

Harmonogram riešenia

Táto kapitola obsahuje návrh podrobného harmonogramu dodávky riešenia v takej detailnej úrovni, aby bolo možné definovať:

* Míľniky projektu (platobné, odovzdávacie, kontrolné)
* Identifikácia súčinnosti objednávateľa
* Náväznosť alebo paralelný súbeh činností

Nezávislé posúdenie bezpečnosti

Kapitola obsahuje popis nezávislého posúdenia bezpečnosti celého dodaného riešenia pred jeho akceptáciou. Definuje spôsob, rozsah, metodiky, zodpovednosti, harmonogram realizácie posúdenia, rozsah výslednej správy a postupy odstránenie nálezov.

Záver / iné

Zhrnutie, prípadne iné poznámky a postrehy.

Otvorené otázky

Uvedú sa otvorené otázky, prípadne otvorené body riešenia.

Prílohy

Vložia sa prílohy.

Zoznam povinných príloh:

1. Biznis špecifikácia objednávateľa