Obsah

1 Funkčné požiadavky

Folder 01 - Byznis architektúra
Riešenie vo všeobecnosti zabezpečuje jednotný prístupový bod - Kontaktné centrum pre občanov a zdravotníckych pracovníkov pre riešenie požiadaviek a incidentov v súvislosti s poskytovaním služieb NZIS v rozsahu: - poskytovanie technickej podpory pokrývajúce riešenie technických problémov súvisiacich s nedostupnosťou alebo zníženou úrovňou kvality služieb NZIS poskytovanie asistencie v procese spracovania špeciálnej požiadavky alebo zmeny stavu služieb NZIS

1.1 Požiadavky na Podporu riadenia prevádzky

Folder A Oblasť Podpora riadenia prevádzky
Cieľom prevádzky vo všeobecnosti je zabezpečiť bezproblémový chod NZIS počas celej jeho životnosti, ako aj minimalizovať prevádzkové náklady súvisiace s prevádzkou NZIS. Kľúčovým faktorom pre naplnenie tohto cieľa je nastavenie a zavedenie IT procesov v rámci prevádzky všetkých existujúcich prostredí NZIS. Konfigurácia a úprava aplikácie za účelom naplnenia špecifických požiadaviek organizácie, ktoré budú vyplývať z IT procesov riadenia prevádzky navrhnutých v spolupráci s obstarávateľom, v súlade s odporúčaniami rámca ITIL v3 je súčasťou implementácie riešenia a cenovej ponuky.

1.1.1 Časť – Service Desk systém

Business layer A.5 Service Desk systém
V rámci riešenia je dodávka, parametrizácia a nasadenie systému Service Desk ako podporného nástroja pre evidenciu a riadenie zavedených IT procesov prevádzky. Service Desk systém je založený na produkte IBM Control Desk, ktorý predstavuje štandardné, robustné a ľahko konfigurovateľné riešenie v oblasti podpory prevádzky a riadenia IT služieb. Slúži ako jednotný kontaktný bod medzi poskytovateľom služieb a používateľom služieb. Typický service desk riadi incidenty a žiadosti o službu a tiež rieši komunikáciu s používateľmi. Produkt IBM Control Desk je integrovaným riešením správy služieb, ktoré pomáha spravovať celý rad procesov, služieb a aktív IT. Produkt využíva odporúčania rámca ITIL v3 (Information Technology Infrastructure Library) a pomáha pri správe IT prostredia, ktoré je stále viac komplexné, virtualizované, distribuované a rôznorodé. IBM Control Desk pomáha optimalizovať výkon infraštruktúry a pracovnej sily. Pomáha získať kontrolu nad správou integrity konfigurácií po plánovaných zmenách a neplánovaných incidentoch a problémoch, ku ktorým dochádza v tomto komplexnom IT prostredí, čím zaistíte spojitosť služieb, rýchlosť odozvy a efektivitu správy. Produkt ponúka inovatívnu funkčnosť v rade oblastí oblastí, vrátane: - jednoduchého a ľahko použiteľného katalógu služieb - nástrojov na jednoduché hlásenie problémov a požiadaviek na služby - aplikácií, ktoré umožnia IT personálu byť produktívny a zodpovedný pri stanovení priorít, sledovaní a vyriešení problémov koncových používateľov - riadenia zmien, konfigurácií, vydaní, incidentov, problémov a aktív v súlade s odporúčaniami rámca ITIL - automatizácie pracovných postupov a priradených úloh - integrovanej správy služieb, aktív a konfigurácií - nástrojov pokročilé analýzy, ktoré ponúkajú prehľad IT prostredia a pomáhajú efektívnejšie spravovať zmeny Produkt umožňuje vykonávať základnú konfiguráciu systému bez programovania, tak aby sa dalo rýchlo prispôsobiť používateľské rozhranie, dátový model a pracovné postupy potrebám konkrétnej organizácie

IBM Control Desk ukladá množstvo dát o službách - incidenty, problémy, požiadavky na služby, aktíva, konfiguračné položky a ďalšie. To umožňuje vytvoriť plán na zlepšenie služieb alebo plán kvality služieb. Je možné zobraziť trendy hlásení na Incidentoch a konfiguračných položkách, ak chcete identifikovať ktoré aplikácie alebo služby najviac potrebujú aktualizovať.
Service Desk systém spĺňa nasledujúce požiadavky:

- poskytuje plnohodnotné webové rozhranie pre používateľov aj administrátorov
- umožňuje jednoduchú implementáciu zmien v aplikácii, vyplývajúcich zo zmeny/úpravy prevádzkových procesov (v réžii obstarávateľa, bez nutnosti programovania)
- umožňuje jednoduchú konfiguráciu a zmenu používateľského rozhrania (v réžii obstarávateľa, bez nutnosti programovania)
- umožňuje pridávať, meniť a mazať dohodnuté procesné notifikácie a eskalácie prostredníctvom grafického používateľského rozhrania (v réžii obstarávateľa, bez nutnosti programovania)
- umožňuje používateľom prispôsobiť si vzhľad úvodnej obrazovky

V oblasti reportovania a vyhodnocovania Service Desk systém spĺňa nasledujúce požiadavky:

- poskytuje prostriedky pre vytváranie a úpravu reportov
- poskytuje podporu pre ad-hoc (jednorazové) a pravidelné reporty
- umožňuje manuálne a automatizované generovanie reportov
- umožňuje automatizovanú distribúciu reportov prostredníctvom emailu
- poskytuje možnosť exportu reportov minimálne do formátov PDF, XLS
- umožňuje vytváranie nových a úpravu existujúcich reportov v používateľsky prívetivom prostredí

V oblasti aplikačnej bezpečnosti riešenie:

- umožňuje definíciu prístupových práv vo forme aplikačných rolí, pričom oprávnenia používateľa sú definované množinou aplikačných rolí
- umožňuje podrobné riadenie prístupov - riadenie prístupov je umožnené na základe operácií nad dátami (napr. vytvorenie, editácia, schválenie) a na základe rozsahu dát (napr. práva len pre priradené incidenty, práva len na incidenty pre určité služby)
- umožňuje riadenie prístupu k údajom na úrovni objektov, atribútov, lokalít, stavov, katalógu služieb, organizácií
- umožňuje auditovanie zmien nad dátami v systéme
- umožňuje overenie identity používateľa (používateľským menom a heslom) pri zmene citlivých dát v systéme
- umožňuje ukladanie a prácu s citlivými údajmi (ukladanie v zašifrovanej forme)

Licencia systému SD, spĺňa minimálne funkčné požiadavky popísané v kapitole 4.3.2. Licencia pokrýva jadro SD systému a nasledovné min. počty klientskych prístupov:

- 15ks paralelných prístupov pre operátorov KC
- 20ks klientskych prístupov pre pomenovaných používateľov (administrátorov 2.úrovne)

SD systém spĺňa požiadavky na výkon, škálovateľnosť a dostupnosť SD:

- systém je navrhnutý s prihliadnutím na možný nárast záťaže, ktorý môže byť následkom niektorých z nasledovných faktorov:
- počet používateľov (celkový a súčasne aktívnych)
- počet poskytovaných a podporovaných služieb
- úroveň používateľnosti každej služby
- podpora systému vysokej dostupnosti (HA)
- podporované operačné systémy - MS Windows Server, Red Hat Enterprise Linux, SUSE Enterprise Linux alebo ekvivalentný

SD systém spĺňa požiadavky na používateľské rozhranie:

- všetky funkcie sú dostupné cez webové rozhranie
- kompatibilné s mobilnými zariadeniami (PDA, smartphone)
- lokalizované do slovenského jazyka (pre všetky úrovne podpory)
- podpora grafického modelovania a definície workflow pre všetky požadované procesy
- podpora grafického zobrazovania stavu procesných objektov (požiadavka, incident, problém, zmena, release, konfiguračný prvok) v ich životnom cykle

SD systém spĺňa požiadavky na integračné rozhranie:

- štandardné a otvorené komunikačné protokoly (HTTP, SMTP, TCP/IP)
- štandardné a otvorené výmenné formáty (XML, SOAP, JSON)
- štandardné protokoly na komunikáciu s poštovými službami (SMTP)
- spracovanie štandardných webových služieb pre potreby integrácie s inými aplikáciami
- jednoduchý import a expnort údajov do textových súborov (min. XML, CSV)

SD systém spĺňa požiadavky na reporting nástroje:

- vytáranie a úprava reportov priamo v nástroji
- automatizácia pregenerovania periodických reportov
- automatizovaná distribúcia reportov emailom
- export reportov do formátov PDF a XLS

Pre SD systém je splnená požadovaná úroveň softvérovej podpory zabezpečujúca Obstarávateľovi počas celej doby platnosti podpory :

- technická podpora 8x5,
- prístup k aktualizáciám produktu a najnovším verziám produktu
- technická podpora v zmysle štandardných licenčných podmienok výrobcu

A.5 Service Desk systém -	
Name	
FP-1 Incident Management	Proces je zodpovedný za včasnú detekciu incidentov, ich evidenciu, a riadenie ich životného cyklu. Cieľom procesu Incident management je obnoviť normálnu prevádzku služby, a to čo najrýchlejšie pri súčasnej minimalizácii dôsledkov výpadku služby na prevádzku (tzn. na zákazníkov a používateľov). Zároveň je cieľom zabezpečiť, aby služby dodávané zákazníkom spĺňali kvalitu podľa dohodnutých SLA. V procese Incident management, SD systém plne podporuje: - evidencia a riadenie priebehu riešenia incidentov - evidencia vzťahov so súvisiacimi záznamami z ostatných procesov (požiadavka, incident, problém, zmena, konfiguračná položka) - vzájomná komunikácia a koordinácia medzi jednotlivými pracovníkmi prevádzky - preradenie/prevzatie rozpracovaného incidentu iného pracovníka - funkčné a hierarchické eskalácie v priebehu riešenia incidentov - evidencia náhradných a trvalých riešení a ich integrácia do znalostnej databázy - vyhľadávanie v znalostnej databáze počas celého životného cyklu incidentu - konfigurovateľná kategorizácia/klasifikácia incidentov - automatické prideľovanie priority na základe procesných pravidiel (vrátane matice dopadu a naliehavosti) - automatické priraďovanie riešiteľských skupín podľa rôznych pravidiel - automatické priraďovanie riešiteľov zo skupín (podľa počtu riešených incidentov, rovnomerne) so zohľadnením dostupnosti jednotlivých riešiteľov - automatická diagnostika a riešenie incidentov

A.5 Service Desk systém -	
Name	
	- definícia a meranie rôznych metrík a kľúčových ukazovateľov výkonnosti procesu - zaznamenávanie histórie spracovania a zmien atribútov jednotlivých objektov, vrátane identifikácie používateľa, ktorý danú aktivitu, resp. zmenu vykonal - poskytovanie výstupov pre vyhodnocovanie úrovne poskytovaných služieb Proces riadenia incidentov, je v systéme SD podporený primárne aplikáciou Incidenty (Incidents). Záznam incidentu v aplikácii zachytáva informácie o udalosti, ktorá sa líši od štandardnej služby, alebo o udalosti, ktorá môže narušiť kvalitu služby. Aplikácia Incidenty sa používa na vytvorenie a úpravu záznamov o incidentoch. Pri riešení incidentu je cieľom agenta obnoviť službu pre zákazníka čo najrýchlejšie. Po vytvorení záznamu incidentu, pri počiatočnom zdokumentovaní incidentu je možné preskúmať potenciálne riešenia. Keď je identifikované riešenie, je možné ho poznačiť do riešenia. Ak vyriešenie incidentu zahŕňa vytvorenie žiadosti o službu, incident, problém alebo pracovný príkaz, je možné ho vytvoriť priamo zo záznamu incidentu v aplikácií Incidenty. K incidentu je tiež možné pripojiť podobné záznamy. Na zjednodušenie manažmentu viacerých ticketov je možnosť označiť lístok ako globálnu záležitosť a ostatné lístky priradiť ku globálnemu záznamu. Aplikácia Incidenty okrem iného umožňuje: - Vytvorenie incidentov - Vytvorenie záznamov z existujúcich záznamov - Vytvorenie vzťahov medzi záznamami - Vytvorenie vzťahov medzi záznamami lístkov a pracovných príkazov - Odstránenie príznakov globálnej záležitosti - Vymazanie vzťahov - Vytvorenie konceptu riešení pre problémy a incidenty - Vyhľadávanie riešení - Zmenu stavu zoznamu záznamov - Vytvorenie položiek protokolu prác - Vytvorenie e-mailovej komunikácie - Zmenu archivovaných lístkov - Definovanie šablón incidentu
FP-2 Reportovanie a vyhodnocovanie	Riešenie obsahuje pre oblasť reportovania a vyhodnocovania nasledujúce nástroje na: - vytváranie a úpravu reportov - podporu pre ad-hoc (jednorazové) a pravidelné reporty - manuálne a automatizované generovanie reportov - automatizovanú distribúciu reportov prostredníctvom emailu - možnosť exportu reportov minimálne do formátov PDF, XLS - vytváranie nových a úpravu existujúcich reportov v používateľsky prívetivom prostredí
FP-3 Aplikačná bezpečnosť	Riešenie obsahuje pre oblasť aplikačnej bezpečnosti nasledujúce nástroje na: - definíciu prístupových práv vo forme aplikačných rolí, pričom oprávnenia používateľa budú definované množinou aplikačných rolí - podrobné riadenie prístupov - riadenie prístupov musí byť umožnené na základe operácií nad dátami (napr. vytvorenie, editácia, schválenie) a na základe rozsahu dát (napr. práva len pre priradené incidenty, práva len na incidenty pre určité služby) - riadenie prístupu k údajom na úrovni objektov, atribútov, lokalít, stavov, katalógu služieb, organizácií - auditovanie zmien nad dátami v systéme

A.5 Service Desk systém -	
Name	
	- overenie identity používateľa (používateľským menom a heslom) pri zmene citlivých dát v systéme - ;ukladanie a prácu s citlivými údajmi (ukladanie v zašifrovanej forme)
FP-4 Problem Management	Proces zodpovedá za včasnú detekciu problémov, ich evidenciu a riadenie ich životného cyklu. Jeho cieľom je zisťovať príčiny incidentov a spôsoby ich odstránenia, rozhodovať o trvalom odstránení chyby, alebo o jej dočasnom, či trvalom zachovaní v IT infraštruktúre. smerovať do procesu change management žiadosti o zmenu, ktorých obsahom je odstránenie chyby z infraštruktúry a potom, keď je chyba skutočne odstránená, overiť, či pôvodné symptómy boli odstránené a k incidentom spôsobených touto chybou už nedochádza. V oblasti podpory procesu Problem management, SD systém plne spĺňa požiadavky: - evidencia a riadenie problémov počas ich celého životného cyklu - evidencia vzťahov so súvisiacimi záznamami z ostatných procesov (incident, problém, zmena, konfiguračná položka) - podpora pre proaktívny Problem Management - identifikácia potenciálnych problémov - podpora pre reaktívny Problem Management - vytváranie problémov na základe výstupov z procesu Incident Management (často opakujúce sa incidenty) - evidencia známych chýb a ich integrácia do znalostnej databázy - integrácia s procesom Change Management pri nasadzovaní trvalých riešení Proces problem management je v systéme SD primárne podporený aplikáciou Problémy (Problems). Aplikácia Problémy sa používa na vytvorenie a úpravu záznamov o problémoch. Záznam o probléme opisuje neznámu príčinu nižšej úrovne pre jeden alebo viacero incidentov. Problém je vyriešený identifikovaním jeho koreňovej príčiny, aby sa zabránilo podobným incidentom alebo aby mali menší dopad na služby. Záznam o probléme je typ tiketu. Aplikácie Problémy, Incidenty a Žiadosti o službu sú úzko prepojené a zdieľajú mnohé funkcie. Je možné definovať vzťahy medzi lístkami, prepájať ich na informačné účely a zobrazovať o nich podrobnosti v príslušných aplikáciách. Aplikácia Problémy okrem iného umožňuje: - Vytvorenie záznamov o probléme - Vytvorenie vzťahov medzi záznamami lístkov a pracovných príkazov - Vytvorenie záznamov z existujúcich záznamov - Vymazanie vzťahov - Odstránenie príznakov globálnej záležitosti - Vytvorenie konceptu riešení pre problémy a incidenty - Vyhľadávanie riešení - Zmenu stavu zoznamu záznamov - Vytvorenie položiek protokolu prác - Vytvorenie e-mailovej komunikácie
FP-5 Change Management	Úlohou procesu Change management je zabezpečiť, aby sa zmeny v rámci organizácie evidovali, plánovali, implementovali a testovali štandardným a kontrolovaným spôsobom a tým sa znížil ich dopad na poskytované služby. V procese Change management SD systém spĺňa všetky nasledujúce požiadavky: - evidencia a riadenie zmien počas ich celého životného cyklu - evidencia vzťahov so súvisiacimi záznamami z ostatných procesov (požiadavka, incident, problém, zmena) - možnosť evidovať vzťahy na konkrétne ovplyvnené konfiguračné prvky z konfiguračnej databázy

A.5 Service Desk systém -	
Name	
	- možnosť definície rôznych workflowov s rôznymi procesnými pravidlami, pre rôzne kategórie a typy zmien (Napr.: Štandardné zmeny, Urgentné zmeny, Normálne zmeny) - možnosť dekompozície zmeny na parciálne úlohy a ich pridelenie na rôznych riešiteľov/riešiteľské skupiny - konfigurovateľné schvaľovacie pravidlá - vizuálne plánovanie zmien s identifikáciou možných konfliktov pri nasadzovaní zmien - plánovanie zmien so zohľadnením garantovanej dostupnosti danej služby - riešenie musí obsahovať kalendár zmien - analýza dopadov zmeny na základe vzťahov medzi konfiguračnými položkami - definícia a meranie rôznych metrík a kľúčových ukazovateľov výkonnosti procesu - zaznamenávanie histórie spracovania a zmien atribútov jednotlivých objektov, vrátane identifikácie používateľa, ktorý danú aktivitu, resp. zmenu vykonal - poskytovanie výstupov pre vyhodnocovanie úrovne poskytovaných služieb Proces riadenia zmien je v systéme SD primárne podporený aplikáciou Aplikáciu Zmeny(Changes), ktorú je možné použiť na naplánovanie, posúdenie a nahlásenie skutočných hodnôt pre implementáciu zmien alebo nasadenie nových, štandardných konfigurácií do existujúcich aktív. Zmeny je tiež možné vytvoriť v iných aplikáciách. Zmena typicky začína, keď niekto pošle žiadosť o úpravu služby alebo aktíva. Po schválení žiadosti sa vytvorí Zmena. Zmena niekedy zahŕňa oveľa zložitejší proces, napríklad získanie schválení z vyšších úrovní, dôkladné otestovanie a validácia. Proces tiež môže zahŕňať upozornenie osoby, ktorá službu používa, o prebiehajúcej zmene a získanie jej súhlasu na čas vykonania zmeny, a tiež identifikáciu možného vplyvu zmeny na iných. Aplikáciu Zmeny je možné použiť na definovanie, naplánovanie a rozvrhnutie práce vyžadovanej na implementáciu zmeny. Je možné ju tiež použiť na priradenie vlastníka k zmene, kategorizáciu zmeny a aktualizáciu jej stavu, ako sa posúva k dokončeniu. K zmene je možné priradiť iné záznamy, aby ste zjednodušili manažment viacerých podobných záznamov, alebo je možné vytvoriť doplňujúce záznamy priamo zo zmeny.
FP-6 Release and Deployment Management	Manažment vydaní a nasadení (Release and deployment management) Proces Manažment vydaní a nasadení zabezpečuje úspešnú distribúciu a nasadenie schválenej zmeny do IT infraštruktúry, zabezpečuje súlad technického aj organizačného aspektu nasadenia zmien. Jednotlivé časti vydaní sú vytvárané tak, aby minimalizovali časový prestoj a riziká počas ich trvania. Manažment vydaní vyžaduje plánovanie a kontrolu hardvérových a softvérových inštalácií. Pri nasadzovaní nových softvérových verzií veľakrát vyplynie aj požiadavka na zmenu hardvéru, preto je nevyhnutné koordinovať nasadzovanie zmien softvéru aj hardvéru v produkčnom prostredí. Manažment vydaní úzko spolupracuje s Manažmentom zmien a spolu tvoria hranicu medzi prevádzkovým a vývojovým prostredím. Service Desk systém plne podporuje: - evidencia a riadenie vydaní pri nasadzovaní nových alebo zmenených služieb NZIS - evidencia vzťahov s ovplyvnenými konfiguračnými prvkami a súvisiacimi záznamami z ostatných procesov (požiadavka, incident, problém, zmena) - podpora pridávania/odoberania zmien z procesu Change Management do jednotlivých vydaní - vytváranie a udržiavanie evidencie knižnice médií - Definitive Media Library (DML) Service desk systém obsahuje aplikáciu Vydania(Releases), v ktorej je možné plánovať, posudzovať a pripravovať veľké dávky zmien v jednej alebo viacerých

A.5 Service Desk systém -	
Name	
	službách. Záznam o vydaní obsahuje podrobnosti o úlohách, plánovaní a osobách alebo skupinách zahrnutých vo vydaní. Aplikáciu Vydania je možné používať na riadenie vydania autorizovaných verzií alebo konfigurácií komponentov do produkčného prostredia. K príkladom patria veľké alebo kritické zmeny hardvéru, podstatné zmeny softvéru a balenie súvisiacich množín zmien. Je možné vytvoriť vydanie, ktoré pomôže naplánovať, posúdiť a vykonať prípravu pre veľké dávky zmien. Záznam o vydaní obsahuje podrobnosti o úlohách, plánovaní a osobách alebo skupinách zahrnutých vo vydaní. Aplikácia umožňuje: - Vytvorenie vydaní - Vydanie určuje informácie o práci, ktorá sa musí vykonať pre aktívum, umiestnenie alebo položku konfigurácie. Je možné pridať pracovné plány alebo pracovné postupy. Je možné tiež zaznamenať denné hodnoty pri postupe práce. - Hlásenie denných hodnôt pre pracovné príkazy - Ako prebieha práca na schválenom pracovnom príkaze, je možné hlásiť skutočné hodiny pracovníka, použitých materiálov, služieb a nástrojov. - Nahlásenie doby výpadku pre aktíva - Je možné nahlásiť začiatočný a koncový čas doby výpadku pre aktívum, keď k nemu dôjde. - Výmena aktív - Je možné vymeniť aktíva priradené k pracovnému príkazu. Akcia výmeny sa použije na pracovný príkaz a všetky aktíva, umiestnenia a položky konfigurácie v jeho dcérskych pracovných príkazoch. Pojem "pracovný príkaz" môže referovať záznam o pracovnom príkaze, zmene, vydaní alebo aktivite. - Vytvorenie súvisiacich záznamov - Je možné vytvoriť nové záznamy a priradiť ich k vášmu vydaniu. Nové záznamy môžu byť vydania, incidenty, problém, vydania, žiadosti o službu a pracovné príkazy. Súvisiace záznamy je možné zobraziť na záložke Súvisiace záznamy. - Kategorizácia úloh vo vydaniach klasifikáciami a atribútmi - Proces hľadania a manažovania záznamov možno zjednodušiť kategorizáciou úloh vo vydaniach. Kategorizácia úloh zahŕňa klasifikáciu a tiež pridanie a zmenu atribútov na ďalšie zoskupenie klasifikácie. - Nastavenie tokov pracovného procesu - Toky pracovného procesu používajú vzťahy medzi pracovnými príkazmi a úlohami na automatizáciu toku zmien stavu. Je možné nastaviť vzťahy medzi pracovnými príkazmi a úlohami, aby sa pri dokončení úlohy mohla iniciovať ďalšia úloha v toku. - Zmena stavu zoznamu záznamov - V aplikáciách je možné meniť stav viacerých záznamov.
FP-7 Event Management	Event management je proces zodpovedný za riadenie udalostí. Udalosť (event) je zmena stavu, ktorá je významná z hľadiska riadenia konfiguračnej položky, alebo služby IT. V rámci procesu Event management podporuje SD systém: - integračné rozhranie pre automatické vytváranie incidentov z centrálneho monitorovacieho systému - poskytovanie informácií o schválených odstávkach poskytovaných služieb centrálnemu monitorovaciemu systému
FP-8 Service Asset and Configuration Management	Manažment riadenia aktív a konfigurácií (Service asset and configuration management) Proces zodpovedá najmä za to, že aktíva požadované pre dodávku služieb sú správne riadené, a že o týchto aktívach sú k dispozícii presné a spoľahlivé informácie kdekoľvek a kedykoľvek sú potrebné. Najdôležitejšou zodpovednosťou procesu je vlastníctvo systému konfiguračného manažmentu (ktorý sa typicky skladá z niekoľkých konfiguračných databáz a prípadne ďalších integrovaných dátových zdrojov) a z toho vyplývajúca zodpovednosť za aktuálnosť údajov a informácií v ňom uložených.

A.5 Service Desk systém -	
Name	
	SD Systém v oblasti podpory procesu SCAM plne spĺňa a podporuje: - štruktúrovaná konfiguračná databáza (CMDB) - kategorizácia konfiguračných prvkov (CI), rôzne typy vzťahov medzi CI - evidencia konfiguračných prvkov v CMDB so vzájomnými vzťahmi - jednoduchá zmena konfigurácie a štruktúry CMDB (pridávanie/zmena atribútov pre jednotlivé typy CI, povinné polia, validácie), bez nutnosti programovania - podpora pre integráciu s discovery nástrojmi - grafická vizualizácia konfiguračných prvkov a väzieb medzi nimi s možnosťou navigácie v CMDB prostredníctvom topológie - poskytovanie dát ostaným prevádzkovým procesom (Incident Management, Change management, CHM...) pre zefektívnenie ich vykonávania zaznamenávanie histórie zmien CI, počas celého ich životného cyklu

Proces SCAM je v systéme SD podporený primárne modulom Infraštruktúra IT a modulom Aktíva.	
FP-9 Service Level Management	Manažment poskytovania služieb (Service level management) Proces SLM sa zaoberá plánovaním, koordináciou, návrhom, uzatváraním, monitorovaním a vyhodnocovaním dohôd a zmlúv o poskytovaní servisnej a prevádzkovej podpory dohodnutej so zákazníkmi vo forme SLA, dohôd a UC. Proces tvorí spojovací článok medzi poskytovateľom a odberateľom IT služieb. Snahou procesu je nájsť kompromis medzi požiadavkami na kvalitu a nákladmi poskytovaných služieb a poskytovanie služby presne vyšpecifikovať a formalizovať do dokumentov - dohôd SLA. Systém SD podporuje: - evidencia rôznych dohodnutých parametrov úrovne služieb - dostupnosť, spoľahlivosť, požadované časy odozvy a riešenia - meranie a vyhodnocovanie dohodnutých časov odozvy a riešenia pre jednotlivé poskytované služby v závislosti od rôznych parametrov (napr.: služba, priorita) - eskalácie v rámci priebehu monitorovania dohodnutých časov spracovania a riešenia incidentov a požiadaviek Proces SLM je v systéme SD primárne podporený aplikáciou Zmluvy o úrovni služieb (Service Level Agreements (SP)), ktorá umožňuje vytváranie a manažovanie zmlúv o úrovni služieb. Zmluvy o úrovni služieb dokumentujú záväzky medzi poskytovateľmi služieb a zákazníkmi. Služby sa skladajú z úloh, ktoré poskytovatelia služieb vykonávajú na splnenie potrieb zákazníka. Záväzky sú zodpovednosti, ktoré musia poskytovatelia služieb dodržiavať na splnenie zmlúv o úrovni služieb.

	Zmluvy o úrovni služieb existujú na úrovni systému. Zmluvy o úrovni služieb je možné obmedziť na úroveň organizácie alebo lokality. Pri vytvorení zmluvy o úrovni služieb, je možné vykonať tieto funkcie: - Hodnotiť zmluvy o úrovni služieb podľa priority, ktorá určuje, ktorá zmluva o úrovni služieb sa použije - Nastaviť začiatočný dátum platnosti, koncový dátum a dátum posúdenia pre zmluvu o úrovni služieb, čo je možné použiť na riadenie procesu pracovného toku - Priradiť zmluvy k zmluve o úrovni služieb - Priradiť súvisiace zmluvy o úrovni služieb k aktuálnej zmluve o úrovni služieb - Priradiť aktíva a umiestnenia k zmluve o úrovni služieb - Vytvoriť kľúčové indikátory výkonu alebo metriky pre zmluvu o úrovni služieb - Vytvoriť eskaláciu na podporu záväzkov v zmluve o úrovni služieb Používatelia systému SD môžu použiť platné zmluvy o úrovni služieb v rámci záznamov z iných aplikácií, napríklad v Incidentoch, Problémoch, Zmenách. Aplikáciu Zmluvy o úrovni služieb a funkčnosť eskalácií je možné použiť na manažovanie a plnenie záväzkov v zmluve o úrovni služieb. Eskalácia je funkcia, ktorá automaticky monitoruje kritické procesy. Zmluva o úrovni služieb môže mať jeden alebo viacero záväzkov, pričom každý má vlastné body eskalácie. Ak má zmluva o úrovni služieb dva záväzky, každý má iný bod eskalácie. Prvý záväzok je odpovedať na všetky incidenty do dvoch hodín. Bod eskalácie pre prvý záväzok upozorní supervízora, ak sa neposkytne odpoveď po prvej hodine. Druhý záväzok je vyriešiť všetky incidenty, do štyroch hodín. Bod eskalácie pre druhý záväzok kontroluje stav incidentu po dvoch hodinách. Ak je incident stále otvorený, vlastníctvo incidentu sa presunie na supervízora.
FP-10 Service Catalogue Management	Manažment katalógu služieb (Service catalogue management) SD systém v oblasti podpory procesu Manažmentu katalógu služieb podporuje: - vytváranie a udržiavanie rôznych pohľadov na katalóg služieb (Technical Service Catalog, Business Service Catalog) - musí poskytovať web rozhranie pre evidenciu požiadaviek o službu (podľa definovaného biznis katalógu služieb)
FP-11 Všeobecné požiadavky	Riešenie obsahuje funkčnosti spĺňajúce nasledovné všeobecné požiadavky: - poskytuje plnohodnotné webové rozhranie pre

	používateľov aj administrátorov - umožnuje jednoduchú implementáciu zmien v aplikácii, vyplývajúcich zo zmeny/úpravy prevádzkových procesov (v réžii obstarávateľa, bez nutnosti programovania) - umožnuje jednoduchú konfiguráciu a zmenu používateľského rozhrania (v réžii obstarávateľa, bez nutnosti programovania) - umožnuje pridávať, meniť a mazať dohodnuté procesné notifikácie a eskalácie prostredníctvom grafického používateľského rozhrania (v réžii obstarávateľa, bez nutnosti programovania) - umožnuje používateľom prispôsobiť si vzhľad úvodnej obrazovky

1.1.2 Časť - Zavedenie IT procesov riadenia prevádzky

Business layer A.1 Zavedenie IT procesov riadenia prevádzky
Procesy riadenia prevádzky sú v ponuknutom riešení implementované v súlade s rámcom frameworku ITIL v3. Prevádzka služby koordinuje a vykonáva aktivity a procesy potrebné na dodávku a riadenie služieb na dohodnutej úrovni pre používateľov podniku a zákazníkov. Prevádzka služby tiež riadi technológiu, ktorá je používaná na dodávku a podporu služieb.

A.1 Zavedenie IT procesov riadenia prevádzky -	
Name	
FP-12 cieľ a rozsah	Cieľom prevádzky vo všeobecnosti je zabezpečiť bezproblémový chod NZIS počas celej jeho životnosti, ako aj minimalizovať prevádzkové náklady súvisiace s prevádzkou NZIS. Kľúčovým faktorom pre naplnenie tohto cieľa je nastavenie a zavedenie IT procesov v rámci prevádzky všetkých existujúcich prostredí NZIS.
FP-13 metodika ITIL v3	V rámci dodávky riešenia budú v spolupráci s obstarávateľom navrhnuté a zavedené IT procesy riadenia prevádzky v súlade s odporúčaniami metodiky ITIL v3 v rozsahu: - manažment incidentov (Incident management) - manažment udalostí (Event management) - manažment požiadaviek (Request fulfilment management) - manažment prístupov (Access management) - manažment problémov (Problem management) - manažment riadenia aktív a konfigurácií (Service asset and configuration management) - manažment zmien (Change management) - manažment vydaní a nasadení (Release and deployment management) - manažment kontinuity IT služieb (IT service continuity management) - manažment kapacít (Capacity management) - manažment dostupností (Availability management) - manažment poskytovania služieb (Service level management) - manažment katalógu služieb (Service catalogue management) - finančný manažment pre IT služby (Financial management for IT services) Zároveň bude pre všetky uvedené procesy vypracovaná procesná dokumentácia, ktorá bude obsahovať: - cieľ a rozsah procesu - procesné aktivity a postupy - role a zodpovednosti - procesné pravidlá - metriky a reporty

1.1.3 Časť - Centrálny monitorovací systém

Business layer A.3 Centrálny monitorovací systém
Riešenie zabezpečí dodávku, parametrizáciu a nasadenie centrálneho monitorovacieho systému ako nástroja proaktívnej podpory pre služby poskytované v rámci NZIS. Centrálnym monitorovacím nástrojom

budú monitorované všetky existujúce prostredia NZIS a v rámci nich minimálne tieto oblasti:

- monitoring harvéru
- monitoring sieťových a bezpečnostných komponentov
- monitoring operačných systémov a platformových produktov
- monitoring aplikácií a biznis služieb

A.3 Centrálny monitorovací systém -	
Name	
FP-14 Funkčné požiadavky na centrálny monitorovací systém:	- riešenie je schopné spracovania výstupov z iných monitorovacích nástrojov a vytvorenia jednotného monitoring nástroja (tzv. umbrella monitoringu) - nástroje riešenia sú schopné vyhodnotenia modelov služieb vytvorených na základe informácií z centrálnej konfiguračnej databázy CMDB evidovanej v rámci SD systému - vyhodnotenie modelov služieb prebieha na základe informácií (udalostí) z dostupných monitoring nástrojov - riešenie zabezpečuje realizáciu monitoringu služieb z pohľadu koncového používateľa - riešenie poskytuje prehľadné rozhrania pre vizualizáciu aktuálneho stavu služieb a rýchle vyhľadanie príčin výpadkov (root cause) - pri výpadku IT zdroja zachytenom monitorovacími nástrojmi systém identifikuje jeho dopad na poskytované služby (impact analysis) - výstupy z CMS sú previazané s procesným nástrojom (automatická tvorba incidentov pre vyhodnotenie poskytovanej úrovne kvality služieb) - riešenie umožnuje vyhodnotenie plánovania výpadkov infraštruktúry a služieb - riešenie umožnuje prístup k monitoring nástrojom s využitím „Single Sign On“ a externej autentifikácie cez AD/LDAP
FP-15 Požiadavky na reportingové nástroje CMS	- nástroj pre spracovanie výstupov z monitoringu poskytuje robustný a schopný rýchleho spracovania a vyhodnotenia dát aj v kritických situáciách (napr. pri vygenerovaní veľkého množstva udalostí) - spracovanie vstupných dát vo forme udalostí je jednoducho a prehľadne konfigurovateľné - riešenie zabezpečuje identifikáciu kritických udalostí nielen podľa základného parametra kritickosti zdroja "severity" ale aj s využitím doplnkovej informácie o dopade (informácia o kritickosti konkrétneho objektu v rámci služby v danom čase) - nástroj riešenia podporuje korelácie udalostí minimálne na úrovni párovania up/down správ, deduplikácie, zmeny priority na základe zdroja udalosti a času - riešenie podporuje štandardné rozhrania pre integráciu s inými nástrojmi (SNMP, WebServices) - riešenie podporuje integráciu s nástrojom Microsoft SCOM 2012 (metódou „out of the box“) - riešenie priamo podporuje príjem udalostí cez SNMP, Syslog, JMX a WMI z rôznych zariadení a systémov

1.1.4 Časť - DRP plány a zálohovanie JRUZ

Business layer A.4 DRP plány a zálohovanie JRUZ
Pre zabezpečenie kontinuity prevádzky systémov a služieb poskytovaných v rámci produkčného prostredia

projektu JRUZ Pripravene DRP plány zabezpečujú:

- inventarizáciu systémov a služieb
- analýzu rizík a analýzu dopadov
- definovanie stratégie obnovy
- vypracovanie návrhu zálohovania systémov a dát
- dodávku, konfiguráciu a nasadenie zálohovacieho riešenia
- vypracovanie plánov obnovy (DRP)
- otestovanie plánov obnovy (DRP)

A.4 DRP plány a zálohovanie JRUZ -	
Name	
FP-16 Analýza rizík	Pomocou analýzy rizík a analýzy dopadov je špecifikovaná pravdepodobnosť výskytu rizík pôsobiacich na prevádzkované systémy a služby a zadefinovať stratégiu obnovy prevádzky kľúčových systémov a služieb vrátane stanovenia priorít obnovy. V zmysle analýzy dopadov je pre jednotlivé systémy a služby zedefinované RTO a RPO parametre popisujúce: - maximálny akceptovateľný čas výpadku systému alebo služby (RTO) - maximálne prípustnú stratu dát za definovaný čas (RPO)
FP-17 Rozsah DRP plánov	DRP plány sú vypravované tak že zohľadnujú nasledovné havarijné scenáre: - výpadok elektrického napájania - výpadok sieťovej konektivity - výpadok kľúčových prvkov infraštruktúry - výpadok spôsobený počítačovým vírusom resp. hackerom - výpadok spôsobený pôsobením prírodných živlov (povodeň, požiar, zemetrasenie) DRP plány obsahujú zoznam činností, ktoré je potrebné vykonať bezprostredne po výskyte mimoriadnej udalosti, na ktorú je havarijný plán písaný vrátane informácií o tom: - kto môže havarijný plán spustiť - kto má čo robiť a v akej postupnosti - aký je účel plánu - aký je cieľový stav po realizácií havarijného plánu Za účelom zabezpečenia kvality, efektívnosti a aktuálnosti DRP plánov budú jednotlivé plány otestované.
FP-18 Zálohovanie systémov JRUZ	Cieľom zálohovania systémov a dát produkčného prostredia JRUZ je mať k dispozícií kópie produkčných dát pre prípad potreby ich obnovy. Implementované je: - vypracovanie návrhu, implementáciu a otestovanie zálohovacieho riešenia vrátane potrebnej infraštruktúry s ohľadom na rozšírenie existujúceho zálohovacieho riešenia implementovaného v rámci ESZ - vytvorenie rutinných procedúr a predpisov pre vykonávanie odsúhlasenej zálohovacej politiky a stratégie vytvárania záložných kópií dát a nacvičovania ich včasnej obnovy Funkčné požiadavky na zálohovacie riešenie: Riešenie zabezpečuje zálohovanie a obnovu: - elektronických dát vytvorených v rámci prostredia JRUZ s garanciou ich integrity

A.4 DRP plány a zálohovanie JRUZ -	
Name	
	a dostupnosti - systémových časti prostredia (napr. databáz, virtuálnych serverov, konfiguračných súborov) s garanciou ich integrity a dostupnosti - riešenie je spoľahlivé a vhodne automatizované - riešenie umožnuje dodržanie stanovených parametrov RPO a RTO - riešenie je navrhnuté tak aby v primeranej miere ovplyvňovali prevádzku poskytovaných služieb z hľadiska výkonu a dostupnosti.

1.2 Požiadavky na bezpečnosť

1.2.1 Funkčné požiadavky

FP-19 Prepojenie produkčného prostredia projektu JRUZ s CMS	Prepojenie produkčného prostredia projektu JRUZ s CMS: - prepojenie bude vytvorené za účelom monitorovania infraštruktúry a systémov prostredia projektu JRUZ - uvedené prepojenie bude kontrolované dodávaným firewallom, ktorý bude začlenený do infraštruktúry ESZ Systémy SD ani CMS nebudú obsahovať citlivé údaje ani neumožnia získať prístup k citlivým údajom ESZ. Na strane NCZI správcu a prevádzkovateľa NZIS budú vykonané opatrenia pre izoláciu sieťových segmentov obsahujúcich prvky riešenia od ostatných častí siete NCZI a ochranu komponentov pri prístupe z vnútra siete NCZI ako aj pri prístupe zvonku.
FP-20 Prístup používateľov do riešenia	Prístup užívateľov (human actorov) do riešenia: - administrátori a iné osoby predstavujúce II.úroveň podpory pristupujú na SD a CMS prostredníctvom existujúcej manažmentovej siete ESZ pri dodržaní rovnakých bezpečnostných opatrení ako sú definované projektom ESZ - agenti KC, predstavujúci I.úroveň podpory budú pristupovať: o k systému KC prostredníctvom infraštruktúry NCZI (správcu a prevádzkovateľa NZIS), pričom pri dátových tokoch ktoré sú mimo perimetra FOB NCZI bude zabezpečená ochrana dôvernosti a integrity a vzájomná autentizácia bodov zabezpečujúcich túto komunikáciu. Ochrana dátových tokov mimo perimetra FOB NCZI je predmetom riešenia. - k systémom SD a centrálneho monitorovacieho systému pomocou VPN z pracovnej stanice operátora, ukončovanej prostriedkami ESZ, pričom prenosová cesta bude zabezpečovaná z priestorov: o Lazaretská - pomocou existujúceho prepojenia so systémom ESZ ktoré zabezpečuje ochranu dôvernosti, integrity a vzájomnú autentizáciu bodov zabezpečujúcich túto komunikáciu Račianska - pomocou prepojenia s NCZI Lazaretská vytvoreného ako súčasť dodávaného riešenia a následne pomocou prepoja NCZI Lazaretská s ESZ. Prepojenia zabezpečia ochranu dôvernosti a integrity a vzájomnú autentizáciu bodov zabezpečujúcich túto komunikáciu
FP-21 Umiestnenie CC	Kontaktné centrum bude umiestnené v priestoroch NCZI mimo produkčného prostredia ESZ.
FP-22 Umiestnenie	Centrálny monitorovací systém bude umiestnený v blokoch EZS spôsobom:

CMS	- frontend server bude vo frontend zóne perimeter bloku ESZ, na virtuálnom serveri ktorý zdieľa fyzický virtualizačný server s virtuálnymi servermi Service Desk backend bude umiestnený v manažmentovej sieti na dedikovanom virtualizačnom serveri, pričom jeho oddelenie a ochranu bude zabezpečovať nový firewall, ktorý bude súčasťou dodávky riešenia
FP-23 Umiestnenie SD	Service Desk bude umiestnený v perimeter bloku ESZ nasledovne: - aplikačný komponent SD bude umiestnený vo frontend zóne bloku perimetra - backend SD bude umiestnený v backend zóne bloku perimetra - komponenty systému SD budú umiestnené na dedikovanom virtualizačnom serveri, oddelenom fyzicky od produkčných serverov ESZ
FP-24 Umiestnenie SD a CSM	Infraštruktúra SD a CMS bude priamo integrovaná do ESZ vrátane sieťovej a bezpečnostnej infraštruktúry tak aby sa neznížila úroveň zabezpečenia ESZ.

1.3 Požiadavky na Kontaktné centrum

Folder C Kontaktné centrum
Za účelom poskytovania reaktívnej podpory pre občanov a zdravotníckych je: Riešenie KC je dimenzované tak, aby zabezpečilo bezproblémovú prevádzku pri nasledujúcich očakávaných počtoch operátorov KC na dvoch lokalitách: celkový počet operátorov pre zabezpečenie prvého kontaktu (1.úroveň podpory) pre služby NZIS = 15ks - 1. 10 operátorov - lokalita NCZI Račianska - 2. 5 operátorov - lokalita NCZI Lazaretská Z technologického pohľadu riešenie KC spĺňa nasledovné požiadavky moderného riešenia: - rozšíriteľnosť - riešenie počíta s postupným nárastom kapacity supervízorov, agentov, ale aj IVR stromov (min. na dvojnásobný počet) - modulárnosť - riešenie počíta s postupným dopĺňaním nových služieb a komunikačných kanálov ako napríklad s prístupom na sociálne siete, KC s podporou videa alebo nástrojmi na riadenie pracovnej sily - flexibilita - riešenie je flexibilné z pohľadu umiestnenia a využívania ľudských zdrojov a tiež schopné vytvárať virtuálne KC skupiny v rôznych geografických lokalitách - integrácia - v oblasti informačných systémov KC umožní integráciu so systémami zákazníka na úrovni webservisov, čítania a zápisu do databáz, prípadne použitím štandardizovaných rozhraní Operátori KC budú mať k dispozícii aktívny prístup k znalostnej databáze, aby bola pre rutinnú prevádzku zabezpečená čo najväčšia univerzálnosť operátorov a tím špecialistov. Podrobnejšia technická špecifikácia je popísaná v technických požiadavkách KC. Agent kontaktného centra bude pracovať s jednou aplikáciou (konkrétne s aplikáciou IS KC), v rámci ktorej mu bude umožnený interaktívny prístup cez iFrame do systému IS SD. Integrácia tohto typu umožní agentom kontaktného centra automatizovaný a rýchly prístup k informáciám uloženým v rámci IS SD ako napríklad: • predfiltrovanie posledných riešených incidentov účastníka u práve prebiehajúceho telefonického rozhovoru na základe telefónneho čísla, • predvyplnie základných informácií účastníka do formulára, za účelom založenia novej udalosti v rámci systému IS SD z prostredia aplikácie IS KC.

1.3.1 Funkčné požiadavky

Business layer Funkčné požiadavky
Zákazník definoval svoje funkčné a iné požiadavky na základe ktorých sme navrhli komplexné riešenie ktoré bude spĺňat definované nároky.

Funkčné požiadavky -	
Name	
FP-25 automatické smerovanie podľa zručností (IVR-Interactive Voice Response)	Riešenie obsahuje pre oblasť IVR nasledujúce funkčnosti: - funkcia IVR umožní odovzdať, resp. prijať určité informácie od koncového používateľa bez nutnej spoluúčasti aktívneho agenta - systém poskytne vizuálne rozhranie pre konfiguráciu a správu IVR v administratívnom rozhraní - administratívne rozhranie poskytne funkcie ako: - vetvenie IVR stromov - nastavenie výziev a číselných volieb (tónovej voľby DTMF-Dual Tone Multi Frequency) - smerovanie hovorov podľa zručností agentov - definovanie hudby pre čakajúce hovory vo frontách
FP-26 automatizované smerovanie hovorov na voľných operátorov (ACD-Automatic Call Distribution)	Riešenie obsahuje pre oblasť smerovania hovorov nasledujúce funkčnosti: prostredníctvom funkcie ACD bude zabezpečené smerovanie, triedenie a frontovanie prichádzajúcich hovorov
FP-27 funkcia Wrap-Up time	Riešenie obsahuje pre oblasť Wrap-Up time nasledujúce funkčnosti: - systém poskytne operátorovi KC po skončení hovoru čas potrebný na zaznamenánie údajov o ukončenom hovore
FP-28 funkcia konferenčného hovoru	Riešenie obsahuje pre oblasť konferenčných hovorov nasledujúcu funkčnosť: - systém umožní operátorovi presmerovať hovor na ďalšieho účastníka (operátora), z ktorých vytvorí konferenčný hovor
FP-29 funkcia odposluchu hovoru agenta	Riešenie obsahuje pre oblasť odposluch horu agenta nasledujúce funkčnosti: - systém umožní supervízorom KC pasívny vstup do zvoleného prebiehajúceho hovoru na KC
FP-30 funkcia podržania hovoru - Hold on	Riešenie obsahuje pre oblasť podržania hovoru nasledujúce funkčnosti: - systém umožní podržanie prebiehajúceho hovoru na voľbu operátora
FP-31 funkcia presmerovania hovoru	Riešenie obsahuje pre oblasť presmerovanie hovorov nasledujúce funkčnosti: - systém umožní operátorovi KC presmerovať prebiehajúci hovor na iného agenta, skupinu agentov s potrebným súborom zručností, telefónne číslo...
FP-32 funkcia vstúpiť	- systém umožní supervízorom KC aktívny vstup do zvoleného prebiehajúceho

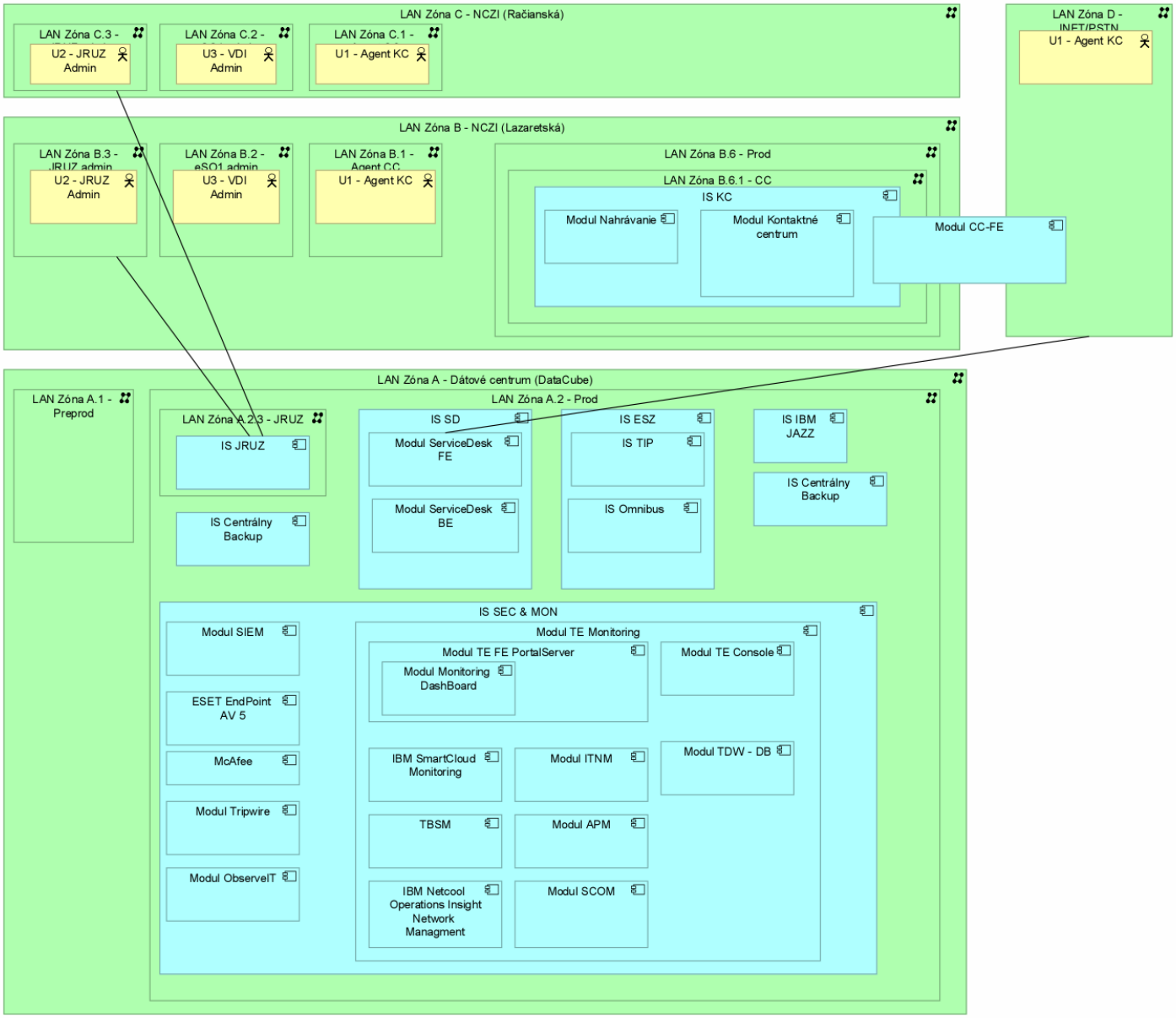
Funkčné požiadavky -		
	Name	
	do hovoru agenta s volajúcim	hovoru agenta s volajúcim
FP-33	manažment hovoru na pracovnej stanici operátora	- systém umožní na pracovnej ploche operátora KC umiestniť integrovanú lištu s ovládačmi potrebnými pre manažment hovorov (zdvihnúť, zložiť, presmerovať, nahrávať, podržať hovor, ...)
FP-34	nástroj pre správu threshold-ov vyťaženia KC (service level), upravovateľné eskalácie dosiahnutia stanovených limitov	- systém umožňuje monitorovať hovory v čakacej rade a čas od vytvorenia incidentu po zmenu na vybrané stavy. V administrácii aplikácie musí byť možnosť nastaviť SLA parametre pre uvedené monitorovanie, následne vyhodnocovať reálny čas úrovne poskytovanej služby s požadovanou (interná SLA). Pri prekročení limitov systém vie zaslať notifikácie supervízorom KC
FP-35	priradenie záznamu hovoru k incidentu	- pri vytvorení nového incidentu alebo aktualizácii existujúceho incidentu kanálom telefón, systém umožní priradenie záznamu hovoru k predmetnému incidentu
FP-36	service level monitoring pre KC	- Riešenie obsahuje pre oblasť Service level monitoring nasledujúce funkčnosti: - systém umožňuje naživo monitorovať (live monitoring) úroveň poskytovaných služieb KC - systém umožňuje naživo reportovať (live reporting) počet volajúcich čakajúcich vo frontách, počet volajúcich, ktorí zavesili pred spojením s operátorom ...
FP-37	viac jazyčné IVR	- systém umožňuje konfiguráciu IVR stromu vo viacerých jazykových mutáciách, primárne v slovenskom jazyku
FP-38	viaceré fronty hovorov	- systém umožňuje nastavenie viacerých front pre volajúcich klientov do KC, ktoré budú obsluhované zadefinovanými skupinami riešiteľov podľa ich súboru zručností
FP-39	zadržanie volajúceho na linke prostredníctvom špecifikovanej hudby	- systém umožňuje nastavenie špecifickej hudby pre klientov čakajúcich vo fronte
FP-40	zaznamenávanie hovoru (automatické i manuálne)	- systém umožňuje nastavenie automatického zaznamenávania všetkých volaní na KC po spojení s operátorom a tiež umožní spustiť nahrávanie operátorovi KC počas hovoru

2 Používatelia IS

Infraštruktúra SD a CMS bude priamo integrovaná do ESZ vrátane sieťovej a bezpečnostnej infraštruktúry tak aby sa neznížila úroveň zabezpečenia ESZ. Prístup a oprávnenia budú definované na základe nižsie uvedenej tabuľky. Pri implementáci zakázky budú prípadne pridaný nový užívateĺia.

Používatelia IS -	
Name	
U1 - Agent KC	agenti KC, predstavujúci I.úroveň podpory a budú pristupovať: - k systému KC prostredníctvom infraštruktúry NCZI (správcu a prevádzkovateľa NZIS), pričom pri dátových tokoch ktoré sú mimo perimetra FOB NCZI bude zabezpečená ochrana dôvernosti a integrity a vzájomná autentizácia bodov zabezpečujúcich túto komunikáciu. Ochrana dátových tokov mimo perimetra FOB NCZI je predmetom riešenia. - k systémom SD a centrálneho monitorovacieho systému pomocou VPN z pracovnej stanice operátora, ukončovanej prostriedkami ESZ, pričom prenosová cesta bude zabezpečovaná z priestorov: o Lazaretská - pomocou existujúceho prepojenia so systémom ESZ ktoré zabezpečuje ochranu dôvernosti, integrity a vzájomnú autentizáciu bodov zabezpečujúcich túto komunikáciu o Račianska - pomocou prepojenia s NCZI Lazaretská vytvoreného ako súčasť dodávaného riešenia a následne pomocou prepoja NCZI Lazaretská s ESZ. Prepojenia zabezpečia ochranu dôvernosti a integrity a vzájomnú autentizáciu bodov zabezpečujúcich túto komunikáciu
U2 - JRUZ Admin	administrátori JRUZ predstavujú II.úroveň podpory pristupujú na SD a CMS prostredníctvom existujúcej manažmentovej siete ESZ pri dodržaní rovnakých bezpečnostných opatrení ako sú definované projektom ESZ
U3 - VDI Admin	administrátori VDI predstavujúce II.úroveň podpory pristupujú na SD a CMS prostredníctvom existujúcej manažmentovej siete ESZ pri dodržaní rovnakých bezpečnostných opatrení ako sú definované projektom ESZ

3 Aplikačná architektúra



3.1 IS KC

3.1.1 Modul Kontaktné centrum

Na základe požiadaviek zákazníka je potrebné dodanie komponentov, v množstve a typoch podľa tabuľky nižšie, ktoré musia spĺňať detailné minimálne požiadavky s dĺžkou podpory 5 rokov:

HW POLOŽKA	MERNÁ JEDNOTKA	POČET KUSOV
Kontaktné centrum	kus	1
IP telefón pre operátora KC	kus	15
Slúchadlá pre operátora KC	kus	15
Pracovná stanica pre operátora KC	kus	15

Funkčné požiadavky na kontaktné centrum sú popísané v kapitole 1.3 Požiadavky na Kontaktné centrum . Z

technologického hľadiska kontaktné centrum pozostáva z týchto častí:

- systém centrálnej logiky KC (procesovanie hovorov, frontovanie hovorov)
- hlasová brána na prestup do verejnej telefónnej siete
- systém pre nahrávanie hovorov

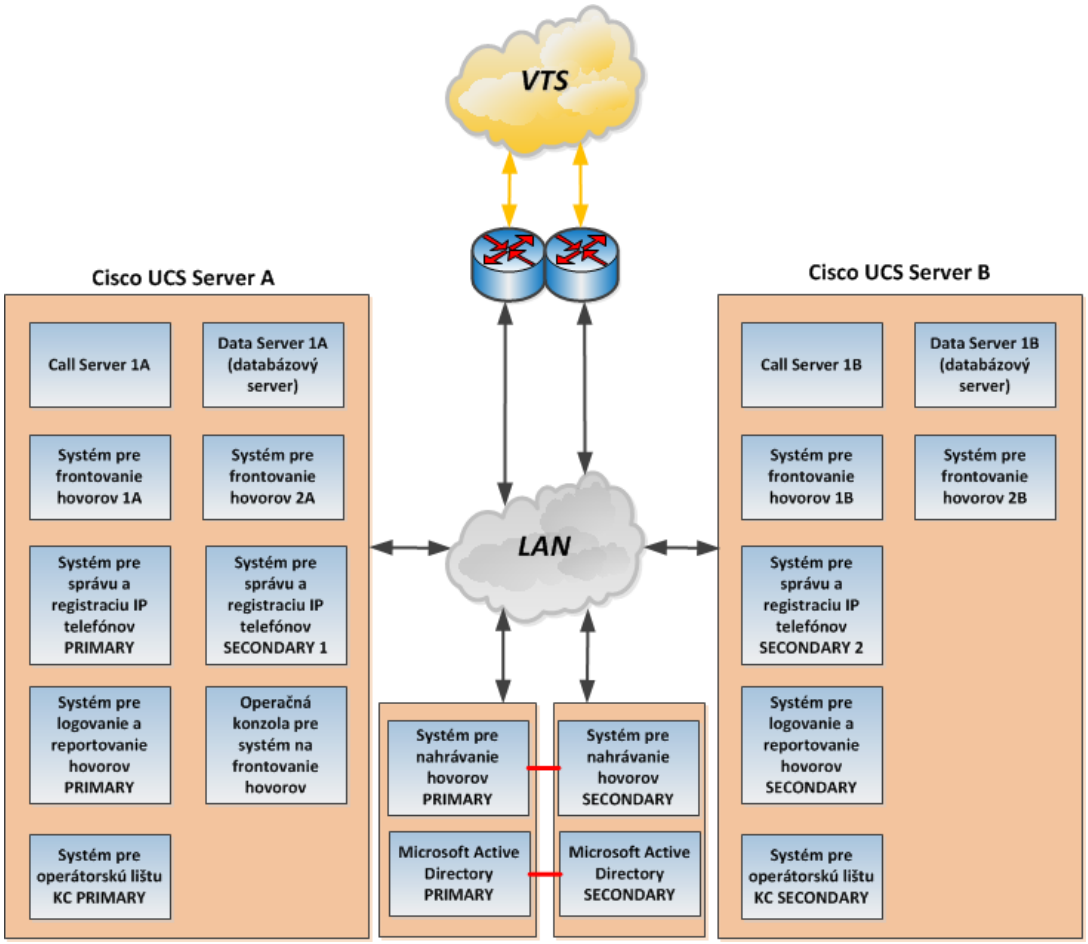
Systém centrálnej logiky KC prináša všetky komponenty potrebné k správnemu a bezchybnému chodu KC. Požadované komponenty KC budú nainštalované a nasadené ako virtualne servery na dvoch fyzických Cisco UCS serveroch v reduntdantnom zapojení, to znamená, že všetky komponenty KC budú redundantné. Takouto podporavanou inštaláciou sa zabezpečí vysoká dostupnosť a ani pri výpadku jedného zo serverov, fyzického alebo virtuálneho, nenastane nedostupnosť žiadnej zo služby KC. Navrhovaný Cisco UCS C240 M3 server je už hardvérovo predkonfigurovaný a pripravený na inštaláciu operačných systémov. Pri zapnutí Cisco UCS servera prebehne inštalácia VMware ESXi operačného systému, kde sa zadefinujú zakladné informácie o danom fyzickom servery.

- prevedenie - Rack 19“
- výška zariadenia - max. 2U
- 2 x 2.70 GHz E5-2680
- 96GB vnútornej operačnej pamäte max 768GB
- 16 x 2.5-inch 300GB 6Gb SAS 15k diskov max 24 x 2.5-inch
- 5 x rozšíriteľný PCIe moduly
- 5 x 10/100/1000 integrované RJ-45 porty

Požiadavky na prevádzku KC a používateľské rozhranie:

- kompletné riešenia KC musí byť schopné behu na jednom fyzickom serveri v redundantnom zapojení a vysokej dostupnosti
- riešenie KC musí byť schopné z pohľadu stavu hardvéru poskytnúť:
    - jednotný inventárny výpis hardvéru KC
    - sledovanie stavu hardvéru KC
    - posielanie oznámení o stave hardvéru KC
- musí podporovať jednotné zberanie a zobrazenie logovania na jednom mieste
- musí podporovať multi operácie - zmenu viacerých položiek naraz z jedného miesta

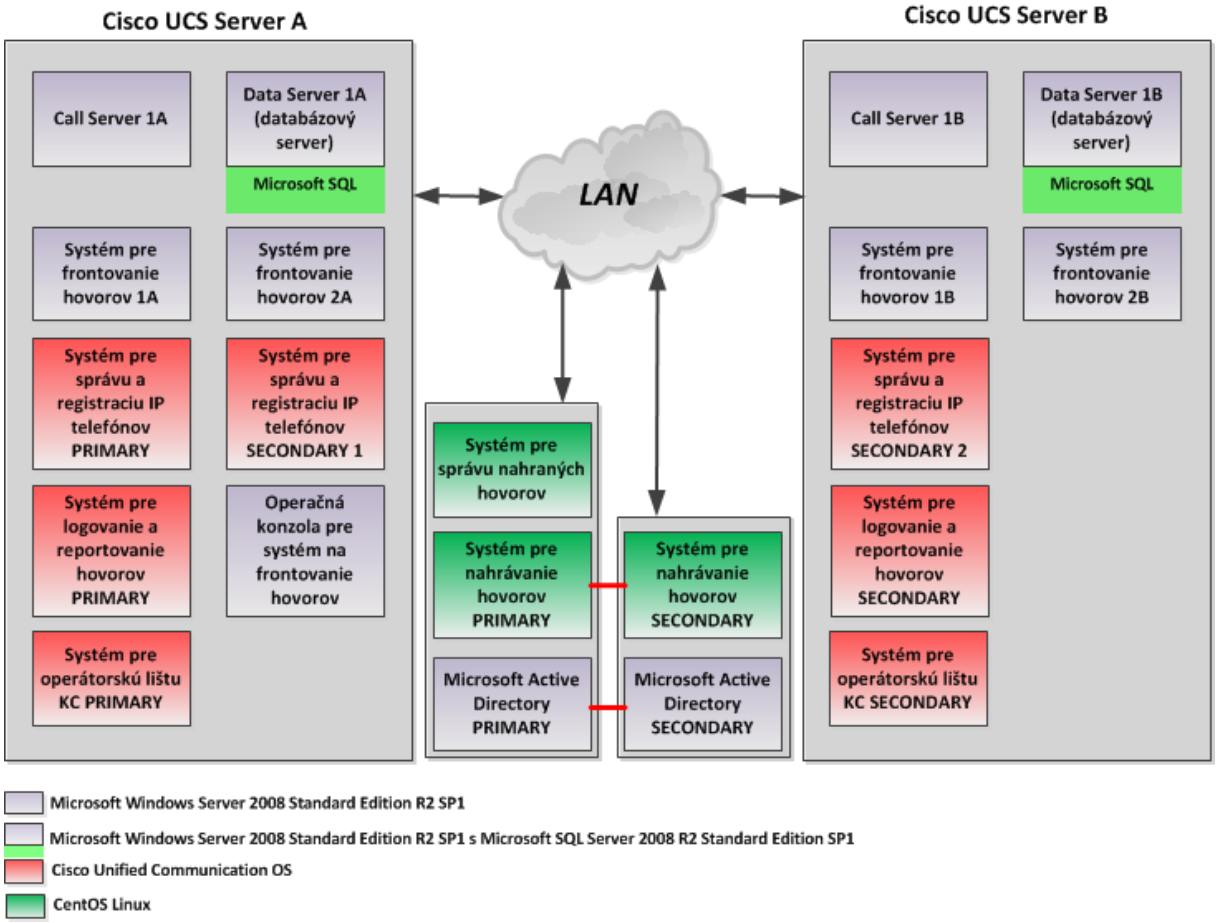
Technické požiadavky na systém centrálnej logiky KC - navrhovaný systém centrálnej logicky KC spĺňa všetky technické požiadavky, ktoré sů uvedené nižšie:



- systém centrálnej logiky KC
- konfigurovateľné rozhranie pre agentov
- integrácia so systémami tretích strán (CTI, Webservice)
- jednoduchý prístup k aplikáciám prístupných cez web rozhranie
- vytváranie a úpravu reportov
- manuálne a automatizované generovanie reportov
- automatizovanú distribúciu reportov prostredníctvom emailu
- možnosť exportu reportov minimálne do formátov PDF, XLS a CSV
- systém pre správu hovorov - rozširuje telefónne funkcie a schopnosti paketových telefónnych sietí tvorených IP telefónmi, zariadenia pre spracovanie multimediálneho obsahu, Voice-over-IP (VoIP) hlasovými bránami a multimediálnymi aplikáciami.
- softvérová IPT ústredňa
- podpora hlasu a videa na jednej platforme
- podpora protokolov RTCP, SRTP, BFCP, FECC
- podpora hlasových protokolov - SIP, SCCP, MGCP, H323, EMCC
- integrácia so systémami tretích strán
- podpora IVR iterácií
- podpora XML (AXL) formátu
- podpora LDAP protokolu
- podpora jednotného prihlásenia sa do systému (SSO)
- natívna podpora IM (Instant Messaging)
- systém pre frontovanie hovorov - prináša nezávislosť na polohe operátorov, zvyšuje ich škálovateľnosť a poskytuje výkonne funkcie automatického rozdeľovania hovorov
- podmienené smerovanie hovorov, správy o zaradení do poradia a o odhadovanom čase do vybavenia, zobrazenie podnikových dát, real-time dát a historických údajov.
- doručovanie notifikácií používateľom
- podpora webových servisov typu WSDL a SOAP
- podpora RTSP, ASR, TTS a MRCPv2
- podpora SNMPv3

- podpora vysokej dostupnosti cez WAN (geografická redundancia)

Operačný systém a softvér pre komponenty KC potrebný pre správne fungovanie navrhovaného riešenia je zahrnutý v cenovej ponuke. Dodávané softvérové riešenie možeme rozdeliť do dvoch skupín, a to softvér priamo od výrobcu navrhovaného KC a softvér tretích strán. Softvér od spoločnosti Cisco Systems je operačným systémom postavený na distribúcii Red Hat Enterprise Linux tzv. Cisco Unified Communications Operating System. Softvér tretích strán bude od spoločnosti Microsoft a jej serverový operačný systém Windows Server 2008. Pre náhrávací softvér výrobca využíva pre svoju aplikáciu operačný systém CentOS Linux. Farebne označené operačné systémy sú zobrazené v obrázku nižšie.
Na základe požiadaviek zákazníka je potrebné dodanie komponentov, v množstve a typoch podľa tabuľky nižšie, ktoré musia spĺňať detailné minimálne požiadavky s dĺžkou podpory 5 rokov:



SW POLOŽKA	MERNÁ JEDNOTKA	POČET KUSOV
Microsoft Windows Server 2008 Standard Edition R2 SP1	kus	11
Microsoft SQL Server 2008 R2 Standard Edition SP1	kus	2
Cisco Unified Communication OS	kus	7
CentOS Linux	Kus	3
VMware vSphere	kus	4
VMware vCenter	kus	1

Funkčné požiadavky na kontaktné centrum sú popísané v kapitole. Z technologického hľadiska kontaktné centrum pozostáva z týchto častí:

- systém centrálnej logiky KC (procesovanie hovorov, frontovanie hovorov)
- hlasová brána na prestup do verejnej telefónnej siete
- systém pre nahrávanie hovorov

Systém centrálnej logiky KC prináša všetky komponenty potrebné k správnemu a bezchybnému chodu KC. Požadované komponenty KC budú nainštalované a nasadené ako virtualne servery na dvoch fyzických Cisco UCS serveroch v reduntdantnom zapojení, to znamená, že všetky komponenty KC budú redundantné. Takouto podporovanou inštaláciou sa zabezpečí vysoká dostupnosť a ani pri výpadku jedného zo serverov, fyzického alebo virtuálneho, nenastane nedostupnosť žiadnej zo služby KC. Navrhovaný Cisco UCS C240 M3 server je už hardvérovo predkonfigurovaný a pripravený na inštaláciu operačných systémov. Pri zapnutí Cisco UCS servera prebehne inštalácia VMware ESXi operačného systému, kde sa zadefinujú zakladné informácie o danom fyzickom servery.

- prevedenie - Rack 19“
- výška zariadenia - max. 2U
- 2 x 2.70 GHz E5-2680
- 96GB vnútornej operačnej pamäte max 768GB
- 16 x 2.5-inch 300GB 6Gb SAS 15k diskov max 24 x 2.5-inch
- 5 x rozšíriteľný PCIe moduly
- 5 x 10/100/1000 integrované RJ-45 porty
- Požiadavky na prevádzku KC a používateľské rozhranie:
- kompletné riešenia KC musí byť schopné behu na jednom fyzickom serveri v redundantnom zapojení a vysokej dostupnosti
- riešenie KC musí byť schopné z pohľadu stavu hardvéru poskytnúť:
    - jednotný inventárny výpis hardvéru KC
    - sledovanie stavu hardvéru KC
    - posielanie oznámení o stave hardvéru KC
- - musí podporovať jednotné zberanie a zobrazenie logovania na jednom mieste
- - musí podporovať multi operácie - zmenu viacerých položiek naraz z jedného miesta

Technické požiadavky na systém centrálnej logiky KC - navrhovaný systém centrálnej logicky KC spĺňa všetky technické požiadavky, ktoré sů uvedené nižšie:

- systém centrálnej logiky KC
    - konfigurovateľné rozhranie pre agentov
    - integrácia so systémami tretích strán (CTI, Webservice)
    - jednoduchý prístup k aplikáciám prístupných cez web rozhranie
    - vytváranie a úpravu reportov
    - manuálne a automatizované generovanie reportov
    - automatizovanú distribúciu reportov prostredníctvom emailu
    - možnosť exportu reportov minimálne do formátov PDF, XLS a CSV

- systém pre správu hovorov - rozširuje telefónne funkcie a schopnosti paketových telefónnych sietí tvorených IP telefónmi, zariadenia pre spracovanie multimediálneho obsahu, Voice-over-IP (VoIP) hlasovými bránami a multimediálnymi aplikáciami.

- softvérová IPT ústredňa
- podpora hlasu a videa na jednej platforme
- podpora protokolov RTCP, SRTP, BFCP, FECC
- podpora hlasových protokolov - SIP, SCCP, MGCP, H323, EMCC
- integrácia so systémami tretích strán
- podpora IVR iterácií
- podpora XML (AXL) formátu
- podpora LDAP protokolu
- podpora jednotného prihlásenia sa do systému (SSO)
- natívna podpora IM (Instant Messaging)

- systém pre frontovanie hovorov - prináša nezávislosť na polohe operátorov, zvyšuje ich škálovateľnosť a poskytuje výkonne funkcie automatického rozdeľovania hovorov - podmienené smerovanie hovorov, správy o zaradení do poradia a o odhadovanom čase do vybavenia, zobrazenie podnikových dát, real-time dát a historických údajov.

- doručovanie notifikácií používateľom
- podpora webových servisov typu WSDL a SOAP
- podpora RTSP, ASR, TTS a MRCPv2
- podpora SNMPv3
- podpora vysokej dostupnosti cez WAN (geografická redundancia)

Operačný systém a softvér pre komponenty KC potrebný pre správne fungovanie navrhovaného riešenia je zahrnutý v cenovej ponuke. Dodávané softvérové riešenie možeme rozdeliť do dvoch skupín, a to softvér priamo od výrobcu navrhovaného KC a softvér tretích strán. Softvér od spoločnosti Cisco Systems je operačným systémom postavený na distribúcii Red Hat Enterprise Linux tzv. Cisco Unified Communications Operating System. Softvér tretích strán bude od spoločnosti Microsoft a jej serverový operačný systém Windows Server 2008. Pre náhrávací softvér výrobca využíva pre svoju aplikáciu operačný systém CentOS Linux. Farebne označené operačné systémy sú zobrazené v obrázku nižšie.

Funkčné požiadavky na kontaktné centrum sú popísané v kapitole. Požiadavky na Kontaktné centrum Požiadavky na Kontaktné centrumZ technologického hľadiska musí kontaktné centrum pozostávať minimálne z týchto častí:

- - systém centrálnej logiky KC (procesovanie hovorov, frontovanie hovorov)
- - hlasová brána na prestup do verejnej telefónnej siete
- - systém pre nahrávanie hovorov
- Požiadavky na prevádzku KC a používateľské rozhranie:
    - - kompletné riešenia KC musí byť schopné behu na jednom fyzickom serveri v redundantnom zapojení a vysokej dostupnosti
- - riešenie KC musí byť schopné z pohľadu stavu hardvéru poskytnúť:
    - jednotný inventárny výpis hardvéru KC
    - sledovanie stavu hardvéru KC
    - posielanie oznámení o stave hardvéru KC
- - musí podporovať jednotné zberanie a zobrazenie logovania na jednom mieste
- - musí podporovať multi operácie - zmenu viacerých položiek naraz z jedného miesta
- Technické požiadavky na systém centrálnej logiky KC:
    - - systém centrálnej logiky KC
    - konfigurovateľné rozhranie pre agentov
- integrácia so systémami tretích strán (CTI, Webservice)
- jednoduchý prístup k aplikáciám prístupných cez web rozhranie
- vytváranie a úpravu reportov
- manuálne a automatizované generovanie reportov
- automatizovanú distribúciu reportov prostredníctvom emailu
- možnosť exportu reportov minimálne do formátov PDF, XLS a CSV
- - systém pre správu hovorov
- softvérová IPT ústredňa
- podpora hlasu a videa na jednej platforme
- podpora protokolov RTCP, SRTP, BFCP, FECC
- podpora hlasových protokolov - SIP, SCCP, MGCP, H323, EMCC
- integrácia so systémami tretích strán
- podpora IVR iterácií
- - podpora XML (AXL) formátu
- podpora LDAP protokolu
- podpora jednotného prihlásenia sa do systému (SSO)
- natívna podpora IM (Instant Messaging)
- - systém pre frontovanie hovorov
- doručovanie notifikácií používateľom
- podpora webových servisov typu WSDL a SOAP
- podpora RTSP, ASR, TTS a MRCPv2
- podpora SNMPv3
- podpora vysokej dostupnosti cez WAN (geografická redundancia)

3.1.2 Modul Nahrávanie

Technické požiadavky na systém pre nahrávanie hovorov – navrhovaný systém nahrávania hovorov Navrhovaný systém nahrávania hovorov ZOOM CallREC, spĺňa všetky technické požiadavky, ktoré sú uvedené nižšie. Systém nahrávania hovorov v navrhovanom riešení bude nasadený vo vysokej dostupnosti a škálovateľnosti s možnosťou nahrávania všetkých 15 operátorov súčastne a s pripravenosťou na postupné navyšovanie počtu operátorov. Vyhľadánie a kompletný menežment s už nahranými hovormi bude možné spracovávať na servery tzv. „Relay Server“, ktorý bude mať nadviazanú sieťovú konektivitu smerom na nahrávacie servery.

- systém umožňuje ukladanie všetkých nahrávok na centrálnom mieste
- systém umožňuje vyhľadávanie hovorov na základe rôznych filtrov vyhľadávania s možnosť uloženia použitých filtrov
- podpora formátov nahrávania hovorov – MP3, WAV
- systém je schopný vytvárať riadený archív hovorov, s možnosťou automatizovaného presunu alebo vymazania hovorov po uplynutí archivačnej doby
- podporované formáty zvuku – G.711a, G.711μ, G.729a, G.729ab, G.722
- systém umožňuje znázornenie celej konverzácie na jednej časovej osi
- kryptovanie a správa kľúčov:
    - štandardy kryptografie verejných kľúčov (PKCS12, JKS, JCEKS)
    - štandardné šifrovacie algoritmy (AES, DES, Blowfish)
    - šifrovanie nahraných hovorov a záznamov obrazoviek
- podpora a dodržiavanie štandardu PCI-DSS pre ochranu súkromných dát
- webové API pre integráciu s aplikáciami tretích strán

Pre produkt je požadovaná úroveň hardvérovej podpory zabezpečujúca Obstarávateľovi počas celej doby platnosti podpory využívať nasledujúce služby:
- technická podpora 8x5, reakčná doba NBD (nasledujúci pracovný deň).

3.1.3 Modul Brána do VTS

Technické požiadavky pre hlasovú bránu na prestup do VTS (Verejnej Telefónnej Siete) - navrhovaná hlasová brána Cisco 2911, spĺňa všetky technické požiadavky, ktoré sů uvedené nižšie. Na prestup do VTS je potrebné špeciálne zariadenie, v tomto prípade smerovač, ktorý zabezpečí transformáciu IP komunikácie do TDM komunikácie. V navrhovanom riešení sa použije ako fyzické médium na prestup do VTS E1 hlasová VWIC karta. Samozrejmosťou ostáva zachovanie redundancie a škálovateľnosti hlasových brán.

- prevedenie - Rack 19“
- výška zariadenia - max. 2U
- min. 256MB vnútornej pamäte rozšíriteľná do 4GB
- min. 512MB systémovej pamäte rozšíriteľná do 2.5GB
- integrované 3 x 10/100/1000 RJ-45 porty
- 1 x rozšíriteľný modul

- 4 x rozšíriteľné WAN sloty
- min. smerovací výkon 180 Mbps
- min. 32 kanálový procesor pre spracovanie hlasu
- podpora T1/E1 kariet a SIP trunk-u
- podpora IP telefónie
- podpora HW šifrovania - 3DES/DES, AES

3.2 IS SD

V rámci riešenia je dodávka, parametrizácia a nasadenie systému Service Desk ako podporného nástroja pre evidenciu a riadenie zavedených IT procesov prevádzky. Service Desk systém je založený na produkte IBM Control Desk, ktorý predstavuje štandardné, robustné a ľahko konfigurovateľné riešenie v oblasti podpory prevádzky a riadenia IT služieb.
Slúži ako jednotný kontaktný bod medzi poskytovateľom služieb a používateľom služieb.

3.2.1 Modul IBM Control Desk

Produkt IBM Control Desk je integrovaným riešením správy služieb, ktoré pomáha spravovať celý rad procesov, služieb a aktív IT. Produkt využíva odporúčania rámca ITIL v3 (Information Technology Infrastructure Library) a pomáha pri správe IT prostredia, ktoré je stále viac komplexné, virtualizované, distribuované a rôznorodé. IBM Control Desk pomáha optimalizovať výkon infraštruktúry a pracovnej sily. Pomáha získať kontrolu nad správou integrity konfigurácií po plánovaných zmenách a neplánovaných incidentoch a problémoch, ku ktorým dochádza v tomto komplexnom IT prostredí. Pomáha zaistiť spojitosť služieb, rýchlosť odozvy a efektivitu správy. Produkt ponúka inovatívnu funkčnosť v rade oblastí oblastí, vrátane:

- jednoduchého a ľahko použiteľného katalógu služieb
- nástrojov na jednoduché hlásenie problémov a požiadaviek na služby
- aplikácií, ktoré umožnia IT personálu byť produktívny a zodpovedný pri stanovení priorít, sledovaní a vyriešení problémov koncových používateľov
- riadenia zmien, konfigurácií, vydaní, incidentov, problémov a aktív v súlade s odporúčaniami rámca ITIL
- automatizácie pracovných postupov a priradených úloh
- integrovanej správy služieb, aktív a konfigurácií
- nástrojov pokročilé analýzy, ktoré ponúkajú prehľad IT prostredia a pomáhajú efektívnejšie spravovať zmeny

Produkt umožňuje vykonávať základnú konfiguráciu systému bez programovania, tak aby sa dalo rýchlo prispôsobiť používateľské rozhranie, dátový model a pracovné postupy potrebám konkrétnej organizácie. IBM Control Desk ukladá množstvo dát o službách - incidenty, problémy, požiadavky na služby, aktíva, konfiguračné položky a ďalšie. To umožňuje vytvoriť plán na zlepšenie služieb alebo plán kvality služieb. Je možné zobraziť trendy hlásení na Incidentoch a konfiguračných položkách, ak chcete identifikovať ktoré aplikácie alebo služby najviac potrebujú aktualizovať.

Hlavné aplikačné moduly, ktoré sú predmetom dodávky, parametrizácie a nasadenia systému IBM Control Desk:

3.2.1.1 Modul Service Desk

Aplikácie z modulu Service Desk sa používajú na správu zákazníckych požiadaviek o pomoc, požiadaviek o informáciu a požiadaviek na služby
Aplikácie z tohto modulu sa primárne používajú na podporu ITIL procesov a funkcií:

- Service Desk
- Incident Management
- Problem Management
- Request fulfillment

V rámci tohto modulu sa spravujú všetky typy ticketov (Service Requesty, Incidenty a Problémy), ktoré sa v aplikácii vyskytujú.

Pre riešenie funkcionality IS SD je ponúkaný nástroj IBM Smart Cloud Control Desk, ktorý je certifikovaný a kompatibilný s IT procesmi, ktoré popisuje rámec ITIL v3. V zmysle požiadavky obstarávateľa uvádzame mapovanie IT procesov na jednotlivé komponenty a moduly v rámci IS SD v nasledujúcej tabuľke:

Proces	Modul
Manažment incidentov	IS SD – Modul Service Desk
Manažment udalostí	IS SD – Modul Service Desk, Modul Integrácie
Manažment prístupov	IS SD – Modul Service Desk
Manažment problémov	IS SD – Modul Service Desk
Manažment riadenia aktív a konfigurácie	IS SD – Modul Infraštruktúra IT
Manažment zmien	IS SD – Modul Zmeny
Manažment vydaní a nasadení	IS SD – Modul Vydania
Manažment kontinuity IT služieb	IS SD – Modul Infraštruktúra IT
Manažment kapacít	IS SD – Modul Infraštruktúra IT
Manažment dostupností	IS SD – Modul Úrovne služieb, Modul Infraštruktúra IT, Modul Integrácie
Manažment úrovne poskytovania služieb	IS SD – Modul Úrovne služieb
Manažment katalógu služieb	IS SD – Modul Úrovne služieb
Finančný manažment pre IT služby	IS SD – Modul Infraštruktúra IT

3.2.1.2 Modul Zmeny

Aplikácie v module Zmeny sa používajú na podporu procesu riadenia zmien. Ten je v systéme primárne podporený aplikáciou Zmeny(Changes), ktorú je možné použiť na naplánovanie, posúdenie a nahlásenie skutočných hodnôt pre implementáciu zmien alebo nasadenie nových, štandardných konfigurácií do existujúcich aktív. Zmeny je tiež možné vytvoriť v iných aplikáciách.

Aplikáciu Zmeny je možné použiť na definovanie, naplánovanie a rozvrhnutie práce vyžadovanej na implementáciu zmeny. Je možné ju tiež použiť na priradenie vlastníka k zmene, kategorizáciu zmeny a aktualizáciu jej stavu, ako sa posúva k dokončeniu. K zmene je možné priradiť iné záznamy, aby ste zjednodušili manažment viacerých podobných záznamov, alebo je možné vytvoriť doplňujúce záznamy priamo zo zmeny

3.2.1.3 Modul Vydania

Aplikácie v module Vydania sa používajú na podporu procesu Manažment vydaní a nasadení (Release and deployment management).

Systém obsahuje aplikáciu Vydania(Releases), v ktorej je možné plánovať, posudzovať a pripravovať veľké dávky zmien v jednej alebo viacerých službách. Záznam o vydaní obsahuje podrobnosti o úlohách, plánovaní a osobách alebo skupinách zahrnutých vo vydaní. Aplikáciu Vydania je možné používať na riadenie vydania autorizovaných verzií alebo konfigurácií komponentov do produkčného prostredia. K príkladom patria veľké alebo kritické zmeny hardvéru, podstatné zmeny softvéru a balenie súvisiacich množín zmien.
Je možné vytvoriť vydanie, ktoré pomôže naplánovať, posúdiť a vykonať prípravu pre veľké dávky zmien. Záznam o vydaní obsahuje podrobnosti o úlohách, plánovaní a osobách alebo skupinách zahrnutých vo vydaní. Aplikácia umožňuje:

- Vytvorenie vydaní - Vydanie určuje informácie o práci, ktorá sa musí vykonať pre aktívum, umiestnenie alebo položku konfigurácie. Je možné pridať pracovné plány alebo pracovné postupy. Je možné tiež zaznamenať denné hodnoty pri postupe práce.
- Hlásenie denných hodnôt pre pracovné príkazy - Ako prebieha práca na schválenom pracovnom príkaze, je možné hlásiť skutočné hodiny pracovníka, použitých materiálov, služieb a nástrojov.
- Nahlásenie doby výpadku pre aktíva - Je možné nahlásiť začiatočný a koncový čas doby výpadku pre aktívum, keď k nemu dôjde.
- Výmena aktív - Je možné vymeniť aktíva priradené k pracovnému príkazu. Akcia výmeny sa použije na pracovný príkaz a všetky aktíva, umiestnenia a položky konfigurácie v jeho dcérskych pracovných príkazoch. Pojem "pracovný príkaz" môže referovať záznam o pracovnom príkaze, zmene, vydaní alebo aktivite.
- Vytvorenie súvisiacich záznamov - Je možné vytvoriť nové záznamy a priradiť ich k vášmu vydaniu. Nové záznamy môžu byť vydania, incidenty, problém, vydania, žiadosti o službu a pracovné príkazy. Súvisiace záznamy je možné zobraziť na záložke Súvisiace záznamy.
- Kategorizácia úloh vo vydaniach klasifikáciami a atribútmi - Proces hľadania a manažovania záznamov možno zjednodušiť kategorizáciou úloh vo vydaniach. Kategorizácia úloh zahŕňa klasifikáciu a tiež pridanie a zmenu atribútov na ďalšie zoskupenie klasifikácie.
- Nastavenie tokov pracovného procesu - Toky pracovného procesu používajú vzťahy medzi pracovnými príkazmi a úlohami na automatizáciu toku zmien stavu. Je možné nastaviť vzťahy medzi pracovnými príkazmi a úlohami, aby sa pri dokončení úlohy mohla iniciovať ďalšia úloha v toku.
- Zmena stavu zoznamu záznamov - V aplikáciách je možné meniť stav viacerých záznamov.

3.2.1.4 Modul Úrovne služieb

Modul Úrovne služieb sa používa na vytváranie a správu SLA dohôd, ktoré dokumentujú záväzky medzi poskytovateľom služieb a zákazníkmi. Modul sa taktitež používa na vytváranie a správu katalógu služieb.

Proces SLM je v systéme primárne podporený aplikáciou Zmluvy o úrovni služieb (Service Level Agreements), ktorá umožňuje vytváranie a manažovanie zmlúv o úrovni služieb. Zmluvy o úrovni služieb dokumentujú záväzky medzi poskytovateľmi služieb a zákazníkmi. Služby sa skladajú z úloh, ktoré poskytovatelia služieb vykonávajú na splnenie potrieb zákazníka. Záväzky sú zodpovednosti, ktoré musia poskytovatelia služieb dodržiavať na splnenie zmlúv o úrovni služieb.
Pri vytvorení zmluvy o úrovni služieb, je možné vykonať tieto funkcie:

- Hodnotiť zmluvy o úrovni služieb podľa priority, ktorá určuje, ktorá zmluva o úrovni služieb sa použije
- Nastaviť začiatočný dátum platnosti, koncový dátum a dátum posúdenia pre zmluvu o úrovni služieb, čo je možné použiť na riadenie procesu pracovného toku
- Priradiť zmluvy k zmluve o úrovni služieb
- Priradiť súvisiace zmluvy o úrovni služieb k aktuálnej zmluve o úrovni služieb
- Priradiť aktíva a umiestnenia k zmluve o úrovni služieb
- Vytvoriť kľúčové indikátory výkonu alebo metriky pre zmluvu o úrovni služieb
- Vytvoriť eskaláciu na podporu záväzkov v zmluve o úrovni služieb

Používatelia systému SD môžu použiť platné zmluvy o úrovni služieb v rámci záznamov z iných aplikácií, napríklad v Incidentoch, Problémoch, Zmenách. Aplikácia Zmluvy o úrovni služieb je úzko previazaná s funkciou eskalácií, ktoré je možné použiť na manažovanie a kontrolu plnenia záväzkov v zmluve o úrovni služieb.

3.2.1.5 Modul Infraštruktúra IT

Aplikácie v module Infraštruktúra IT umožňujú správu konfiguračných položiek v IT prostredí. Zaisťujú logický model infraštruktúry IT tým, že pomáhajú identifikovať, riadiť, spravovať a overiť verzie všetkých konfiguračných položiek, ich atribútov a relácií v prostredí. Modul Infraštruktúra IT poskytuje nástroje na definovanie a správu konfiguračnej databázy (CMDB), jej jednoduché prehliadanie a vizualizáciu.

Hlavnú aplikáciu, Položky konfigurácie je možné použiť na definovanie, vytváranie a manažovanie vzťahov medzi položkami konfigurácie podľa pravidiel vzťahov, ktoré sa definujú v aplikácii Vzťahy. Položka konfigurácie je ľubovoľný komponent štruktúry informačných technológií, ktorý je riadený manažmentom konfigurácií. V

aplikácii Položky konfigurácie je možné manažovať kolekcie položiek konfigurácií a vytvárať žiadosti o službu, incidenty, problémy, pracovné príkazy, zmeny a vydania pre položku konfigurácie.

3.2.1.6 Modul Aktíva

Modul Aktíva obsahuje aplikácie, ktoré sú navrhnúte na správu vlastnených alebo prenajatých aktív, od nákupu, po prevzatie, a od začiatku do konca životného cyklu aktíva.

V rámci tohto modulu je hlavná aplikácia Aktíva, ktorá sa používa na vytváranie a ukladanie aktív a súvisiacich informácií, ako sú umiestnenie, dodávateľ, stav a náklady na údržbu pre každé aktívum. Aplikácia umôžňuje vytvoriť hierarchiu aktív ako usporiadanie budov, oddelení, aktív a podradených aktív. Hierarchia aktív poskytuje pohodlný spôsob navršovania nákladov na údržbu, aby bolo možné kedykoľvek skontrolovať akumulované náklady na ľubovoľnej úrovni.

3.2.1.7 Modul Konfigurácia systému

Modul Konfigurácia systému obsahuje podmoduly Konfigurácia platformy a modul Migrácia.

Aplikácie z modulu Konfigurácia platformy sa používajú na konfiguráciu parametrov systému, ktoré majú dopad na celý systém. V rámci tohto modulu je možné okrem iného:

- meniť nastavenia systémovej konfigurácie,
- nastavovať rôzne úrovne logovania aplikácie,
- pridávať alebo meniť kódové polia,
- pridávať alebo meniť atribúty a vzťahy jednotlivých business objektov,
- pridávať alebo upravovať jednotlivé aplikácie,
- pridávať alebo meniť workflowy,
- pridávať alebo meniť opakujúce sa úlohy (cron tasky),
- pridávať alebo meniť štandardné notifikačné šablóny

Aplikácie v module Migrácia sa používajú na presúvanie obsahu a konfiguráci z jedného prostredia do druhého (napr. nasadzovanie nových/upravených biznis procesov, z testovacieho prostredia do produkčného).

3.2.1.8 Modul Integrácie

Modul Integrácie obsahuje sadu aplikácií, ktoré umožňujú integrovať systém s inými aplikáciami používanými v organizácii. Kľúčové súčasti integračného frameworku:

- Preddefinovaný obsah, ktorý pomáha urýchliť proces implementácie integračných použiadaviek. Tento obsah je súhrnnou sadou výstupných (kanály) a vstupných (služby) integračných rozhraní, ktoré sú k dispozícii pre okamžité použitie.
- Aplikácie, ktoré slúžia na konfiguráciu, preddefinovanie a vytvorenie nových integračných rozhraní.
- Aplikácie, ktoré zjednodušujú prispôsobenie preddefinovaného obsahu použitím pravidiel, JAVA tried a XSLT transformácií.

Modul Integrácie podporuje viacero komunikačných režimov, vrátane:

- webových služieb,
- HTTP,
- JMS (Java Message Service),
- rozhrania databázových tabulie,
- XML/ jednoduchých textových súborov,
- spracovávania odchádzajúcich a prichádzajúcich správ,
- podpory pre klastrované prostredia, ktoré znižujú výpadky systému, zvyšujú dostupnosť systému a vylepšujú výkon systému,

- podpory pre integrácie v rámci používateľského rozhrania, vrátane kontextového spúštania externých aplikácií,
- podpory pre Operational Management Products (OMPs),
- podpory pre hromadný export dát pomocou používateľského SQL príkazu,
- podpory pre hromadný import súborov XML alebo jednoduchých textových súborov,
- dynamického generovania XML schém pre všetky artefakty integrácie (kanály a služby)
- dynamického generovania webových služieb kompatibilných s Web Services Interoperability (WS-I), vrátane Web Service Definition Language (WSDL),

IS Service Desk štandardne podporuje zasielanie email notifikácií v plain-text aj HTML formáte. Zároveň je možné prostredníctvom Modulu Integrácie pridať nové spôsoby a formáty notifikácií podľa potreby ako napr.:

- SMS,
- Jabber,
- sociálne siete.

3.2.2 Modul IBM Tivoli Common Reporting

je reportovací nástroj umožňujúci posielanie pravidelných reportov aj reportov prehľadne konfigurovateľných podľa individuálnych požiadaviek. Obsahuje nástroje na:

- vytváranie a úpravu reportov
- podporu pre ad-hoc (jednorazové) a pravidelné reporty
- manuálne a automatizované generovanie reportov
- automatizovanú distribúciu reportov prostredníctvom emailu
- možnosť exportu reportov minimálne do formátov PDF, XLS
- vytváranie nových a úpravu existujúcich reportov v používateľsky prívetivom prostredí

3.3 IS SEC & MON

Informačná bezpečnosť je jedným zo základných kritérií budovania IS ako IS VS, ktorý taktiež spracováva osobné údaje musí plniť ďalšie požiadavky v súlade s aktuálne platnou legislatívou v čase podpisu zmluvy.

Keďže IS bude tvorený vo významnej miere existujúcimi prvkami, súčasťou bezpečnostnej architektúry sú aj existujúce bezpečnostné prvky. Implementácia nových bezpečnostných komponentov je závislá od miery realizovateľnosti na existujúcich prvkoch.

Bezpečnostná architektúra bude obsahovať prvky tvoriace prepojený celok chrániaci systém do hĺbky a vo viacerých vrstvách v celom jeho životnom cykle.

Úlohou bezpečnosti je stanoviť požiadavky a verifikovať splnenie formou špecializovaných bezpečnostných testov a revízie dizajnu.

3.3.1 SmartCloud

3.3.2 Modul Centrálny monitorovací systém (CMS).

Centrálny monitorovací systém bude monitorovať všetky IT prostredia NZIS a zabezpečovať proaktívnu podporu pre IT služby poskytované v rámci NZIS. V monitoringu budú zahrnuté nasledovné oblasti IT infraštruktúry:

- Monitoring hardvéru
- Monitoring sieťových a bezpečnostných komponentov
- Monitoring operačných systémov a platformových produktov
- Monitoring aplikácií a biznis služieb

Centrálny monitorovací systém bude zabezpečovať:

- Aktuálny stav IT prostredia a služieb
- Identifikáciu primárnej príčiny výpadku služby
- Predikciu potencionálnych problémov pred ich samotným výskytom
- Z dôvodu zabezpečenia vysokej dostupnosti a variability riešenia, ktorého možnosti kompatibility z inými monitorovacími nástrojmi a možnosťami rozširovania nie sú obmedzené, bol ako centrálny monitorovací nástroj (tzv. umbrella monitoring) zvolený nástroj IBM Tivoli Enterprise Monitoring.

Centrálny monitorovací systém je navrhnutý ako nástroj pre spracovanie a vyhodnotenie dát vlastnými prostriedkami, štandardnými monitorovacími protokolmi a tiež umožňujúci zber monitorovaných údajov z iných monitorovacích nástrojov.

Prostredie je navrhnuté ako robustné riešenie s vysokou dostupnosťou a bude zabezpečovať všetky požadované funkcionality:

- Možnosť spracovania výstupov aj z iných monitorovacích nástrojov zastrešených jedným monitoring nástrojom (tzv. umbrella monitoring)
- Možnosť vyhodnotenia modelov služieb vytvorených na základe informácií z centrálnej konfiguračnej databázy CMDB evidovanej v rámci SD systému
- Vyhodnotenie modelov služieb bude prebiehať na základe informácií z dostupných monitoring nástrojov
- Riešenie bude zabezpečovať realizáciu monitoringu služieb z pohľadu koncového používateľa
- Riešenie bude poskytovať prehľadné rozhranie aj s vizualizáciou aktuálneho stavu služieb a rýchle vyhľadanie príčin výpadkov (root cause)
- V prípade výpadku IT zdroja zachytenom monitorovacími nástrojmi bude identifikovaný dopad na poskytované služby (impact analysis)
- Centrálny monitorovací systém bude previazaný s procesným nástrojom na automatické vytváranie incidentov
- Možnosť plánovania výpadkov infraštruktúry a služieb
- Možnosť prístupu k monitorovacím nástrojom s využitím „Single Sing On“ cez externú autentifikáciu v AD/LDAP
- Riešenie podporuje štandardné rozhranie pre integráciu s inými nástrojmi (SNMP, WebServices)
- Riešenie priamo podporuje integráciu s nástrojom Microsoft SCOM 2012 metódou „out of the box“
- Riešenie umožňuje príjem udalostí cez SNMP, Syslog, JMX, PerfMon, WMI z rôznych zariadení a systémov
- Súčasťou monitoringu je aj dohľad nad databázami MSSQL, Oracle, MySQL a iné
- Súčasťou monitoringu je aj dohľad nad aplikáciami na heterogénnych OS platformách.
- Systém umožňuje tvorbu vlastných monitorovacích postupov pre priamo nepodporované aplikácie
- Podpora funkcionality „network discovery“
- Vizualizácia sieťovej topológie a „topology based root cause analysis“
- Sieťový monitoring podporuje OOTB s podporou štandardných protokolov a zariadení (SNMP verzie 1,2,3)

Centrálny monitorovací systém využíva na spracovanie reportov robustný nástroj, ktorý umožňuje rýchle vyhodnotenie dát aj v kritických situáciách.
Centrálny monitorovací systém je navrhnutý s vysokou dostupnosťou (HA) a schopnosťou monitorovania a spracovania veľkého počtu objektov (rádovo v tisíckach). V prípade požiadavky je možné Centrálny monitorovací systém rozširovať pridávaním ďalších R-TEMS (IBM Remote Tivoli Enterprise Monitoring) na monitorovanie ďalšieho nového prostredia NZIS. CMS je plne škálovateľný a rozširovateľky podľa aktuálnych potrieb.

3.3.2.1 Modul IBM Tivoli Netcool Operations Insight (OMNIbus)

Ako centrálny monitorovací nástroj bude použitý produkt IBM Tivoli Netcool/OMNIbus, ktorý takmer v reálnom čase menežuje správu udalostí v celej infraštruktúre dátového centra. Modul poskytuje plnú správu a automatizáciu na uľahčenie dostupnosti služieb a aplikácií. Umožňuje operátorom spúšťať automatizované scripty na riešenie opakujúcich a predvídateľných problémov. Umožňuje integrovať iné nástroje na monitorovanie. Napríklad nástroj Microsoft SCOM 2012 s ktorým bude priamo integrovaný.

3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring

Produkt
Ako monitorovací nástroj bude použitý produkt **IBM SmartCloud APM** a jeho nosnoným modulom **Tivoli Enterprise Monitoring Server (TEMS)**. Ktorý bude monitorovať virtuálne prostredie a operačné systémy okrem Windows, ktorý bude monitorovaný prostredníctvom nástroja Microsoft SCOM 2012. Monitorovanie operačných systémov je podporované prostredníctvom inštalovaného IBM Tivoli Monitoring Agenta operačné systémy: AIX, HP-UX, Linux, Solaris a Windows.

IBM Remote Tivoli Enterprise Monitoring (R-TEMS) je monitoring nástroj pre logicky oddelené prostredie, ktorý zabezpečuje zber údajov rovnako ako TEMS a následne posiela údaje do centrálneho monitorovacieho nástroja OMNIBUS Pomocou tohto modulu je možné škálovať monitorovacie prostredia v logicky oddelených sieťach. Inštalovaním modulu R-TEMS je aj rozloženie záťaže medzi centrálny a remote monitorovacie systémy. Aj v prípade vzniku poruchy, ktorého dôvodom bude vznik veľkého počtu zasielaných informacií monitorovaciemu nástroju, nedôjde k preťaženiu centrálneho monitorovacieho systému,

3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP)

Administrátori budú mať k dispozícií **IBM Tivoli Integrated Portal (TIP)**, ktorý zabezpečuje administráciu **ITNM (**monitoring siete**), administráciu TBSM** (monitoring služieb**)**.

Operátori budú mať k dispozícií prostredníctvom nástroja **IBM JAZZ for Service Management** zjednodušený a vizuálne prehľadný nástroj na kontrolu stavu poskytovaných služieb so zobrazením dopadu na prevádzku v prípade poruchy s možnosťou vytvárania reportov.

3.3.2.4 Modul IBM Tivoli Common Reporting (TCR)

je nástroj ktorý vytvára pravidelné reporty, ktoré sú prehľadne konfigurovateľné podľa individuálnych požiadaviek. Následne ich môže zasielať. Je možné pomocou tohto nástroja zobrazovať históriu z nazbieraných údajov. Súčasne je umožňuje zobrazovanie trendov využívania systémov (napr. zobrazenia CPU, Memory, obsadenosť diskov). Následne je možné identifikovať ktoré systémy sú ako využívané.

3.3.2.5 Modul IBM Tivoli Network Manager (ITNM)

zabezpečuje monitoring a automaticky vyhľadáva zariadenia pripojené do siete na sieťových vrstvách L2 a L3. Vie zabezpečiť aj monitoring optických prepojov a bezdrôtových sietí 2G/3G. Tento modul dokáže aj v roziahlých sieťach identifikovať problém a príčinu vzniku poruchy prípadne stratu spojenia medzi zariadeniami alebo lokalitami. Zabezpečuje aj koreláciu udalostí, identifikáciu zdroja problému s vizuálnym zobrazením siete v reálnom čase.

3.3.2.6 Modul IBM Tivoli Business Service Manager (TBSM)

zabezpečuje real time analýzu a vyhodnotenie stavu služieb podľa modelu služby odrážajúceho závislosti medzi jej jednotlivými komponentami. Rýchlo vyhodnocuje informácie z rôznych zdrojov a umožňuje identifikovať príčinu problému v súlade s obchodnými požiadavkami a plnením SLA. Súčasťou modulu je aj vizuálne

zobrazenie, ktoré je plne konfigurovateľné. Je možné vytvárať vizuálne widgety s prístupom k dátam ako sú rôzne meradlá, tabuľky a zoznamy. Umožňuje vytvárať aj vlastné dashboardy.

Modul je prepojený s CMDB a modely služieb sú s nej priamo prenášané.

3.3.3 Modul Centrálny Backup

IS Centrálny Backup je sústava aplikačných komponentov ktoré vykonávaju zálohovanie a obnovu dát.
Pojem "zálohovanie" znamená proces vytvárania kópií za účelom obnovy originálu, v prípade ak dôjde k čiastočnému poškodeniu alebo úplnému zničeniu originálu.
Zálohovanie dát je teda procesom vytvárania kópií dát, za účelom obnovy pôvodných dát v prípade ak dôjde k užívateľskému alebo aplikačnému znehodnoteniu dát, alebo k ich úplnému zničeniu.
Pojem "obnova" znamená proces kompletnej rekonštrukcie originálu s pomocou zálohy.
Obnova dát je teda procesom kompletnej rekonštrukcie dát do takého stavu, v akom boli v dobe vytvárania zálohy. Obnova dát je komplexný proces, ktorý pozostáva z niekoľkých krokov:

- Obnova hardvéru - zabezpečenie totožného alebo ekvivalentného (kompatibilného) hardvéru
- Serverový hardvér
- Úložný priestor
- Komunikačná sieťová infraštruktúra pre dáta a storage
- Obnova virtualizačnej platformy (v prípade že servery pôvodné dáta boli spracúvané vo virtuálnych serveroch)
- Obnova prostredia pre beh aplikácie a spracovanie dát
- Operačný systém, vrátane patchov, driverov, nastavení a hardeningu
- Platformový produkt (aplikácia alebo databáza), vrátane patchov, nastavení a hardeningu
- Obnova samotných dát

Popis komponentov centralizovaného zálohovacieho riešenia a komunikačných tokov:

- Backup server - centrálny server pre riadenie záloh
    - Má nainštalovaný a bežiaci softvér, ktorý riadi proces zálohovania a obnovy dát - ich časovanie, vydávanie manažovacích príkazov (zoznam zálohovaných dát, úroveň záloh, retenčná doba, umiestnenie na Backup Destination)
    - Monitoruje a riadi priebeh zálohovania a obnovy a monitoruje a úspešnosť/neúspešnosť záloh
    - Vedie databázu o zálohovaných systémoch (serveroch) a zdrojoch dát ktoré obsahujú
    - Vedie databázu o zálohovacích cieľoch - úložiskách záložných kópií dát, zozname, stave a úrovni naplnenia médií (diskov a/alebo pások)
    - Vedie databázu o zálohách - zoznam záloh, obsah záloh, dobu platnosti a retencie záloh, úspešnosť/neúspešnosť záloh
    - Vedie databázu o obnovách dát
    - Riadi proces skartácie neúspešných a/alebo neplatných a/alebo expirovaných záloh
- Backup source - zdroj dát - spravidla server na ktorom sa spracúvajú alebo sú uložené dáta
- Akceptuje a vykonáva manažovacie príkazy od Backup servera
- Číta originálne dáta, pripravuje dáta na prenos (šiftuje a/alebo komprimuje a/alebo deduplikuje) a posiela dáta na určený Backup Destination
- Backup destination - úložisko, kde sú na určenú dobu ukladané kópie pôvodných dát, spravidla v inom (blokovom, komprimovanom alebo šifrovanom) formáte ako sú originálne dáta
    - Spravuje úložné zariadenia (vlastné alebo externé disky a/alebo páskové knižnice a mechaniky)
    - Spravuje úložné dátové médiá (filesystemy a/alebo dátové súbory v špecializovanom formáte a/alebo páskové médiá)
    - Akceptuje a vykonáva riadiace povely od Backup servera
    - Prijíma dáta od zdrojov dát
    - Pripravuje dáta na uloženie (šifruje a/alebo komprimuje a/alebo deduplikuje a/alebo prekladá dáta do formátu vhodného na ukladanie)
    - Ukladá dáta na dátové médiá
    - Vykonáva skartáciu záloh podľa príkazov Backup servera
- Management traffic
    - Interaktívna sieťová komunikácia medzi Backup serverom a Backup source a/alebo Backup

serverom a Backup destination
    - Typicky je táto komunikácia šifrovaná
    - Typicky sa jedná o komunikáciu ktorá nie je citlivá na prenosovú rýchlosť ani latenciu
- Data Traffic
    - Spravidla jednosmerná sieťová komunikácia z Backup source na Backup destination
    - Typicky je táto komunikácia šifrovaná
    - Typicky sa jedná o prenos veľkých objemov dát. Táto komunikácia je teda citlivá na prenosovú rýchlosť. Nie je však bezprostredne citlivá na latenciu

3.3.4 Monitorovanie bezpečnosti

Monitorovanie bezpečnosti komponentov, ktoré budú umiestnené v blokoch ESZ bude realizované existujúcim dedikovaným bezpečnostným dohľadovým centrom (SOC) zriadeným v NCZI (u správcu a prevádzkovatela NZIS).

Pre monitorovanie bezpečnosti bude použitý SIM nástroj netForensics SIM One, ktorý má distribuovanú architektúru a predstavuje centralizované riešenie monitorovania bezpečnosti. Skladá sa z centrálnej časti, ktorá sa nachádza v SOC a obsahuje databázu, nástroje na zbieranie informácií, centrálny systém na koreláciu a spracovanie informácií a webový prezentačný server.

Do technologického komponentu pre monitorovanie bude realizovaný zber relevantných zdrojov informácií:

- Bezpečnostné sieťové prvky
- Sieťové prvky
- OS na serverch
- Bezpečnostné komponenty na serveroch
- Databázy

Zbierané hlásenia budú transformované do jednotnej platformovo nezávislej formy a umiestnené v centrálnej databáze pre potreby bezpečnostnej analýzy. Zber sa bude vykonávať near-to-real-time, čím bude minimalizované riziko spätnej modifikácie hlásení na zdrojovom komponente predtým, ako sú odoslané do SIM.

SIM pre svoju správnu funkčnosť a realizovateľnosť monitorovania predpokladá jednotný synchronizovaný čas aj na nových monitorovaných komponentoch.

3.3.5 Modul Endpoint Antivirus

ESET Antivirus predstavuje nový prístup k integrovanej počítačovej bezpečnosti. Výsledkom je inteligentný systém, ktorý je neustále v pohotovosti pred útokmi, či škodlivým softvérom, ktoré ohrozujú váš počítač.

ESET NOD32 Antivirus je komplexné bezpečnostné riešenie a je výsledkom dlhodobého úsilia spojiť maximálnu bezpečnosť s minimálnou záťažou systému. Tieto pokročilé technológie, založené na umelej inteligencii, sú schopné proaktívne eliminovať preniknutie vírusov, spyware, trójskych koní, červov, adware, rootkitov a ďalších internetových útokov šírených bez toho, aby brzdili výkon systému alebo spôsobili nefunkčnosť operačného systému počítača.

3.3.5.1 Endpoint Security

Proaktívne deteguje a lieči známe i neznáme vírusy, červy, trojany a rootkity. Pokročilá heuristická technológia odhaľuje dokonca aj doteraz neznáme hrozby a neutralizuje ich skôr, než môžu spôsobiť škodu vo vašom počítači. Ochrana prístupu na web a Anti-Phishing spočíva hlavne v monitorovaní komunikácie prehliadačov internetových stránok so servermi (vrátane SSL).

Antivírus a Antispyware

Eliminuje rôzne typy hrozieb.

Anti-Phishing

Chráni pred falošnými stránkami, ktoré sa snažia ukradnúť citlivé informácie.

Podpora virtualizácie

Ukladá metadáta z už skontrolovaných súborov do virtuálneho prostredia a urýchľuje tak nasledujúce skenovanie.

Exploit Blocker

Posilňuje bezpečnosť aplikácií ako napríklad prehliadačov, PDF čítačiek a iných.

Pokročilá kontrola pamäte

Sleduje správanie podozrivých procesov a kontroluje ich po ich rozbalení v pamäti.

Štít zraniteľností

Detekcia zraniteľností na často používaných protokoloch ako SMB, RPC a RDP.

Ochrana pred botnetmi

Chráni pred botnet malvérom a spustením spamových a sieťových útokov z vášho zariadenia.

Webová kontrola

Obmedzuje prístup na stránky podľa kategórií (herné, sociálne siete, obchody atď.).

Obojsmerný firewall

Chráni pred neoprávneným prístupom do firemnej siete a k dátam.

Klientský antispam

Efektívne filtruje spam a vyhľadáva malvér v prichádzajúcich e-mailoch.

Host-based Intrusion Prevention (HIPS)

Umožňuje definovať pravidlá pre procesy, aplikácie a súbory.

Inštalačná služba

Počas inštalácie riešenia vyhľadá iné bezpečnostné riešenia a odinštaluje ich.

3.3.5.2 File Security

Antivírus a Antispyware

Eliminuje rôzne typy hrozieb.

Exploit Blocker

Posilňuje bezpečnosť aplikácií ako napríklad prehliadačov, PDF čítačiek a iných.

Pokročilá kontrola pamäte

Sleduje správanie podozrivých procesov a kontroluje ich po ich rozbalení v pamäti.

Podpora virtualizácie

Ukladá metadáta z už skontrolovaných súborov do virtuálneho prostredia a urýchľuje tak nasledujúce skenovanie.

Natívna podpora klastrovania

Spojte viaceré zväzky ESET File Security do jedného klastra a riaďte ich ako jeden.

Kontrola úložiska

Spustite on-demand skenovanie pripojených Network Attached Storage (NAS) zariadení.

Windows Management

Instrumentation (WMI) Provider Monitoruje hlavné funkcie ESET File Security cez rámec WMI. Umožňuje tak integrovať programy tretích strán a SIEM programy.

Modulárna inštalácia

Vyberte si, ktoré komponenty sa majú inštalovať, a zaistite lepšiu optimalizáciu. Nízke systémové požiadavky Viac systémových zdrojov pre programy, ktoré potrebujete.

3.3.5.3 ESET Remote Administrator

Vzdialené riadenie

Riaďte servery, koncové zariadenia, smartfóny a virtuálne zariadenia – všetky z jednej konzoly.

ESET Remote Administrator Server

Stará sa o komunikáciu s agentmi, zbiera a ukladá aplikačné dáta do databázy.

Nezávislý agent

Všetky úlohy, nastavenia a udalosti sú spúšťané nezávislým agentom priamo na zariadení. A to aj bez pripojenia na ESET Remote Administrator.

Webová konzola

Umožňuje spravovanie sieťovej bezpečnosti odkiaľkoľvek cez webové rozhranie s možnosťami

prekliknutia.

ESET Remote Administrator Proxy

Zbiera a preposiela agregované dáta zo vzdialených lokácií do hlavného servera, bez potreby serverovej inštalácie.

Rogue Detection Sensor

Vyhľadáva v sieti nechránené a neriadené zariadenia, ktoré si vyžadujú pozornosť.

Multiplatformová podpora

ESET Remote Administrator je kompatibilný so zariadeniami s operačnými systémami Windows aj Linux, alebo s tými, ktoré vystupujú ako virtuálne zariadenia.

Endpoint nasadenie

Všetky inštalačné súbory sú k dsipozícii na serveroch ESET a podporujú caching na web-proxy úrovni a eliminujú tak možnosť duplicitného stiahnutia vo vašej firemnej sieti.

Kontrola prístupových práv

Vytvorte viacero používateľských účtov, každý s nastaviteľnými privilégiami.

Zabezpečená peer komunikácia

Využíva Transport Layer Security (TLS) 1.0 štandard a používa vlastné certifikáty na peer identifikáciu.

Vzdialené riadenie

Riaďte servery, koncové zariadenia, smartfóny a virtuálne zariadenia – všetky z jednej konzoly.

ESET Remote Administrator Server

Stará sa o komunikáciu s agentmi, zbiera a ukladá aplikačné dáta do databázy.

Nezávislý agent

Všetky úlohy, nastavenia a udalosti sú spúšťané nezávislým agentom priamo na zariadení. A to aj bez pripojenia na ESET Remote Administrator.

Webová konzola

Umožňuje spravovanie sieťovej bezpečnosti odkiaľkoľvek cez webové rozhranie s možnosťami prekliknutia.

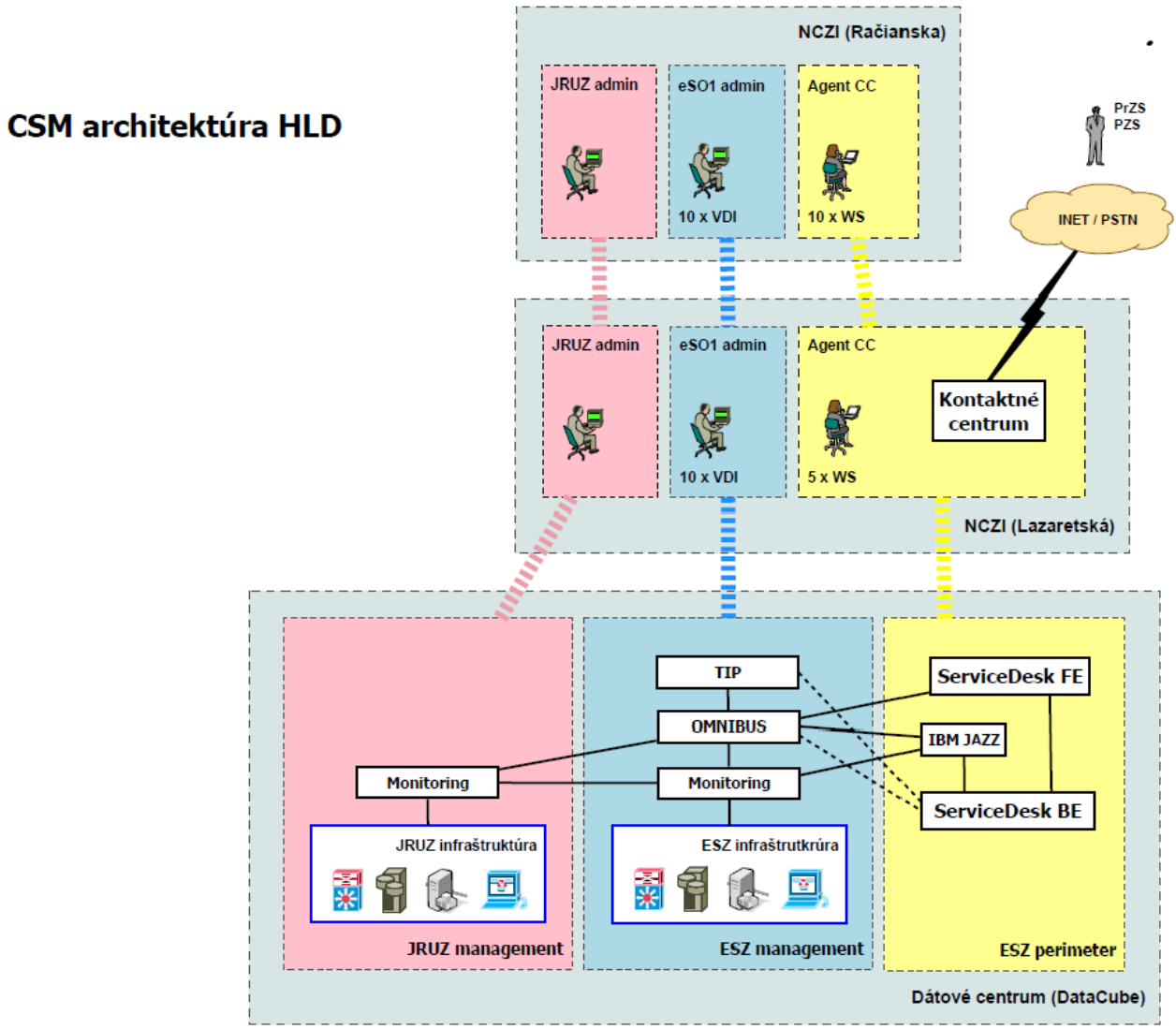
ESET Remote Administrator Proxy

Zbiera a preposiela agregované dáta zo vzdialených lokácií do hlavného servera, bez potreby serverovej inštalácie.

Rogue Detection Sensor

Vyhľadáva v sieti nechránené a neriadené zariadenia, ktoré si vyžadujú pozornosť.

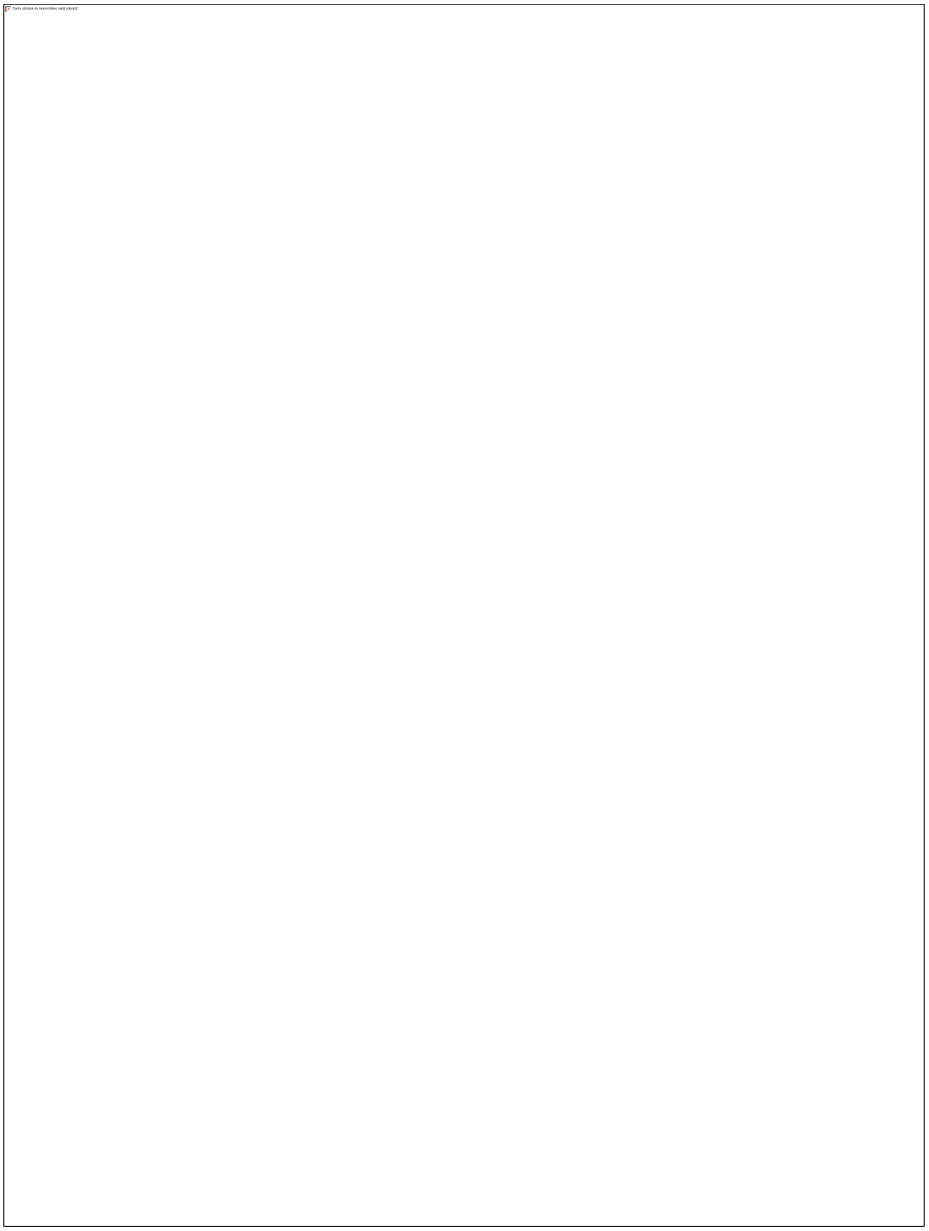
3.4 HL Architektura zón



Návrh budovania jednotlivých zón vychádza z konceptu segregovaných rozprestretých zón. Koncept je tobrazený na obrázku vyššie.

Sú oddelené jednotlivé skupiny užívateľov. Zónovanie plne korešponduje s geografickým členením jednotlivých zón a reálne vyvhádza zo spôsobu budovania komunikačných trás. Tento spôsob prepojenia jednotlivých lokalít sa prejavý aj v koncepte budovania DRP.

3.5 High level popis bezpecnostneho konceptu



Produkčná infraštruktúra service desku a monitoringu bude vhodne integrovaná do produkčného prostredia ESZ vrátane sieťovej a bezpečnostnej infraštruktúry tak, aby sa neznížila úroveň zabezpečenia ESZ.
Systém ServiceDesk (SD) bude fyzicky umiestnený v produkčnom prostredí ESZ, v perimeter bloku nasledovne:

- aplikačný komponent SD bude umiestnený vo frontend zóne bloku perimetra v dedikovanej bezpečnostnej zóne,
- backend SD bude umiestnený v backend zóne bloku perimetra v dedikovanej bezpečnostnej zóne,
- komponenty systému SD budú umiestnené na dedikovanom virtualizačnom serveri, oddelenom fyzicky od produkčných serverov ESZ.

Pripojenie na sieťovú infraštruktúru bude realizované v prístupovej vrstve sieťovej infraštruktúry perimeter bloku s využitím dopĺňaných 10Gb modulov a rozšírením počtu licencií FC prepínača Cisco Nexus 5548

Systém Monitoring ESZ (Centrálny monitorovací systém, CMS) bude fyzicky umiestnený v produkčnom prostredí ESZ, v blokoch EZS spôsobom:

- frontend server, určený pre prístup agentov Kontakntného centra, bude vo frontend zóne perimeter bloku ESZ v dedikovanej bezpečnostnej zóne, na virtuálnom serveri ktorý zdieľa fyzický virtualizačný server s

virtuálnymi servermi ServiceDesk,
- backend bude umiestnený v manažmentovej sieti v dedikovanej bezpečnostnej zóne na dedikovanom virtualizačnom serveri, pričom jeho pripojenie budú realizovať dedikované prepínače Cisco Catalyst 3750X a oddelenie a ochranu zabezpečí nový vysokodostupný firewall Cisco ASA 5515X, určený pre ochranu systému Monitoringu ESZ, ktorý bude súčasťou dodávky riešenia.

Systém CallCentrum (Kontaktné centrum, KC) bude fyzicky umiestnené v priestoroch NCZI mimo produkčného prostredia ESZ vo vlastnej bezpečnostnej zóne.
Prístup ľudských aktérov do riešenia:

- agenti KC, predstavujúci I.úroveň podpory budú pristupovať (označené zelenou farbou):
    - k systému KC prostredníctvom infraštruktúry NCZI (správcu a prevádzkovateľa NZIS), pričom pri dátových tokoch ktoré sú mimo perimetra FOB NCZI bude zabezpečená ochrana dôvernosti a integrity a vzájomná autentizácia bodov zabezpečujúcich túto komunikáciu pomocou IPsec VPN. Ochrana dátových tokov mimo perimetra FOB NCZI je predmetom riešenia.
    - k systémom SD a CMS pomocou remote access VPN z pracovnej stanice operátora, ukončovanej prostriedkami ESZ, pričom prenosová cesta bude zabezpečovaná z priestorov:
- Lazaretská – pomocou existujúceho prepojenia so systémom ESZ ktoré zabezpečuje ochranu dôvernosti, integrity a vzájomnú autentizáciu bodov zabezpečujúcich túto komunikáciu:
- Račianska – pomocou prepojenia s NCZI Lazaretská vytvoreného ako súčasť dodávaného riešenia a následne pomocou prepoja NCZI Lazaretská s ESZ. Prepojenia zabezpečia ochranu dôvernosti a integrity a vzájomnú autentizáciu bodov zabezpečujúcich túto komunikáciu.
- Využívané prepoje:
    - Cisco ASA 5515X (dedikovaný pár FW, určený pre ochranu používateľských sietí, dodaný v rámci rozšírenia NCZI Račianska) - Cisco ASR1002 (NCZI Lazaretská) - nový prepoj v rámci riešenia
    - Cisco ASR1002 (NCZI Lazaretská) - Cisco ASR1002 (ESZ DC) - existujúci prepoj v rámci ESZ
- administrátori a iné osoby predstavujúce II.úroveň podpory pristupujú na SD a CMS prostredníctvom existujúcej manažmentovej siete ESZ pri dodržaní rovnakých bezpečnostných opatrení ako sú definované projektom ESZ (označené modrou farbou).
- Využívané prepoje:
    - Cisco ASA 5515X (dedikovaný pár FW, určený pre ochranu sietí určených pre administrátorov ESZ, dodaný v rámci rozšírenia NCZI Račianska) - Cisco ASR1002 (NCZI Lazaretská) - nový prepoj v rámci riešenia
    - Cisco ASR1002 (NCZI Lazaretská) - Cisco ASR1002 (ESZ DC) - existujúci prepoj v rámci ESZ

Prepojenie produkčného prostredia projektu JRUZ s CMS:

- prepojenie bude vytvorené striktne za účelom monitorovania infraštruktúry a systémov prostredia projektu JRUZ,
- uvedené prepojenie bude kontrolované dodávaným dedikovaným vysokodostupným firewallom Cisco ASA 5515X, určeným pre ochranu systému Monitoringu ESZ, ktorý bude začlenený do infraštruktúry manažmentovej siete ESZ,
- Uvedené prepojenie umožní iba komunikáciu potrebnú pre správnu a efektívnu funkčnosť monitorovania JRUZ systémom CSM.

Východiská riešenia:

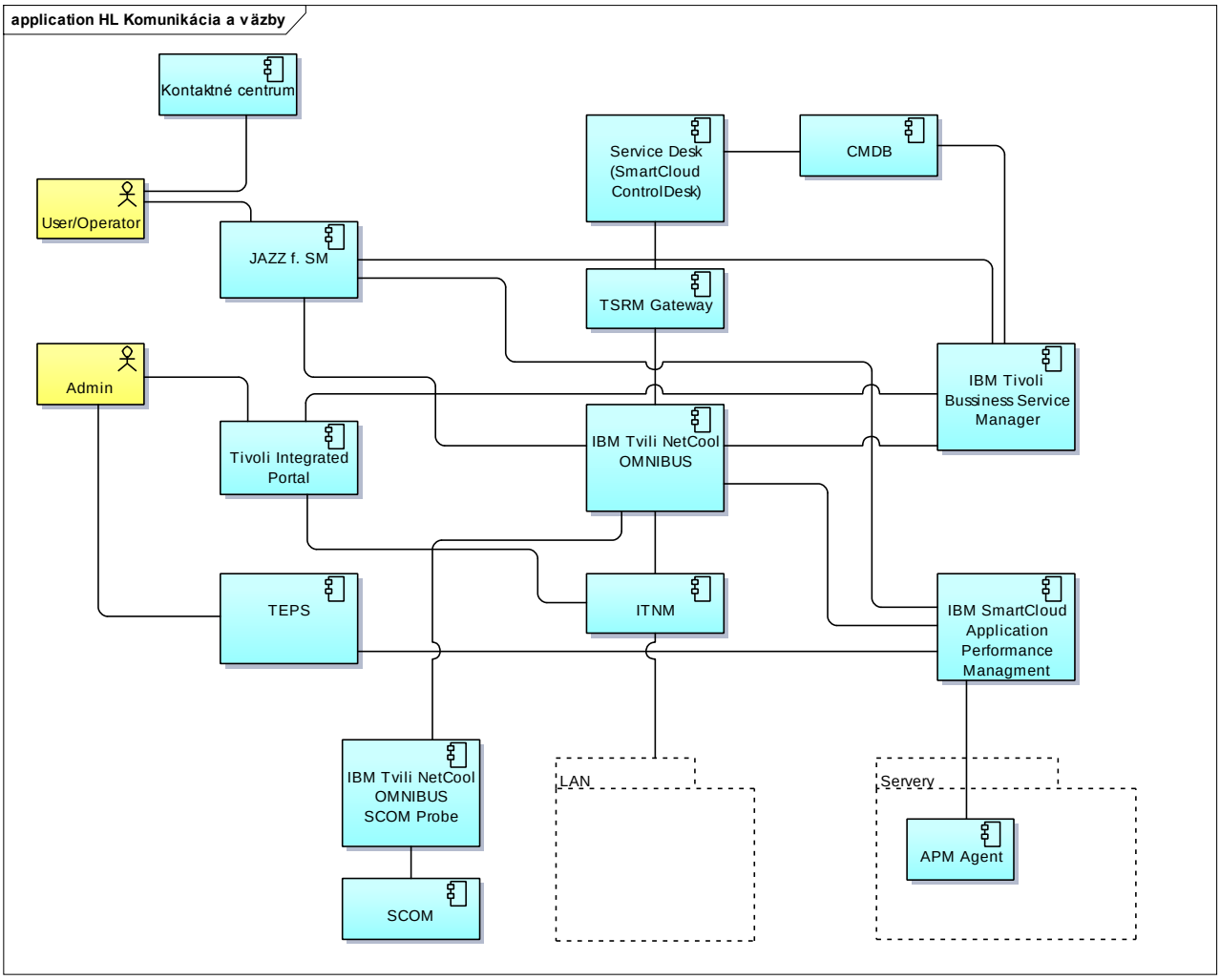
1. Systémy SD ani CMS nebudú obsahovať citlivé, údaje ani neumožnia získať prístup k citlivým údajom ESZ.
2. Na strane NCZI správcu a prevádzkovateľa NZIS budú vykonané opatrenia pre izoláciu sieťových segmentov, obsahujúcich prvky riešenia, od ostatných častí siete NCZI a ochranu komponentov pri prístupe z vnútra siete NCZI ako aj pri prístupe zvonku.
3.

Servery, ktoré budú začlenené do prostredia ESZ budú pre zachovanie úrovne bezpečnosti ESZ prostedia zabezpečené nasledovnými bezpečnostnými mechanizmami:

- integrovanou ochranou serverov – pre antimalware ochranu,
- ochranou integrity operačných systémov
- integrovaná ochrana serverov –pre kontrolu súladu konfigurácie systémov so
- schválenou konfiguráciou
- systémom pre zaznamenávanie interaktívných činností pri ich správe
- Systémom pre detekciu zmien- pre monitorovanie súborového systému

Na databázach a sieťových zariadeniach, ktoré budú začlenené do prostredia ESZ, bude implementované monitorovanie integrity.

3.6 HL Komunikácia a väzby



Vyšie uvedený obrázok popisuje logické organizáciu jednotlivých modulov vo vsťahu k operátorom a administrátorom systému. Operátor bude mať prístup k modulom ktoré priamo využíva pri svojej činnosti. Sú to primárne tieto IS:

- Kontaktné centrum – Obsluha klientských komikačných kanálov
- Servicedesk – Vykonávanie činností nad jednotlivými zadanými incidentmi.
- Monitoring a bezpečnosť - Portál s agregovanými informáciami z monitoringu prevádzky a bezpečnosti.

4 Kontaktné centrum

P.č.	Technická požiadavka	Oblasť	Uchádzač spĺňa kritérium (A/N)	Uvedené v kapitole tech. Dok.
1	Z technologického hľadiska musí kontaktné centrum pozostávať minimálne z týchto častí: • systém centrálnej logiky KC (procesovanie hovorov, frontovanie hovorov) • hlasová brána na prestup do verejnej telefónnej siete • systém pre nahrávanie hovorov	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1IS KC	5
2	Systém centrálnej logiky KC procesovanie a frontovanie hovorov s podporou webových servisov typu WSDL a SOAP.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5
3	Systém pre aktívne narávanie hovorov v šifre a vo formáte MP3 a WAV, zobrazenie celej konverzácie na jednej časovej osi.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.2 Modul Nahrávanie	5
4	Ponúkané riešenie KC schopné behu na jednom fyzickom serveri v redundantnom zapojení a vysokej dostupnosti v maximálnej veľkosti 2U.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5
5	Podpora systému KC pre jednotné zberanie a zobrazenie logovania na jednom mieste.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5
6	Podpora systému KC pre multi operácie – zmena viacerých položiek naraz z jedného miesta.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5

7	Podpora systému KC pre manuálne a automatizované generovanie reportov a ich distribúciu prostredníctvom emailov vo formáte PDF, XLS a CSV.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5
8	Softvérová IP telefónna ústredňa s hlasovou a video komunikáciou, postavená na protokole IP, a to na jednej platforme s podporou protokolov SIP, SCCP, MGCP, H323 a EMCC.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5
9	Riešenie KC musí byť schopné z pohľadu stavu hardvéru poskytnúť: • jednotný inventárny výpis hardvéru KC • sledovanie stavu hardvéru KC • posielanie oznámení o stave hardvéru KC	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5
10	Všetky zariadenia v rackovom prevedení 19", maximálna veľkosť 2U.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5
11	Supervízorský a agentský IP telefón s interným dvojportovým prepínačom, USB konektorom a Bluetooth s podporou MIC a LSC certifikátov.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1IS KC	5
12	Automatizované smerovanie hovorov na voľných operátorov - prostredníctvom funkcie ACD musí byť zabezpečené smerovanie, triedenie a frontovanie prichádzajúcich hovorov.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum • FP-25 automatické smerovanie podľa zručností (IVR-Interactive Voice Response)	4

13	Automatické smerovanie podľa zručností (IVR-Interactive Voice Response): • funkcia IVR musí umožniť odovzdať, resp. prijať určité informácie od koncového používateľa bez nutnej spoluúčasti aktívneho agenta • systém musí poskytnúť vizuálne rozhranie pre konfiguráciu a správu IVR v administratívnom rozhraní • administratívne rozhranie musí poskytovať funkcie ako: • vetvenie IVR stromov • nastavenie výziev a číselných volieb (tónovej voľby DTMF) • smerovaní podľa zručností agentov • definovanie hudby pre čakajúce hovory vo frontách	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum • FP-25 automatické smerovanie podľa zručností (IVR-Interactive Voice Response)	4
14	Viaceré fronty hovorov - systém musí umožniť nastavenie viacerých front pre volajúcich klientov do KC, ktoré budú obsluhované zadefinovanými skupinami riešiteľov podľa ich súboru zručností.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum • FP-25 automatické smerovanie podľa zručností (IVR-Interactive Voice Response) • FP-25 automatické smerovanie podľa zručností (IVR-Interactive Voice Response)	4
15	Viac jazyčné IVR - systém musí umožniť konfiguráciu IVR stromu vo viacerých jazykových mutáciách, primárne v slovenskom jazyku.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • FP-37 viac jazyčné IVR	4
16	Zadržanie volajúceho na linke prostredníctvom špecifikovanej hudby - systém musí umožniť nastavenie špecifickej hudby pre klientov čakajúcich vo fronte.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • FP-30 funkcia podržania	4

			hovoru - Hold on	
17	Manažment hovoru na pracovnej stanici operátora - systém musí umožniť na pracovnej ploche operátora KC umiestniť integrovanú lištu s ovládačmi potrebnými pre manažment hovorov (zdvihnúť, zložiť, presmerovať, nahrávať, podržať hovor, ...)	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
18	Funkcia podržania hovoru - Hold on - systém musí umožniť podržanie prebiehajúceho hovoru na voľbu operátora.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
19	Funkcia Wrap-Up time - systém musí poskytnúť operátorovi KC po skončení hovoru čas potrebný na zaznamenanie údajov o ukončenom hovore.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
20	Funkcia presmerovania hovoru - systém musí umožniť operátorovi KC presmerovať prebiehajúci hovor na iného agenta, skupinu agentov s potrebným súborom zručností, telefónne číslo…	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
21	Funkcia konferenčného hovoru - systém musí umožniť operátorovi presmerovať hovor na ďalšieho účastníka (operátora), z ktorých vytvorí konferenčný hovor.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
22	Funkcia odposluchu hovoru agenta - systém musí umožniť supervízorom KC pasívny vstup do zvoleného prebiehajúceho hovoru na KC.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
23	Funkcia vstúpiť do hovoru agenta s volajúcim - systém umožní supervízorom KC aktívny vstup do zvoleného prebiehajúceho hovoru agenta s volajúcim.	CallCentrum	A – Áno • 3.1.1 Modul Kontaktné centrum	4

24	Zaznamenávanie hovoru (automatické i manuálne) - systém musí umožniť nastavenie automatického zaznamenávania všetkých volaní na KC po spojení s operátorom a tiež umožní spustiť nahrávanie operátorovi KC počas hovoru.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
25	Priradenie záznamu hovoru k incidentu - pri vytvorení nového incidentu alebo aktualizácii existujúceho incidentu kanálom telefón, systém musí umožniť priradenie záznamu hovoru k predmetnému incidentu.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
26	Service level monitoring pre KC: • systém musí umožniť naživo monitorovať (live monitoring) úroveň poskytovaných služieb KC • systém musí umožniť naživo reportovať (live reporting) počet volajúcich čakajúcich vo frontách, počet volajúcich, ktorý zavesili pred spojením s operátorom ...	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
27	Nástroj pre správu threshold-ov vyťaženia KC (service level), upravovateľné eskalácie dosiahnutia stanovených limitov threshold-ov KC - systém musí umožniť monitorovať hovory v čakacej rade a čas od vytvorenia incidentu po zmenu na vybrané stavy. V administrácii aplikácie musí byť možnosť nastaviť SLA parametre pre uvedené monitorovanie, následne vyhodnocovať reálny čas úrovne poskytovanej služby s požadovanou (interná SLA). Pri prekročení limitov systém musí vedieť zaslať notifikácie supervízorom KC.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
28	Zabezpečenie bezproblémovej prevádzky pri očakávaných počtoch operátorov KC na dvoch lokalitách - celkový počet operátorov pre zabezpečenie prvého kontaktu (1.úroveň podpory) pre služby NZIS je 15ks.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
29	Z technologického pohľadu musí riešenie KC spĺňať požiadavky moderného riešenia: • rozšíriteľnosť – riešenie musí počítať s postupným nárastom kapacity supervízorov, agentov, ale aj IVR stromov (min. na dvojnásobný počet) • modulárnosť – riešenie musí počítať s postupným dopĺňaním nových služieb a komunikačných kanálov ako napríklad	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4

	s prístupom na sociálne siete, KC s podporou videa alebo nástrojmi na riadenie pracovnej sily • flexibilita – riešenie musí byť flexibilné z pohľadu umiestnenia a využívania ľudských zdrojov, riešenie musí byť schopné vytvárať virtuálne KC skupiny v rôznych geografických lokalitách • integrácia – v oblasti informačných systémov musí KC umožniť integráciu so systémami zákazníka na úrovni webservisov, čítania a zápisu do databáz, prípadne použitím štandardizovaných rozhraní			
30	Operátori KC musia mať k dispozícií aktívny prístup k znalostnej databáze, aby bola pre rutinnú prevádzku zabezpečená čo najväčšia univerzálnosť operátorov a tím špecialistov.	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	4
31	Technické požiadavky na systém centrálnej logiky KC: • systém centrálnej logiky KC • konfigurovateľné rozhranie pre agentov • integrácia so systémami tretích strán (CTI, Webservice) • jednoduchý prístup k aplikáciám prístupných cez web rozhranie • vytváranie a úpravu reportov manuálne a automatizované generovanie reportov • automatizovanú distribúciu reportov prostredníctvom emailu • možnosť exportu reportov minimálne do formátov PDF, XLS a CSV • systém pre správu hovorov • softvérová IPT ústredňa • podpora hlasu a videa na jednej platforme • podpora protokolov RTCP, SRTP, BFCP, FECC • podpora hlasových protokolov – SIP, SCCP, MGCP, H323, EMCC • integrácia so systémami tretích strán • podpora IVR iterácií • podpora XML (AXL) formátu • podpora LDAP protokolu • podpora jednotného prihlásenia sa do systému (SSO) • natívna podpora IM (Instant Messaging) • systém pre frontovanie hovorov	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.1 Modul Kontaktné centrum	5

	• doručovanie notifikácií používateľom • podpora webových servisov typu WSDL a SOA • podpora RTSP, ASR, TTS a MRCPv2 • podpora SNMPv3 • podpora vysokej dostupnosti cez WAN (geografická redundancia)			
32	Technické požiadavky na hlasovú bránu na prestup do VTS (Verejnej Telefónnej Siete) • prevedenie – Rack 19“ • výška zariadenia – max. 2U • min. 256MB vnútornej pamäte rozšíriteľná do 4GB • min. 512MB systémovej pamäte rozšíriteľná do 2.5GB • integrované 3 x 10/100/1000 RJ-45 porty • 1 x rozšíriteľný modul • 4 x rozšíriteľné WAN sloty • min. smerovací výkon 180 Mbps • min. 32 kanálový procesor pre spracovanie hlasu • podpora T1/E1 kariet a SIP trunk-u • podpora IP telefónie • podpora HW šifrovania – 3DES/DES, AES	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.3 Modul Brána do VTS	5
33	Technické požiadavky na systém pre nahrávanie hovorov: • systém musí zabezpečiť ukladanie všetkých nahrávok na centrálnom mieste • systém musí umožniť vyhľadávanie hovorov na základe rôznych filtrov vyhľadávania s možnosť uloženia použitých filtrov • podpora formátov nahrávania hovorov – MP3, WAV • musí byť schopný vytvárať riadený archív hovorov, s možnosťou automatizovaného presunu alebo vymazania hovorov po uplynutí archivačnej doby • podporované formáty zvuku – G.711a, G.711μ, G.729a, G.729ab, G.722 • znázornenie celej konverzácie na jednej časovej osi • kryptovanie a správa kľúčov: • štandardy kryptografie verejných kľúčov (PKCS12, JKS, JCEKS) • štandardné šifrovacie algoritmy (AES, DES, Blowfish) • šifrovanie nahraných hovorov a	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1.3 Modul Brána do VTS	5

	záznamov obrazoviek • podpora a dodržiavanie štandardu PCI-DSS pre ochranu súkromných dát • webové API pre integráciu s aplikáciami tretích strán			
34	Minimálne technické požiadavky na IP telefón pre operátora Kontaktného centra: • podporované kodeky – G.711a, G.711μ, G.722 G.729a, • interný prepínač – 2x 10/100/1000 RJ-45 • min. 1 USB konektor s 500mA príkonom • min. Bluetooth 3.0 • min. 2 funkčné a 6 programovateľných tlačidiel • farebný 5“displej s min. rozlíšením 800x480 24-bit • rozhranie pre pripojenie Headset RJ-9 port • tlačidla na ovládanie hlasitosti • PoE 802.3af (Class 3) a 802.3at napájanie • signalizačný protokol SIP • autentifikácia telefónu využitím MIC a LSC certifikátov • zobrazovanie informácií na displeji cez XML • šifrovanie hlasu • možnosť napájania cez napájací zdroj • všetky potrebné licencie na fungovanie so softvérovou ústredňou	CallCentrum	A – Áno – Funkcionalita bude implementovaná	5
35	Minimálne technické požiadavky na slúchadlá pre operátora Kontaktného centra: • monaurálne alebo binaurálne prevedenie • mikrofón s filtrom na rušenie okolitého hluku • možnosť prepojenia s IP telefónom (VoIP) • 7 nastaviteľných osí zabezpečujúcich celodenný komfort • audio QuickDisconnect alebo USB rozhranie • podpora optimalizácie pre produkt Microsoft Lync	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1IS KC	5

36	Minimálne technické požiadavky na počítačovú zostavu pre operátora KC: • Prevedenie – midi/mini tower • CPU – Procesor triedy x64 dosahujúci výsledok v teste „PassMark CPU Mark" na úrovni min. 7225 bodov • RAM – 4GB DDR3 • HDD – 500GB 7200RPM SATA 3.5“ • DVD – Mechanika DVD-ROM • VGA – dedikovaná grafická karta, 1GB DDR3, PCI Express 2.0 • Zvuková karta – integrovaná zvuková karta Rozhrania: • sieťová karta 10/100/1000 LAN, RJ-45 • 4x USB 2.0, z toho min. 2x USB 3.0 • 1x DVI, 1x VGA, 1x HDMI • o audio vstup MIC, LINE IN, stereo výstup na slúchadlá Jack 3.5 • Zdroj – max. 300W • Operačný systém kompatibilný s klientskou aplikáciou KC • Príslušenstvo – USB klávesnica SK, USB optická myš Obrazovka: • veľkosť obrazovky 24” LED • pomer strán 16:10 • natívne rozlíšenie obrazovky 1920x1200 • jas min. 300cd/m2 • max. doba odozvy 7ms • uhol zobrazenia min. 178°/178° • rozhrania 1xDVI, 1xVGA • výškovo nastaviteľný stojan min. 110mm • zvislé naklonenie aspoň 30 stupňov dozadu • príslušenstvo – 1x DVI, alebo 1x VGA kábel	CallCentrum	A – Áno – Funkcionalita bude implementovaná • 3.1IS KC	5

5 Monitoring

P.č.	Technická požiadavka	Oblasť	Uchádzač spĺňa kritérium (A/N)	Uvedené v kapitole tech. Dok.
1	podpora monitoringu hardvéru (inventarizácia, dostupnosť, stav, prediktívne chyby)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS).	4.3.3
2	podpora monitoringu sieťových a bezpečnostných komponentov	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	4.3.3
3	podpora monitoringu operačných systémov a platformových produktov	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	4.3.3
4	podpora monitoringu aplikácií a biznis služieb	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	4.3.3
5	CMS musí byť schopný spracovania výstupov z iných monitorovacích nástrojov a vytvorenia jednotného monitoring nástroja (tzv. umbrella monitoringu)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém	4.3.3

			(CMS).	
6	nástroje CMS musia byť schopné vyhodnotenia modelov služieb vytvorených na základe informácií z centrálnej konfiguračnej databázy CMDB evidovanej v rámci SD systému	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP)	4.3.3
7	vyhodnotenie modelov služieb musí prebiehať na základe informácií (udalostí) z dostupných monitoring nástrojov implementovaných v rámci riešenia	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP)	4.3.3
8	CMS musí zabezpečiť realizáciu monitoringu služieb z pohľadu koncového používateľa	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS).	4.3.3
9	CMS musí poskytnúť prehľadné rozhrania pre vizualizáciu aktuálneho stavu služieb a rýchle vyhľadanie príčin výpadkov (root cause)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.4 Modul IBM Tivoli Common Reporting (TCR)	4.3.3
10	pri výpadku IT zdroja zachytenom monitorovacími nástrojmi musí vediet CMS identifikovať jeho dopad na poskytované služby (impact anal ysis)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	4.3.3
11	výstupy z CMS musia byť previazané s procesným nástrojom (automatická tvorba incidentov pre vyhodnotenie poskytovanej úrovne kvality služieb)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém	4.3.3

			(CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	
12	CMS musí umožniť vyhodnotenie plánovania výpadkov infraštruktúry a služieb	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring • 3.3.2.4 Modul IBM Tivoli Common Reporting (TCR)	4.3.3
13	CMS musí umožniť prístup k monitoring nástrojom s využitím „Single Sign On“ a externej autentifikácie cez ActiveDirectory/LDAP	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS).	4.3.3
14	nástroj pre spracovanie výstupov z CMS musí byť robustný a schopný rýchleho spracovania a vyhodnotenia dát aj v kritických situáciách (napr. pri vygenerovaní veľkého množstva udalostí)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.4 Modul IBM Tivoli Common Reporting (TCR)	4.3.3
15	spracovanie vstupných dát vo forme udalostí musí byť jednoducho a prehľadne konfigurovateľné	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	4.3.3

			• 3.3.2.4 Modul IBM Tivoli Common Reporting (TCR)	
16	CMS musí zabezpečiť identifikáciu kritických udalostí nielen podľa základného parametra kritickosti zdroja "severity" ale aj s využitím doplnkovej informácie o dopade (informácia o kritickosti konkrétneho objektu v rámci služby v danom čase)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	4.3.3
17	CMS musí podporovať korelácie udalostí minimálne na úrovni párovania up/down správ, deduplikácie, zmeny priority na základe zdroja udalosti a času	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	4.3.3
18	CMS musí podporovať štandardné rozhrania pre integráciu s inými nástrojmi (SNMP, WebServices)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP)	4.3.3
19	CMS musí priamo podporovať integráciu s nástrojom Microsoft SCOM 2012 (metódou „out of the box“)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	4.3.3
20	CMS musí priamo podporovať príjem udalostí cez SNMP, Syslog, JMX a WMI z rôznych zariadení a systémov	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.2.3 Modul IBM	4.3.3

			Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	
21	požiadavka na integráciu CMS so SD systémom • medzi CMS a SD systémom musí existovať rozhranie pre automatizovaný prenos udalosti z monitoringu do SD v rámci Event management procesu.	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP)	4.3.3
22	Požiadavky na licenčné pokrytie CMS pre Produkčné prostredia NZIS (ESZ+JRUZ) v rozsahu: • monitoring sieťových komponentov (prepínač, router, firewall, loadbalancer) v počte min. 141ks • integráciu monitorovaných objektov z aplikácie MS SCOM v počte min. 172ks • monitoring operačných systémov Linux v počte min. 21ks • integrácia diagnostiky stavu biznis služieb vyhodnocovaných prostredníctvom volania WS služieb SysCheck a Ping v počte min. 526ks • monitoring sieťových zariadení monitorovaných prostredníctvom SNMP protokolu v počte min. 271ks • monitoring biznis služieb na základe stromov závislosti vytváraných z monitorovaných objektov v počte min. 605ks	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS).	5.2
23	Požiadavky na licenčné pokrytie CMS pre PredProdukčné prostredia NZIS (ESZ+JRUZ): • monitoring sieťových komponentov (prepínač, router, firewall, loadbalancer) v počte min. 68ks • integráciu monitorovaných objektov z aplikácie MS SCOM v počte min. 23ks • monitoring operačných systémov Linux v počte min. 11ks • integrácia diagnostiky stavu biznis služieb vyhodnocovaných prostredníctvom volania WS služieb SysCheck a Ping v počte min. 526ks • monitoring sieťových zariadení monitorovaných prostredníctvom SNMP protokolu v počte min. 91ks	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS).	5.2

	• monitoring biznis služieb na základe stromov závislosti vytváraných z monitorovaných objektov v počte min. 193ks			
24	podpora funkcionality "network discovery"	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
25	podpora vizualizácie topológie a "topology based root cause analysis"	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
26	OOTB podpora SNMP v 1,2,3	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
27	OOTB podpora štandardných protokolov a zariadení	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	

28	požiadavka na vysokú mieru konfigurovateľnosti CMS: • možnosť rozšírenia topologického modelu, • možnosť tvorby vlastných nástrojov pre network discovery, • dotazovanie a vizualizácia zariadení na základe filtrov.	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
29	podpora zberu a vyhodnocovania dát z aplikácií a databáz na heterogénnych OS platformách	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring • 3.3.2.4 Modul IBM Tivoli Common Reporting (TCR)	5.2
30	agent pre monitoring musí poskytovať spoločný zber dát pre fault aj performance monitoring	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
31	podpora automatizovanej sumarizácie nameraných dát	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring • 3.3.2.4 Modul IBM Tivoli Common Reporting (TCR)	5.2

32	podpora súčasného zobrazenia aktuálnych aj historických dát	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.4 Modul IBM Tivoli Common Reporting (TCR)	5.2
33	podpora tvorby vlastných monitorovacích postupov pre priamo nepodporované aplikácie	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
34	CMS musí vedieť poskytnúť základnú funkcionalitu monitoringu bez nutnosti dodatočného vývoja	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
35	vysoká miera integrácie dielčich monitorovacích nástrojov s CMS	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2

36	schopnosť generovať udalosti v rámci event management procesu na základe zmeny stavu monitorovanej služby, alebo jej časti	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
37	schopnosť zohľadniť a zobraziť informácie z externých zdrojov pri vyhodnocovaní modelov služieb	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM SmartCloud APM/SmartCloud Monitoring	5.2
38	schopnosť monitorovania a vyhodnocovania veľkého počtu objektov (rádovo 1000-ky)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS).	5.2
39	podpora systému vysokej dostupnosti (HA)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS).	5.2
40	podpora operačných systémov – MS Windows Server, Red Hat Enterprise Linux, SUSE Enterprise Linux alebo ekvivalentných	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP) • 3.3.2.2 Modul IBM	5.2

			SmartCloud APM/SmartCloud Monitoring	
41	schopnosť rozširovania systému do šírky (riešenie musí umožniť integrovať ďalšie prostredia NZIS do CMS)	Monitoring	A – Áno – Funkcionalita bude implementovaná • 3.3.1 SmartCloud • Modul Centrálny monitorovací systém (CMS). • 3.3.2.3 Modul IBM Tivoli Integrated Portal (TIP)	5.2

6 ServiceDesk

P.č.	Technická požiadavka	Oblasť	Uchádzač spĺňa kritérium (A/N)	Uvedené v kapitole tech. Dok.
1	evidencia a riadenie priebehu riešenia incidentov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk	4.3.2
2	evidencia vzťahov so súvisiacimi záznamami z ostatných procesov (požiadavka, incident, problém, zmena, konfiguračná položka)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul Service Desk	4.3.2
3	vzájomná komunikácia a koordinácia medzi jednotlivými pracovníkmi prevádzky - možnosť preradiť/previať rozpracovaný incident iného pracovníka	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul Service Desk	4.3.2
4	funkčné a hierarchické eskalácie v priebehu riešenia incidentov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul Service Desk	4.3.2
5	evidencia náhradných a trvalých riešení a ich integrácia do znalostnej databázy	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul Service Desk	4.3.2
6	vyhľadávanie v znalostnej databáze počas celého životného cyklu incidentu	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul	4.3.2

			Service Desk	
7	konfigurovateľná kategorizácia/klasifikácia incidentov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2 IS SD • 3.2.1 Modul IBM Control Desk	4.3.2
8	automatické prideľovanie priority na základe procesných pravidiel (napr. matica dopadu a naliehavosti)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul Service Desk	4.3.2
9	automatické priraďovanie riešiteľských skupín podľa rôznych pravidiel	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému	4.3.2
10	automatické priraďovanie riešiteľov zo skupín (podľa počtu riešených incidentov, rovnomerne) so zohľadnením dostupnosti jednotlivých riešiteľov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému	4.3.2
11	automatická diagnostika a riešenie incidentov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2 IS SD • 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul Service Desk	4.3.2
12	definícia a meranie rôznych metrík a kľúčových ukazovateľov výkonnosti procesu	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.2 Modul IBM Tivoli Common	4.3.2

			Reporting	
13	zaznamenávanie histórie spracovania a zmien atribútov jednotlivých objektov, vrátane identifikácie používateľa, ktorý danú aktivitu, resp. zmenu vykonal	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému	4.3.2
14	poskytovanie výstupov pre vyhodnocovanie úrovne poskytovaných služieb	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.4 Modul Úrovne služieb • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
15	evidencia a riadenie problémov počas ich celého životného cyklu	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk	4.3.2
16	evidencia vzťahov so súvisiacimi záznamami z ostatných procesov (incident, problém, zmena, konfiguračná položka)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.2Modul Zmeny • 3.2.1.7 Modul Konfigurácia systému	4.3.2
17	podpora pre proaktívny Problem Management - identifikácia potenciálnych problémov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul Service Desk • 3.2.1.2Modul Zmeny • 3.2.1.5 Modul Infraštruktúra IT • 3.2.1.7 Modul Konfigurácia systému	4.3.2

18	podpora pre reaktívny Problem Management • vytváranie problémov na základe výstupov z procesu Incident Management (často opakujúce sa incidenty)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
19	evidencia známych chýb a ich integrácia do znalostnej databázy	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul Integrácie	4.3.2
20	integrácia s procesom Change Management pri nasadzovaní trvalých riešení	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.2Modul Zmeny • 3.2.1.7 Modul Konfigurácia systému	4.3.2
21	evidencia a riadenie zmien počas ich celého životného cyklu	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.2Modul Zmeny	4.3.2
22	evidencia vzťahov so súvisiacimi záznamami z ostatných procesov (požiadavka, incident, problém, zmena)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk	4.3.2
23	možnosť evidovať vzťahy na konkrétne ovplyvnené konfiguračné prvky z konfiguračnej databázy	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	4.3.2

			• 3.2.1 Modul IBM Control Desk • 3.2.1.1 Modul Service Desk • 3.2.1.5 Modul Infraštruktúra IT • 3.2.1.6 Modul Aktíva • 3.2.1.7 Modul Konfigurácia systému	
24	možnosť definície rôznych workflowov s rôznymi procesnými pravidlami, pre rôzne kategórie a typy zmien (Napr.: Štandardné zmeny, Urgentné zmeny, Normálne zmeny)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul Integrácie	4.3.2
25	možnosť dekompozície zmeny na parciálne úlohy a ich pridelenie na rôznych riešiteľov/riešiteľské skupiny	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému	4.3.2
26	konfigurovateľné schvaľovacie pravidlá	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému	4.3.2
27	vizuálne plánovanie zmien s identifikáciou možných konfliktov pri nasadzovaní zmien	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.2Modul Zmeny • 3.2.1.5 Modul Infraštruktúra IT	4.3.2
28	plánovanie zmien so zohľadnením garantovanej dostupnosti danej služby	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	4.3.2

			• 3.2.1.1 Modul Service Desk • 3.2.1.2Modul Zmeny • 3.2.1.4 Modul Úrovne služieb	
29	riešenie musí obsahovať kalendár zmien	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.2Modul Zmeny • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
30	analýza dopadov zmeny na základe vzťahov medzi konfiguračnými položkami	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.2Modul Zmeny	4.3.2
31	definícia a meranie rôznych metrík a kľúčových ukazovateľov výkonnosti procesu	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
32	zaznamenávanie histórie spracovania a zmien atribútov jednotlivých objektov, vrátane identifikácie používateľa, ktorý danú aktivitu, resp. zmenu vykonal	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.2Modul Zmeny	4.3.2
33	poskytovanie výstupov pre vyhodnocovanie úrovne poskytovaných služieb	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.4 Modul Úrovne služieb	4.3.2
34	evidencia a riadenie vydaní pri nasadzovaní nových alebo zmenených služieb NZIS	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.3 Modul Vydania • 3.2.1.4 Modul	4.3.2

			Úrovne služieb	
35	evidencia vzťahov s ovplyvnenými konfiguračnými prvkami a súvisiacimi záznamami z ostatných procesov (požiadavka, incident, problém, zmena)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
36	podpora pridávania/odoberania zmien z procesu Change Management do jednotlivých vydaní	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.2Modul Zmeny	4.3.2
37	vytváranie a udržiavanie evidencie knižnice médií - Definitive Media Library (DML)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.5 Modul Infraštruktúra IT • 3.2.1.6 Modul Aktíva • 3.2.1.7 Modul Konfigurácia systému	4.3.2
38	integračné rozhranie pre automatické vytváranie incidentov z centrálneho monitorovacieho systému	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.5 Modul Infraštruktúra IT • 3.2.1.8 Modul Integrácie	4.3.2
39	poskytovanie informácií o schválených odstávkach poskytovaných služieb centrálnemu monitorovaciemu systému	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2 IS SD • 3.2.1 Modul IBM Control Desk • 3.2.1.8 Modul Integrácie	4.3.2

40	štruktúrovaná konfiguračná databáza (CMDB) - kategorizácia konfiguračných prvkov (CI), rôzne typy vzťahov medzi CI	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.6 Modul Aktíva • 3.2.1.7 Modul Konfigurácia systému	4.3.2
41	evidencia konfiguračných prvkov v CMDB so vzájomnými vzťahmi	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.6 Modul Aktíva • 3.2.1.7 Modul Konfigurácia systému	4.3.2
42	jednoduchá zmena konfigurácie a štruktúry CMDB (pridávanie/zmena atribútov pre jednotlivé typy CI, povinné polia, validácie), bez nutnosti programovania	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.6 Modul Aktíva • 3.2.1.7 Modul Konfigurácia systému	4.3.2
43	podpora pre integráciu s discovery nástrojmi	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.8 Modul Integrácie	4.3.2
44	grafická vizualizácia konfiguračných prvkov a väzieb medzi nimi s možnosťou navigácie v CMDB prostredníctvom topológie	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2

45	poskytovanie dát ostaným prevádzkovým procesom (Incident Management, Change management, CHM...) pre zefektívnenie ich vykonávania	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.8 Modul Integrácie • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
46	zaznamenávanie histórie zmien CI, počas celého ich životného cyklu	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk	4.3.2
47	evidencia rôznych dohodnutých parametrov úrovne služieb - dostupnosť, spoľahlivosť, požadované časy odozvy a riešenia	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.4 Modul Úrovne služieb	4.3.2
48	meranie a vyhodnocovanie dohodnutých časov odozvy a riešenia pre jednotlivé poskytované služby v závislosti od rôznych parametrov (napr.: služba, priorita)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
49	eskalácie v rámci priebehu monitorovania dohodnutých časov spracovania a riešenia incidentov a požiadaviek	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul Integrácie	4.3.2
50	vytváranie a udržiavanie rôznych pohľadov na katalóg služieb (Technical Service Catalog, Business Service Catalog)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
51	musí poskytovať web rozhranie pre evidenciu požiadaviek o službu (podľa definovaného biznis katalógu	ServiceDesk	A – Áno – Funkcionalita bude	4.3.2

	služieb)		implementovaná • 3.2.1.4 Modul Úrovne služieb	
52	musí poskytovať plnohodnotné webové rozhranie pre používateľov aj administrátorov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	4.3.2
53	musí umožniť jednoduchú implementáciu zmien v aplikácii, vyplývajúcich zo zmeny/úpravy prevádzkových procesov (v réžii obstarávateľa, bez nutnosti programovania)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému	4.3.2
54	musí umožniť jednoduchú konfiguráciu a zmenu používateľského rozhrania (v réžii obstarávateľa, bez nutnosti programovania)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému	4.3.2
55	musí umožňovať pridávať, meniť a mazať dohodnuté procesné notifikácie a eskalácie prostredníctvom grafického používateľského rozhrania (v réžii obstarávateľa, bez nutnosti programovania)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	4.3.2
56	musí používateľom umožniť prispôsobiť si vzhľad úvodnej obrazovky	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.1 Modul Service Desk	4.3.2
57	poskytovať prostriedky pre vytváranie a úpravu reportov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
58	poskytovať podporu pre ad-hoc (jednorazové) a pravidelné reporty	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
59	umožňovať manuálne a automatizované generovanie reportov	ServiceDesk	A – Áno – Funkcionalita bude	4.3.2

			implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	
60	umožňovať automatizovanú distribúciu reportov prostredníctvom emailu	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul Integrácie • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
61	poskytovať možnosť exportu reportov minimálne do formátov PDF, XLS	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
62	umožňovať vytváranie nových a úpravu existujúcich reportov v používateľsky prívetivom prostredí	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	4.3.2
63	definíciu prístupových práv vo forme aplikačných rolí, pričom oprávnenia používateľa budú definované množinou aplikačných rolí	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému •	4.3.2
64	podrobné riadenie prístupov - riadenie prístupov musí byť umožnené na základe operácií nad dátami (napr. vytvorenie, editácia, schválenie) a na základe rozsahu dát (napr. práva len pre priradené incidenty, práva len na incidenty pre určité služby)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému •	4.3.2
65	riadenie prístupu k údajom na úrovni objektov, atribútov, lokalít, stavov, katalógu služieb, organizácií	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	4.3.2

			• 3.2.1.7 Modul Konfigurácia systému • 3.2.2 Modul IBM Tivoli Common Reporting	
66	auditovanie zmien nad dátami v systéme	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	4.3.2
67	overenie identity používateľa (používateľským menom a heslom) pri zmene citlivých dát v systéme	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	4.3.2
68	ukladanie a prácu s citlivými údajmi (ukladanie v zašifrovanej forme)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	4.3.2
69	všetky funkcie dostupné cez webové rozhranie	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	5.2
70	kompatibilné s mobilnými zariadeniami (PDA, smartphone)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	5.2
71	lokalizované do slovenského jazyka (pre všetky úrovne podpory)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	5.2
72	podpora grafického modelovania a definície workflow pre všetky požadované procesy	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému	5.2
73	podpora grafického zobrazovania stavu procesných objektov (požiadavka, incident, problém, zmena, release, konfiguračný prvok) v ich životnom cykle	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	5.2
74	štandardné a otvorené komunikačné protokoly (HTTP, SMTP, TCP/IP)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná	5.2
75	štandardné a otvorené výmenné formáty (XML, SOAP, JSON)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1 Modul IBM Control Desk • 3.2.1.8 Modul Integrácie	5.2
76	štandardné protokoly na komunikáciu s poštovými službami (SMTP)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul	5.2

			Integrácie	
77	spracovanie štandardných webových služieb pre potreby integrácie s inými aplikáciami	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul Integrácie	5.2
78	jednoduchý import a export údajov do textových súborov (min. XML, CSV)	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul Integrácie	5.2
79	vytváranie a úprava reportov priamo v nástroji	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	5.2
80	automatizácia pregenerovania periodických reportov	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul Integrácie • 3.2.2 Modul IBM Tivoli Common Reporting	5.2
81	automatizovaná distribúcia reportov emailom	ServiceDesk	A – Áno – Funkcionalita bude implementovaná • 3.2.1.7 Modul Konfigurácia systému • 3.2.1.8 Modul Integrácie • 3.2.2 Modul IBM Tivoli Common Reporting	5.2
82	export reportov do formátov PDF a	ServiceDesk	A – Áno –	5.2

	XLS		Funkcionalita bude implementovaná • 3.2.2 Modul IBM Tivoli Common Reporting	