Název operačního programu: Technická pomoc
Označení operačního programu: **OPTP 2007 - 2013**
Projekt: Zajištění služby Bezpečnostního dohledu pro MS2014+
Reg. č. projektu: CZ.1.08/2.1.00/13.00167

Č.j.: MMR-23591/2015-24/8
Číslo v CES: 5390
Čísla úkolů: 3691/5168/50/24
3691/5168/51/24]

SMLOUVA O POSKYTOVÁNÍ SLUŽEB

Smluvní strany:

Česká republika – Ministerstvo pro místní rozvoj

se sídlem:	Staroměstské náměstí 6, 110 15 Praha 1
zastoupen:	RNDr. Blankou Fischerovou, ředitelkou Odboru správy monitorovacího systému
IČ:	66 00 22 22
Bankovní spojení:	ČNB Praha 1, Na Příkopě 28
Číslo účtu:	629001/0710
Datová schránka:	26iaava

(dále jen „***Objednatel***“, v jednotlivých částech Příloh této Smlouvy o dílo označen též jako „***Zadavatel***“)

a

T-Mobile Czech Republic a.s.

se sídlem:	Tomíčkova 2144/1, Praha 4, 148 00
IČ:	64949681
DIČ:	CZ64949681
Bankovní spojení:	[redacted]
Číslo účtu:	

zapsána v obchodním rejstříku vedeném u rejstříkového soudu v Praze, oddíl B, vložka 3787

zastoupena:	Ing. Petrem Malimánkem, na základě pověření Radkem Podzemským, na základě pověření
Datová schránka:	ygwch5i

(dále jen „***Poskytovatel***“)

(Objednatel a **Poskytovatel** dále jednotlivě též jen „***Smluvní strana***“ nebo společně „***Smluvní strany***“)

OBSAH:

I. ÚVODNÍ USTANOVENÍ ... 3
II. ÚČEL SMLOUVY ... 5
III. PŘEDMĚT SMLOUVY ... 6
IV. DOBA A MÍSTO PLNĚNÍ ... 7
V. CENA A PLATEBNÍ PODMÍNKY ... 8
VI. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN ... 12
VII. ZMĚNOVÉ ŘÍZENÍ ... 18
VIII. AKCEPTACE VÝSLEDKŮ POSKYTOVANÉHO PLNĚNÍ ... 19
IX. ODPOVĚDNOST ZA ŠKODU, ODPOVĚDNOST ZA VADY, ZÁRUKA ... 20
X. VLASTNICKÉ PRÁVO A PRÁVO UŽITÍ ... 21
XI. OCHRANA OSOBNÍCH ÚDAJŮ A DŮVĚRNÝCH INFORMACÍ ... 23
XII. OZNÁMENÍ A KOMUNIKACE ... 23
XIII. OPRÁVNĚNÉ OSOBY ... 24
XIV. KREDITACE A SANKCE ... 25
XV. DOBA TRVÁNÍ A ZÁNIK SMLOUVY ... 27
XVI. ZÁVĚREČNÁ USTANOVENÍ ... 29

I. ÚVODNÍ USTANOVENÍ

1.1 Smluvní strany se dohodly, že se jejich závazkový vztah řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „ObčZ“).

1.2 Smluvní strany prohlašují, že jejich identifikační údaje uvedené v záhlaví Smlouvy jsou v souladu s právní skutečností v době uzavření této smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí písemně bez prodlení druhé Smluvní straně. V případě změny účtu Poskytovatele je Poskytovatel povinen rovněž doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu. Při změně identifikačních údajů Smluvních stran včetně změny účtu není nutné uzavírat ke Smlouvě dodatek.

1.3 Smluvní strany prohlašují, že osoby podepisující Smlouvu jsou k tomuto úkonu oprávněny.

1.4 Pojmy s velkými počátečními písmeny definované v této Smlouvě budou mít význam, jenž je jim ve Smlouvě včetně jejích příloh a dodatků připisován. Pro zajištění jednotného výkladu pojmů používaných v rámci této Smlouvy definují Smluvní strany rovněž tento základní slovníček pojmů:

Pojem:	**Význam:**
Aplikace MS2014+	Souhrn programového vybavení, který společně tvoří logický celek Aplikaci MS2014+. Aplikace MS2014+ je dodávána, spravována a provozována Provozovatelem Aplikace MS2014+ na základě jiného smluvního vztahu.
MS2014+	Monitorovací systém Evropských strukturálních a investičních fondů (dále jen „ESI fondy“) na programové období 2014 - 2020 sestávající se z „Aplikace MS2014+“, „HW platformy a Infrastruktury serverovny pro Aplikaci MS2014+“ a „Bezpečnostního dohledu pro MS2014+“.
Smlouva o poskytování služeb	Tato smlouva (dále jen "***Smlouva***")
Veřejná zakázka	Veřejná zakázka s názvem "Zajištění služby Bezpečnostního dohledu pro MS2014+ pro MS2014+" ev. č. Věstníku veřejných zakázek 400671, zahájená Objednatelem dne 25. 10. 2014.
Zadávací dokumentace	Zadávací dokumentace Veřejné zakázky včetně všech jejích příloh.

HW platforma	Jedná se o veškeré HW vybavení provozované v primární a zálohovací / záložní lokalitě pro potřeby provozování Aplikace MS2014+. Součástí HW platformy jsou i vybrané prvky ze zálohovacího a testovacího/školícího prostředí.
Infrastruktura serverovny	Zajištění příslušných služeb datového centra včetně síťové infrastruktury, konektivity datového centra, housingu HW platformy, řízení a správy provozního prostředí, podpory HW a SW prvků třetích stran a dalších služeb pro Aplikaci MS2014+.
Prostředí	Představuje souhrn Infrastruktury serverovny, HW platformy a veškerého dalšího SW vybavení mimo Aplikace MS2014+ pro potřeby provozování Aplikace MS2014+. Případné výjimky budou Objednatelem protokolárně schváleny.
Provozovatel Aplikace MS2014+	Subjekt odpovědný za správu, provoz, rozvoj a údržbu Aplikace MS2014+ v rozsahu stanoveném na základě jiného smluvního vztahu (viz https://ezak.mmr.cz/contract_display_668.html).
Poskytovatel služeb Prostředí	Subjekt odpovědný za zajištění služeb provozu, správy, údržby a podpory Prostředí v rozsahu stanoveném na základě jiného smluvního vztahu (viz https://ezak.mmr.cz/contract_display_823.html).
Technický dozor	Subjekt zajišťující služby technického dozoru nad realizací celého projektu MS2014+ na základě jiného smluvního vztahu (viz https://ezak.mmr.cz/contract_display_730.html).
Bezpečnostní dohled	Subjekt zajišťující služby bezpečnostního dohledu MS2014+ na základě této Smlouvy

1.5 Smlouva byla uzavřena na základě výsledku zadávacího řízení na Veřejnou zakázku zadávanou Objednatelem jako zadavatelem ve smyslu zákona č. 137/2006 Sb., o veřejných zakázkách, v platném znění (dále jen „***ZVZ***“); neboť nabídka Poskytovatele byla v zadávacím řízení na Veřejnou zakázku vybrána jako nejvhodnější.

1.6 Poskytovatel dále prohlašuje, že se náležitě seznámil se všemi podklady, které byly součástí Zadávací dokumentace Veřejné zakázky a které stanovují požadavky na předmět plnění této Smlouvy, a že je odborně způsobilý ke splnění všech jeho závazků podle této smlouvy.

1.7 Poskytovatel se dále zavazuje, že bude Služby dle čl. 3.1 této Smlouvy poskytovat v souladu s veškerými požadavky obsaženými v Zadávací dokumentaci Veřejné zakázky a v souladu se svým návrhem a popisem způsobu poskytování Služeb, který tvoří Přílohu č. 4 této Smlouvy. Zadávací dokumentace bez příloh je součástí této Smlouvy jako její Příloha č. 3.

1.8 Pro vyloučení jakýchkoliv pochybností o vztahu Smlouvy a Zadávací dokumentace jsou stanovena tato výkladová pravidla:

1.8.1 v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel Veřejné zakázky vyjádřený Zadávací dokumentací;

1.8.2 v případě chybějících ustanovení Smlouvy budou použita dostatečně konkrétní ustanovení Zadávací dokumentace;

1.8.3 v případě rozporu mezi ustanoveními Smlouvy a Zadávací dokumentace budou mít přednost ustanovení této Smlouvy.

1.9 Poskytovatel prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění dle této Smlouvy, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění dle této Smlouvy a že disponuje takovým technickým vybavením, kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění dle této Smlouvy za dohodnutou smluvní cenu uvedenou v této Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění Veřejné zakázky.

1.10 Poskytovatel se zavazuje plnit předmět Smlouvy v souladu s platnými právními předpisy, jakož i v souladu se všemi normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kritéria k zajištění, že postupy a služby, případně materiály či výrobky, vyhovují předmětu Smlouvy a veškerým zadávacím podmínkám Veřejné zakázky. Poskytovatel se dále zavazuje, že jím poskytnuté plnění dle této Smlouvy bude splňovat požadavky na informační systémy dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, a návazných prováděcích předpisů.

II. ÚČEL SMLOUVY

2.1 Účelem Smlouvy je zajištění služby Bezpečnostního dohledu pro MS2014+ v rozsahu specifikovaném čl. III této Smlouvy.

2.2 Předmět plnění této Smlouvy bude realizován v rámci projektu spolufinancovaného ze strukturálních fondů Evropské unie v programovém období 2007 – 2013 a následně 2014 - 2020 (dále jen „***Projekt***“). O spolufinancování předmětu plnění Smlouvy ze strukturálních fondů Evropské unie Objednatel Poskytovatele bez zbytečného odkladu písemně

vyrozumí, včetně sdělení relevantních pravidel příslušného operačního programu, jež bude Poskytovatel povinen v souladu s touto Smlouvou, zejména jejím čl. VI, dodržovat.

III. PŘEDMĚT SMLOUVY

3.1 Předmětem této Smlouvy je závazek Poskytovatele poskytovat Objednateli za podmínek uvedených v této Smlouvě služby Bezpečnostního dohledu (dále jen "*Služby*") v následujících oblastech:

- BS01_Informační bezpečnost
- BS02_Ochrana osobních údajů
- BS03_Bezpečnostní monitoring
- BS04_Kontrola kvality poskytovaných služeb
- BS05_Audit prostředí

Detailní specifikaci, obsah, náležitosti a detailní vymezení provozních parametrů Služeb, včetně vymezení vad, dob a lhůt uvádí Příloha č. 1 této Smlouvy - Katalog služeb a podmínky poskytování bezpečnostního dohledu.

3.2 Předmětem této Smlouvy je dále závazek Objednatele uhradit cenu plnění ve výši a způsobem sjednaným v této Smlouvě.

3.3 Objednatel si vyhrazuje právo provést jednostrannou změnu rozsahu Služeb poskytovaných dle odst. 3.1 této Smlouvy a parametrů těchto Služeb a tomu adekvátní změnu celkové ceny stanovené v odst. 5.1 této Smlouvy, a to při splnění následujících podmínek:

3.3.1 ke změně rozsahu poskytovaných Služeb a jejich parametrů nedojde dříve než po 4 letech od podpisu této Smlouvy,

3.3.2 Objednatel bude o datu změny rozsahu Služeb informovat Poskytovatele s předstihem nejméně 4 (slovy: čtyř) měsíců;

3.3.3 Objednatel vypracuje aktualizovanou Přílohu č. 1 Smlouvy, definující požadovaný rozsah a parametry Služeb;

3.3.4 Na základě aktualizované Přílohy č. 1 Smlouvy navrhne Objednatel novou výši paušální ceny za poskytování Služeb, která vyjde z původní výše paušální ceny a zohlední kvantitativní a kvalitativní změnu poskytovaných Služeb, přičemž nejvýše bude odpovídat ceně v čase a v místě obvyklé. Objednatel je oprávněn pro potřeby posouzení nové výše paušální ceny přizvat soudního znalce a požádat jej o zpracování posudku. Poskytovatel soudnímu znalci poskytne nezbytnou součinnost;

3.3.5 Objednatel navrhne soudního znalce dle odst. 3.3.4 této Smlouvy a písemně jej oznámí Poskytovateli. V případě, že Poskytovatel ze závažných důvodů nebude s navrženým soudním znalcem souhlasit, je oprávněn písemně soudního znalce společně s uvedením těchto závažných důvodů ve lhůtě do 10 dní od přijetí oznámení odmítnout. V takovém případě Objednatel navrhne a písemně Poskytovateli oznámí soudního znalce nového. Poskytovatel je oprávněn písemně odmítnout soudního znalce oznámeného postupem dle tohoto odstavce nejvýše dvakrát;

3.3.6 změna paušální ceny Služeb a aktualizace Přílohy č. 1 Smlouvy bude provedena na základě písemného dodatku k této Smlouvě.

IV. DOBA A MÍSTO PLNĚNÍ

4.1 Poskytovatel se zavazuje zahájit poskytování Služeb na základě výzvy Objednatele a k datu, které Objednatel jednostranně určí, ne však dříve než 7 dní ode dne odeslání výzvy Objednatelem.

4.2 Služby dle odst. 3.1 této Smlouvy bude Poskytovatel plnit od okamžiku stanoveného v odst. 4.1 Smlouvy kontinuálně po celou dobu účinnosti Smlouvy v souladu s podmínkami a termíny stanovenými pro každou Službu v Příloze č. 1 této Smlouvy.

4.3 Nestanoví-li tato Smlouva jinak, je místem plnění "primární lokalita" - datové centrum zajišťované Poskytovatelem služeb Prostředí na adrese Jeremenkova 40b, Olomouc, záložní / testovací / školící lokalita Prostředí a Aplikace MS2014+ na adrese sídla Objednatele (dále též „zálohovací lokalita“ nebo "záložní lokalita") nebo jiné místo, které určí Objednatel nejpozději 30 (slovy: třicet) dní před zahájením plnění Služeb dle odst. 4.1 Smlouvy. Poskytovatel je oprávněn poskytovat části plnění prostřednictvím vzdáleného přístupu v případě, že (i) Objednatel vzdálený přístup schválí a (ii) charakter Služeb jejich plnění prostřednictvím vzdáleného přístupu umožňuje.

V. CENA A PLATEBNÍ PODMÍNKY

5.1 Cena za předmět plnění (Služby) je stanovena dohodou na základě nabídky Poskytovatele následovně:

5.1.1 Celková cena za 1 vyhodnocovací období (zde 1 kalendářní měsíc) činí **507 392,28** Kč (slovy: pět set sedm tisíc tři sta devadesát dvě koruny české dvacet osm haléřů) bez DPH, tj. **613 944,66** Kč (slovy: šest set třináct tisíc devět set čtyřicet čtyři koruny české šedesát šest haléřů) vč. DPH ve výši 21 %.

5.1.2 Celková cena dle odst. 5.1.1 Smlouvy je tvořena součtem paušálních cen za 1 vyhodnocovací období (zde 1 kalendářní měsíc) pro jednotlivé Služby dle Přílohy č. 1 této Smlouvy. Paušální cena za 1 vyhodnocovací období (zde 1 kalendářní měsíc) je pro jednotlivé Služby stanovena následovně:

Služba	Cena za plnění v Kč bez DPH	DPH v Kč	Cena za plnění v Kč včetně DPH
BS01_Informační bezpečnost	78 893,90 Kč	16 567,72 Kč	95 461,61 Kč
BS02_Ochrana osobních údajů	52 208,00 Kč	10 963,68 Kč	63 171,68 Kč
BS03_Bezpečnostní monitoring	282 084,47 Kč	59 237,74 Kč	341 322,21 Kč
BS04_Kontrola kvality poskytovaných služeb	26 300,00 Kč	5 523,00 Kč	31 823,00 Kč
BS05_Audit prostředí	67 905,92 Kč	14 260,24 Kč	82 166,16 Kč

5.2 Veškeré ceny uvedené v odst. 5.1 této Smlouvy jsou cenami maximálními a nejvýše přípustnými. Součástí cen uvedených v odst. 5.1 této Smlouvy jsou veškeré práce, poplatky a veškeré jiné náklady nezbytné pro řádné a úplné poskytování předmětu plnění. Součástí ceny jsou i práce, které v Zadávací dokumentaci nebo této Smlouvě výslovně uvedeny nejsou, ale Poskytovatel jakožto odborník o nich vědět měl nebo mohl vědět, že jsou k řádnému plnění předmětu této Smlouvy nezbytné.

5.3 Veškeré ceny uvedené v odst. 5.1 této Smlouvy jsou ceny v korunách českých. Stane-li se v průběhu trvání smlouvy Česká republika členem Evropské měnové unie a bude-li závazně stanoven koeficient pro přepočet CZK na EUR, budou ceny sjednané v CZK přepočteny na EUR na základě tohoto koeficientu sjednaného v mezinárodních úmluvách, kterými bude Česká republika vázána, jakož i v souladu s případnou tomu odpovídající vnitrostátní právní úpravou České republiky.

5.4 Poskytovatel odpovídá za to, že sazba daně z přidané hodnoty je stanovena v souladu s platnými právními předpisy.

5.5 Veškeré ceny je možné v průběhu plnění Smlouvy změnit pouze z důvodů uvedených v tomto článku Smlouvy.

5.5.1 Prvním důvodem je, že dojde v průběhu plnění ke změnám právních předpisů upravujících výši DPH, nebo jiné daně či povinných poplatků souvisejících s předmětem plnění. Změna smluvní ceny bude odpovídat výši změny daně nebo poplatku.

5.5.2 Druhým důvodem je úprava ceny z důvodu inflace s účinností od 1. 4. kalendářního roku, v němž je úprava provedena.

Inflace je pro účely úpravy ceny vypočítána na základě „míry inflace vyjádřenou přírůstkem průměrného ročního indexu spotřebitelských cen“, kterou pro jednotlivé kalendářní roky vyhlašuje Český statistický úřad (dále jen „roční míra inflace“). Roční míra inflace bude pro účely výpočtu dle této Smlouvy převedena do matematického tvaru 1 + i/100, kde i je přepočítávaná roční míra inflace.

Inflace je vypočítána jako součin ročních měr inflace za po sobě jdoucí zohledněné kalendářní roky. Prvním zohledněným kalendářním rokem je rok, v němž byla uzavřena tato smlouva, a to až do doby, kdy bude provedena první úprava ceny z důvodu inflace. Poté bude prvním zohledněným rokem vždy ten kalendářní rok, v němž byla úprava ceny z důvodu inflace provedena naposledy.

Cena však bude v aktuálním kalendářním roce upravena z důvodu inflace, pouze pokud součin ročních měr inflace za po sobě jdoucí zohledněné kalendářní roky bude 1,05 nebo vyšší.

Změna ceny z důvodu inflace bude provedena tak, že se veškeré ceny uvedené v odst. 5.1, vynásobí součinem ročních měr inflace za po sobě jdoucí zohledněné kalendářní roky a takto získané číslo se zaokrouhlí na celé koruny dle matematických pravidel.

Změna ceny z důvodu inflace je aplikována automaticky, dodatek smlouvy se neuzavírá. Na žádost kterékoli ze smluvních stran však bude písemně potvrzeno aktuální znění odst. 5.1 této Smlouvy.

5.6 Cena za řádně poskytnuté Služby bude Poskytovateli hrazena na základě daňového dokladu – faktury (dále jen „***faktura***“), a to následovně:

5.6.1 U všech Služeb předloží Poskytovatel Objednateli spolu s fakturou seznam, který bude obsahovat rozpis Služeb poskytovaných pracovníky Poskytovatele v člověkodnech v daném vyhodnocovacím období (dále jen „***Výkaz plnění***“). Účelem Výkazu plnění je zásadně pouze dokladovat, že Služba byla poskytnuta

řádně v souladu se všemi požadavky této Smlouvy, neboť ceny Služeb dle odst. 5.1 této Smlouvy jsou sjednány jako ceny paušální a nepřekročitelné, ledaže by zvláštní ustanovení této Smlouvy stanovilo jinak.

5.6.2 V případě, že Služby byly poskytovány pouze část vyhodnocovacího období, bude za příslušné vyhodnocovací období uhrazena pouze poměrná část paušální ceny.

5.6.3 Objednatel může odmítnout schválení Výkazu plnění, který nemá požadované přílohy. Přílohou Výkazu plnění budou Objednatelem akceptované ***Protokoly o poskytnuté službě*** v rozsahu a obsahu definovaném pro každou Službu Přílohou č. 1 této Smlouvy.

5.6.4 Objednatel je povinen ve lhůtě splatnosti dané faktury přiložený Výkaz plnění schválit nebo uvést, ve které části neodpovídá skutečnosti, a nebo uplatnit nárok jeho úpravu postupem dle této Smlouvy. Uvede-li Objednatel ve stanovené lhůtě připomínky k Výkazu plnění, zahájí smluvní strany jednání o jejich bezodkladném vyřešení.

5.6.5 Cena za poskytnuté plnění dle této Smlouvy bude Objednatelem hrazena na základě faktury vystavené nejdříve k pátému pracovnímu dni kalendářního měsíce následujícího po měsíci, v němž bylo plnění dle této Smlouvy poskytováno, přičemž jejím podkladem bude Výkaz plnění schválený Objednatelem. Uvedl-li Objednatel své připomínky k Výkazu plnění, Poskytovatel není oprávněn do jejich vyřešení fakturovat odměnu za rozporované plnění, je však oprávněn Výkaz plnění použít jako podklad pro fakturaci v rozsahu, který nebyl Objednatelem zpochybněn. Poskytovatel je povinen původní, rozporovanou fakturu stornovat a následně je Poskytovatel oprávněn vystavit fakturu na cenu nerozporovaného plnění dle této Smlouvy a cenu rozporovaného plnění bude oprávněn fakturovat až po jeho vzájemném vyřešení v souladu s dohodou dosaženou v této věci s Objednatelem.

5.6.6 Smluvní strany pro vyloučení pochybností stanoví, že nedojde-li k akceptaci výsledku poskytovaného plnění, vzniká Objednateli nárok na vrácení ceny za takové plnění, přičemž zápočet ze strany Objednatele se připouští.

5.7 Poskytovatel se zavazuje ve faktuře a Výkazu plnění vždy zohlednit a výslovně uvést a řádně vyčíslit příslušný nárok Objednatele na slevu z ceny či smluvní pokuty dle článku XIV této Smlouvy a odpovídajícím způsobem snížit cenu.

5.8 Lhůta splatnosti fakturovaných částek je stanovena na třicet (30) kalendářních dní od doručení faktury Objednateli. Poskytovatel se zavazuje odeslat fakturu Objednateli nejpozději následující pracovní den po jejím vystavení. V případě, že má lhůta splatnosti faktury uplynout v období od 16. do 31. prosince, bude se za poslední den lhůty splatnosti takovéto faktury považovat první pracovní den po skončení uvedeného období. Faktura

bude doručena doporučenou listovní zásilkou, datovou schránkou nebo osobně pověřenému zaměstnanci Objednatele proti písemnému potvrzení převzetí. Totožná lhůta splatnosti je stanovena i pro placení jiných plateb dle této Smlouvy (smluvních pokut, úroků z prodlení, náhrady škody apod.).

5.9 Všechny faktury musí splňovat náležitosti řádného daňového dokladu požadované zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, avšak výslovně vždy musí obsahovat následující údaje:

- označení smluvních stran a jejich adresy,
- IČ, DIČ (je-li přiděleno),
- údaj o tom, že vystavovatel faktury je zapsán v obchodním rejstříku včetně spisové značky,
- číslo této Smlouvy v CES a datum jejího uzavření,
- pojmenování akce, ke které se Faktura vztahuje, ve znění: „Zajištění služeb Bezpečnostního dohledu pro MS2014+“,
- registrační číslo projektu dle OPTP: CZ.1.08/2.1.00/13.00167“, se zvýrazněným textem „OPTP 2007-2013“,
- identifikace poskytnutého plnění,
- číslo faktury,
- den vystavení a lhůtu splatnosti faktury,
- označení peněžního ústavu a číslo účtu, na který se má platit,
- fakturovanou částku,
- razítko a podpis oprávněné osoby, která fakturu vystavila, včetně kontaktního telefonu,
- přílohou faktury musí být vždy Výkaz plnění.

Dle § 435 ObčZ je Poskytovatel po vzniku práva fakturovat povinen vystavit a Objednateli předat Fakturu ve dvou vyhotoveních.

5.10 Nebude-li faktura obsahovat stanovené náležitosti a přílohy, nebo v ní nebudou správně uvedené údaje dle této Smlouvy (zejména nezohlednění slev z ceny a/nebo smluvních pokut dle článku XIV této Smlouvy), je Objednatel oprávněn vrátit ji ve lhůtě její splatnosti Poskytovateli. V takovém případě se přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury.

5.11 Platby peněžitých částek se provádí bankovním převodem na účet druhé smluvní strany uvedený ve faktuře. Peněžitá částka se považuje za zaplacenou okamžikem jejího

odepsání z účtu odesílatele ve prospěch účtu příjemce. Poskytovatel není oprávněn nárokovat bankovní poplatky nebo jiné náklady vztahující se k převodu poukazovaných částek mezi Smluvními stranami na základě této Smlouvy.

5.12 V případě prodlení kterékoliv smluvní strany se zaplacením peněžité částky vzniká oprávněné straně nárok na úrok z prodlení dle občanskoprávních předpisů. Tím není dotčen ani omezen nárok na náhradu vzniklé škody.

5.13 Objednatel neposkytuje Poskytovateli na předmět plnění této Smlouvy jakékoliv zálohy.

VI. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

6.1 Poskytovatel se zavazuje:

6.1.1 při poskytování Služeb dle této Smlouvy postupovat v profesionální kvalitě a s odbornou péčí, podle nejlepších znalostí a schopností, aplikovat procesy „best practice“, sledovat a chránit oprávněné zájmy Objednatele; dostane-li se Poskytovatel do prodlení s povinností poskytovat Služby řádně bez zavinění Objednatele či v důsledku okolností vylučujících odpovědnost za škodu po dobu delší pěti (5) kalendářních dnů, je Objednatel oprávněn zajistit plnění dle této Smlouvy po dobu prodlení Poskytovatele jinou osobou; v takovém případě nese náklady spojené s náhradním plněním Poskytovatel;

6.1.2 poskytovat Služby řádně a včas, a to bez faktických a právních vad a v kvalitě definované v jednotlivých Service Level Agreements (dále jen „SLA“), které jsou stanoveny v Příloze č. 1 této Smlouvy a/nebo v rozsahu odpovídajícím popisu jednotlivých dílčích Služeb a závazných činností definovaných pro jednotlivé dílčí Služby a další plnění v Příloze č. 1 této Smlouvy v případě, že daná dílčí Služba nemá definované SLA;

6.1.3 upozorňovat Objednatele včas na všechny hrozící vady či potenciální výpadky plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro plnění Smlouvy nezbytné;

6.1.4 informovat bezodkladně Objednatele o jakýchkoliv zjištěných překážkách plnění, byť by za ně Poskytovatel neodpovídal, o vznesených požadavcích orgánů státního dozoru a o uplatněných nárocích třetích osob, které by mohly plnění této Smlouvy ovlivnit;

6.1.5 na své náklady a s péčí řádného hospodáře podporovat, spravovat a udržovat veškeré technické prostředky Objednatele, které Poskytovatel převzal v souvislosti s touto Smlouvou;

6.1.6 neprodleně oznámit písemnou formou Objednateli překážky, které mu brání v plnění předmětu Smlouvy a výkonu dalších činností souvisejících s plněním předmětu Smlouvy;

6.1.7 neprodleně písemně oznámit Objednateli změny svého majetkoprávního postavení, jako je např. přeměna společnosti, snížení základního kapitálu, vstup do likvidace, úpadek či prohlášení konkurzu apod.;

6.1.8 upozornit Objednatele na potenciální rizika vzniku škod a včas a řádně dle svých možností provést taková opatření, která riziko vzniku škod zcela vyloučí nebo dostatečně sníží;

6.1.9 i bez pokynů Objednatele provést neodkladně nutné úkony, které, ač nejsou předmětem této Smlouvy, pokud budou s ohledem na nepředvídané okolnosti pro plnění Smlouvy nezbytné nebo jsou nezbytné pro zamezení vzniku škody; jde-li o zamezení vzniku škod nezapříčiněných Poskytovatelem, má Poskytovatel právo na úhradu nezbytných a účelně vynaložených nákladů; Poskytovatel však zároveň bez zbytečného odkladu informuje Objednatele o nutnosti provést neodkladně nutné úkony;

6.1.10 dodržovat bezpečnostní, hygienické, požární, organizační a ekologické předpisy na pracovištích Objednatele, se kterými byl seznámen nebo které jsou všeobecně známé, a dále zajistit, aby i všechny osoby podílející se na plnění jeho závazků z této Smlouvy, které se budou zdržovat v prostorách nebo na pracovištích Objednatele, dodržovaly účinné právní předpisy o bezpečnosti a ochraně zdraví při práci a veškeré interní předpisy Objednatele, s nimiž Objednatel Poskytovatele předem obeznámil nebo které jsou všeobecně známé;

6.1.11 informovat Objednatele o plnění svých povinností podle této Smlouvy a o důležitých skutečnostech, které mohou mít vliv na výkon práv a plnění povinností smluvních stran;

6.1.12 chránit práva duševního vlastnictví Objednatele a třetích osob;

6.1.13 upozorňovat Objednatele na možné či vhodné rozšíření či změny Služeb za účelem jejich lepšího využívání v rozsahu této Smlouvy;

6.1.14 upozorňovat Objednatele v odůvodněných případech na případnou nevhodnost pokynů Objednatele;

6.1.15 vypracovávat a Objednateli doručovat přehledné a kompletní ***Protokoly o poskytnuté službě*** (viz Příloha č. 1 této Smlouvy), ze kterých musí jednoznačně vyplývat, zda byly Služby poskytovány v kvalitě definované v jednotlivých SLA dle této Smlouvy (a není-li pro určitou Službu či další plnění dle této Smlouvy SLA definováno, zda splňuje specifikaci Služby sjednanou v této Smlouvě). Protokoly musí odpovídat skutečnosti. Protokoly budou vypracovávány vždy pro vyhodnocovací období uvedené pro danou Službu a další plnění dle této Smlouvy (dále jen „Vyhodnocovací období“) a budou Objednateli doručeny nejpozději do pěti (5) pracovních dnů od ukončení daného Vyhodnocovacího období. Není-li délka Vyhodnocovacího období uvedena v této Smlouvě (resp. její Příloze č. 1), platí, že jeho délka je jeden (1) kalendářní měsíc.

6.2 Objednatel se zavazuje poskytnout ke splnění smluvních závazků Poskytovatele účelnou součinnost, dokumentaci a informace definované v této Smlouvě nebo potřebné pro

účelné plnění předmětu této Smlouvy, a dále bude odpovědné zástupce Poskytovatele včas informovat o všech organizačních změnách, poznatcích z kontrolní činnosti, podnětech vlastních zaměstnanců a dalších skutečnostech významných pro plnění předmětu Smlouvy.

6.3 Poskytovatel je povinen zajistit plnění Služeb prostřednictvím osob, které mají potřebnou kvalifikaci i zkušenosti k plnění svých úkolů. Poskytovatel je povinen zajistit plnění příslušné části Služeb pomocí osob, jejichž prostřednictvím prokázal splnění kvalifikace v zadávacím řízení Veřejné zakázky a nebo je uvedl jako členy týmů v rámci své nabídky na Veřejnou zakázku (viz Příloha č. 5 této Smlouvy). Poskytovatel je oprávněn změnit osobu, jejímž prostřednictvím prokazoval splnění kvalifikace v zadávacím řízení Veřejné zakázky, pouze s předchozím písemným souhlasem Objednatele a je povinen takovou osobu vždy nahradit osobou s minimálně stejnou kvalifikací, jakou disponovala původní osoba uvedená v nabídce Poskytovatele. U osob, kterými Poskytovatel neprokazoval splnění kvalifikace a pouze je uvedl jako členy týmu do Přílohy č. 5 této Smlouvy, je Poskytovatel povinen zajistit a udržovat stejnou úroveň kvalifikace a zkušeností, jaká byla na danou roli požadována pro splnění kvalifikace v zadávacím řízení Veřejné zakázky. Objednatel je oprávněn kontrolovat u Poskytovatele splnění této povinnosti kdykoliv v průběhu trvání této Smlouvy.

6.4 Poskytovatel je povinen písemně informovat Objednatele o všech svých subdodavatelích (včetně jejich identifikačních a kontaktních údajů a o tom, které Služby dle této Smlouvy pro něj v rámci předmětu plnění každý ze subdodavatelů poskytuje) a o jejich změně, a to nejpozději do 7 (slovy: sedmi) kalendářních dnů ode dne, kdy Poskytovatel vstoupil se subdodavatelem ve smluvní vztah či ode dne, kdy nastala změna. Poskytovatel je oprávněn změnit subdodavatele, pomocí něhož prokázal část splnění kvalifikace v rámci zadávacího řízení Veřejné zakázky jen z vážných objektivních důvodů a s předchozím písemným souhlasem Objednatele, přičemž nový subdodavatel musí disponovat kvalifikací ve stejném či větším rozsahu, který původní subdodavatel prokázal za Poskytovatele. Objednatel nesmí souhlas se změnou subdodavatele bez objektivních důvodů odmítnout, pokud mu budou příslušné doklady v ujednané lhůtě předloženy. Tím není dotčena výlučná odpovědnost Poskytovatele za poskytování řádného plnění dle této Smlouvy.

6.5 Poskytovatel je povinen udržovat po celou dobu účinnosti této Smlouvy v platnosti veškeré certifikáty a osvědčení stanovené v Zadávací dokumentaci pro prokázání splnění kvalifikace Poskytovatele.

6.6 Poskytovatel je povinen za účelem ověření plnění svých povinností vytvořit podmínky subjektům oprávněných dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, k provedení kontroly vztahující se k realizaci předmětu plnění této Smlouvy, poskytnout

oprávněným osobám veškeré doklady vztahující se k realizaci plnění, umožnit průběžné ověřování souladu údajů o realizaci plnění a poskytnout součinnost všem osobám oprávněným k provádění kontroly, včetně toho, že se Poskytovatel podrobí této kontrole a bude působit jako osoba povinná ve smyslu ust. § 2 písm. e) uvedeného zákona. Těmito oprávněnými osobami jsou Objednatel, Ministerstvo financí České republiky, Ministerstvo pro místní rozvoj České republiky, Centrum pro regionální rozvoj, Evropská komise, Evropský účetní dvůr, Nejvyšší kontrolní úřad, příslušný finanční úřad, Evropský úřad pro boj proti podvodům (OLAF), případně další orgány oprávněné k výkonu kontroly.

6.7 Poskytovatel se zavazuje umožnit osobám oprávněným k výkonu kontroly Projektu provést kontrolu dokladů souvisejících s plněním předmětu Smlouvy, a to po dobu nejméně 10 (slovy: deset) let od ukončení financování předmětu Smlouvy způsobem, který je v souladu s platnými právními předpisy České republiky a Evropských společenství.

6.8 Poskytovatel je povinen na své náklady řádně uchovávat veškerou dokumentaci související s realizací předmětu plnění této Smlouvy, včetně účetních dokladů, v souladu s předpisy Evropských společenství (příslušné Nařízení Rady (ES)) minimálně do 10 (slovy: deseti) let od ukončení financování předmětu Smlouvy. Pokud je v českých právních předpisech stanovena lhůta delší než v evropských předpisech, musí být pro úschovu použita delší lhůta. Každý originální účetní doklad musí obsahovat informaci, že se jedná o projekt spolufinancovaný z operačního programu, z jehož aktivit jsou požadované Služby financovány a musí být označen číslem Projektu daného operačního programu.

6.9 Poskytovatel je dále povinen do 10 (slovy: deseti) let od ukončení financování předmětu Smlouvy za účelem ověřování plnění povinností vyplývajících z podmínek daného operačního programu, z něhož bude zajištěno spolufinancování předmětu plnění Smlouvy, poskytovat požadované informace a dokumentaci zaměstnancům nebo zmocněncům pověřených orgánů (Ministerstvo pro místní rozvoj České republiky, Centrum pro regionální rozvoj, Ministerstvo financí České republiky, Evropská komise, Evropský účetní dvůr, Evropský úřad pro boj proti podvodům (OLAF), Nejvyšší kontrolní úřad, příslušný finanční úřad a další oprávněné orgány státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly, vztahující se k realizaci této Smlouvy a poskytnout jim při provádění kontroly součinnost.

6.10 Poskytovatel je povinen poskytnout Objednateli veškerou součinnost při provádění informačních a propagačních opatření na základě příslušných Nařízení Komise (ES), které se budou vztahovat k informačním a propagačním opatřením pro programové období 2014-2020, a v souladu s pravidly stanovenými v budoucí Příručce pro žadatele a příjemce v operačním programu, z něhož bude zajištěno spolufinancování předmětu plnění

Smlouvy a které budou uvedeny na webu operačního programu, a kde mimo jiné bude stanovena odpovědnost příjemců, pokud jde o informační a propagační opatření pro veřejnost. Poskytovatel je povinen se se shora uvedenými pravidly seznámit neprodleně poté, co bude Objednatelem v souladu s odst. 2.2 Smlouvy písemně informován o příslušném operačním programu, přičemž se musí řídit vždy pouze aktuálními pravidly. Součinnost dle tohoto odst. 6.10 Smlouvy poskytuje Poskytovatel bezplatně. Objednatel se zavazuje, že Poskytovateli bez zbytečného odkladu písemně sdělí veškeré nezbytné informace a podklady, které se budou vztahovat k součinnosti při provádění informačních a propagačních opatření na základě příslušného Nařízení Komise (ES) pro programové období 2014-2020.

6.11 Poskytovatel je povinen všechny písemné zprávy, písemné výstupy či případné prezentace související s plněním předmětu této Smlouvy opatřit vizuální identitou Projektu dle pravidel příslušného operačního programu, ze kterého se aktivity financují dle odst. 6.10 této Smlouvy, a to od okamžiku písemného oznámení těchto pravidel Objednatelem. V případě, že v průběhu plnění této Smlouvy dojde ke změně těchto pravidel, je Objednatel povinen o této skutečnosti Poskytovatele bezodkladně informovat.

6.12 Poskytovatel je povinen zajistit, aby povinnosti dle odst. 6.6 až 6.11 tohoto článku Smlouvy plnili do 10 (slovy: deseti) let od ukončení financování předmětu Smlouvy také jeho případní subdodavatelé podílející se na realizaci plnění či jeho dílčí části.

6.13 Poskytovatel je povinen Objednateli poskytnout veškerou nezbytnou součinnost k naplnění účelu této Smlouvy.

6.14 Poskytovatel je povinen na žádost Objednatele spolupracovat či poskytnout součinnost případným dalším dodavatelům Objednatele, zejména Provozovateli Aplikace MS2014+, Poskytovateli služeb Prostředí a Technickému dozoru.

6.15 Objednatel je rovněž oprávněn spolupracovat při provádění dohledu nad stavem plnění dle této Smlouvy s vybranou, nezávislou, odborně erudovanou třetí osobou (neuvedenou v čl. 6.14) pro zajištění odborné garance řádného plnění na straně Objednatele. Poskytovatel je povinen plně respektovat postavení takové třetí osoby, spolupracovat s ní a poskytnout jí maximální součinnost dle pokynů Objednatele.

6.16 S ohledem na povinnosti Smluvních stran uložené jim § 147a ZVZ se Poskytovatel rovněž zavazuje:

6.16.1 předložit Objednateli v průběhu plnění této Smlouvy každý rok vždy k 28. únoru písemný seznam subdodavatelů, ve kterém uvede subdodavatele, jimž za plnění subdodávky uhradil více než 10% z celkové částky uhrazené mu na základě této Smlouvy za uplynulý kalendářní rok. Má-li subdodavatel uvedený v seznamu formu akciové společnosti, bude přílohou seznamu i seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10% základního kapitálu,

vyhotovený ve lhůtě 90 dnů před dnem předložení seznamu subdodavatelů. Poskytovatel předkládá seznam subdodavatelů i tehdy, pokud v nabídce uvedl, že nezamýšlí zadat část(i) Veřejné zakázky jinému subjektu;

6.16.2 předložit Objednateli do 60 dnů od splnění této Smlouvy seznam subdodavatelů, ve kterém uvede subdodavatele, jimž za plnění subdodávky uhradil více než 10% z celkové částky uhrazené mu na základě této Smlouvy za celou dobu jejího trvání. Má-li subdodavatel uvedený v seznamu formu akciové společnosti, bude přílohou seznamu i seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10 % základního kapitálu, vyhotovený ve lhůtě 90 dnů před dnem předložení seznamu subdodavatelů. Poskytovatel předkládá seznam subdodavatelů i tehdy, pokud v nabídce uvedl, že nezamýšlí zadat část(i) Veřejné zakázky jinému subjektu.

6.17 Poskytovatel je povinen ke dni podpisu této Smlouvy a následně po celou dobu až do ukončení poskytování plnění dle této Smlouvy splňovat požadavky na nezávislost, která je Objednatelem požadována pro výkon kontrolní role Poskytovatele a vyplývá z požadovaného rozsahu a obsahu Služeb (viz Příloha č. 1 této Smlouvy) a nepřípustnosti stavu, kdy by fyzická nebo právnická osoba kontrolovala plnění a kvalitu plnění sama sobě, osobě ze stejného podnikatelského seskupení nebo svým obchodním partnerům na základě dále definovaných smluvních vztahů. Poskytovatel se proto zavazuje, že on sám, osoby tvořící s ním stejné podnikatelské seskupení či jiná fyzická nebo právnická osoba uvedená v rámci této Smlouvy, zejména v její Příloze č. 2 a Příloze č. 5, nebude poskytovat Služby dle této Smlouvy, zejména pokud:

6.17.1 byl/byla vybrána jako vítězný uchazeč v rámci zadávacího řízení "Pořízení aplikace MS2014+ a zajištění jejího provozu a rozvoje" a nebo je pracovníkem/zaměstnancem vítězného uchazeče (nebo osobou v obdobném postavení) a nebo je subdodavatelem vítězného uchazeče anebo je pracovníkem/zaměstnancem tohoto subdodavatele (nebo osobou v obdobném postavení) a aktuálně na základě platné smlouvy poskytuje Objednateli plnění při realizaci veřejné zakázky "Pořízení aplikace MS2014+ a zajištění jejího provozu a rozvoje",

6.17.2 byl/byla vybrána jako vítězný uchazeč v rámci zadávacího řízení "Pořízení HW platformy a Infrastruktury serverovny pro MS2014+" a nebo je pracovníkem/zaměstnancem vítězného uchazeče (nebo osobou v obdobném postavení) a nebo je subdodavatelem vítězného uchazeče anebo je pracovníkem/zaměstnancem tohoto subdodavatele (nebo osobou v obdobném postavení) a aktuálně na základě platné smlouvy poskytuje Objednateli plnění při realizaci veřejné zakázky "Pořízení HW platformy a Infrastruktury serverovny pro MS2014+".

6.18 Splněním této Smlouvy se rozumí zejména:

6.18.1 den, kdy nastaly právní účinky výpovědi dle odst. 15.2 této Smlouvy, bez ohledu na to, která ze Smluvních stran tuto Smlouvu vypověděla;

6.18.2 den, kdy nastaly právní účinky odstoupení dle odst. 15.2 této Smlouvy, bez ohledu na to, která ze Smluvních stran od této Smlouvy odstoupila.

VII. ZMĚNOVÉ ŘÍZENÍ

7.1 Kterákoliv ze smluvních stran je oprávněna písemně navrhnout změnu způsobu poskytování Služeb. Žádná ze smluvních stran však není povinna navrhovanou změnu akceptovat.

7.2 Poskytovatel se zavazuje provést hodnocení dopadů kteroukoliv smluvní stranou navrhovaných změn Služeb na termíny plnění, cenu a součinnost Objednatele. Poskytovatel je povinen toto hodnocení provést bez zbytečného odkladu, nejpozději do deseti (10) pracovních dnů ode dne doručení návrhu kterékoliv smluvní strany druhé smluvní straně.

7.3 Jakékoliv změny Služeb či jejich poskytování musí být sjednány v souladu se ZVZ a písemně ve formě dodatku k této Smlouvě podepsaného osobami oprávněnými zavazovat smluvní strany, nestanoví-li tato Smlouva jinak. V závislosti na těchto písemných ujednáních může být upraven požadovaný rozsah plnění, termíny plnění, cena Služeb, platební podmínky, součinnost Objednatele atd.

VIII. AKCEPTACE VÝSLEDKŮ POSKYTOVANÉHO PLNĚNÍ

8.1 Výsledky poskytnutého plnění dle této Smlouvy budou akceptovány Objednatelem na základě akceptační procedury.

8.2 Náležitosti akceptační procedury jsou upraveny v rámci popisu jednotlivých Služeb, který je blíže specifikován v Příloze č. 1 této Smlouvy. V případě, že tato příloha nespecifikuje náležitosti akceptační procedury, uplatní se akceptační procedura dle článku 8.3 dále.

8.3 Akceptační procedura zahrnuje ověření, zda poskytnuté plnění dle této Smlouvy vedlo k výsledku, ke kterému se smluvní strany zavázaly touto Smlouvou, a to porovnáním skutečných vlastností jednotlivých dílčích výsledků plnění (výstupů) poskytnutých dle této Smlouvy s jejich specifikací uvedenou v této Smlouvě.

8.3.1 Poskytovatel se zavazuje průběžně konzultovat práce na přípravě/zhotovení výstupu s Objednatelem.

8.3.2 Poskytovatel se zavazuje předat první verzi výstupu (např. dokumentu) Objednateli k akceptaci ve lhůtě domluvené mezi Poskytovatelem a Objednatelem na základě této Smlouvy, nebo jinak stanovené v souladu s touto Smlouvou. V pochybnostech má přednost lhůta, která byla za součinnosti obou smluvních stran v souladu s touto Smlouvou stanovena později.

8.3.3 Objednatel se zavazuje vznést veškeré své výhrady nebo připomínky k první verzi výstupu předložené dle článku 8.3.2 do patnácti (15) pracovních dnů od jeho doručení. Nevznese-li Objednatel ve stanovené lhůtě k první verzi výstupu žádné výhrady ani připomínky, považují smluvní strany výstup ve znění jeho první verze za Poskytovatelem řádně předaný a Objednatelem řádně převzatý.

8.3.4 Vznese-li Objednatel ve stanovené lhůtě výhrady nebo připomínky k první verzi výstupu, zavazuje se Poskytovatel bez zbytečného odkladu, avšak nejpozději do deseti (10) kalendářních dnů provést veškeré potřebné úpravy výstupu dle výhrad a připomínek Objednatele a takto upravený výstup předat jako jeho druhou verzi Objednateli k akceptaci.

8.3.5 Objednatel se zavazuje vznést veškeré své výhrady nebo připomínky k druhé verzi výstupu předložené dle článku 8.3.4 výše do patnácti (15) pracovních dnů od jejího doručení. Nevznese-li Objednatel ve stanovené lhůtě k druhé verzi výstupu žádné výhrady ani připomínky, považují smluvní strany výstup ve znění jeho druhé verze za Poskytovatelem řádně předaný a Objednatelem řádně převzatý.

8.3.6 Vznese-li Objednatel ve stanovené lhůtě své výhrady nebo připomínky k druhé verzi výstupu, zavazují se smluvní strany zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a akceptace výstupu, a to nejpozději do pěti (5) pracovních dnů od doručení výzvy kterékoliv smluvní strany k jednání.

8.3.7 Smluvní strany se zavazují po řádném předání a převzetí výstupu dle článků 8.3.3, 8.3.5 a 8.3.6 potvrdit toto předání a převzetí sepsáním písemného protokolu příslušného dané Službě, který za smluvní strany podepíší oprávněné osoby nejpozději do tří (3) pracovních dnů od řádného předání a převzetí výstupu. protokol jednotlivých výstupů musí být podepsán osobami oprávněnými jednat za smluvní strany (statutární orgán, člen statutárního orgánu apod.) nebo osobami, které k tomu smluvní strany výslovně písemně zmocnily.

8.3.8 Bude-li trvání akceptační procedury ovlivněné vznesením případných výhrad nebo připomínek k výstupu a potřebou jejich vyřešení, nebude to mít vliv na dohodnuté termíny pro předání výstupu.

8.3.9 Plnění Poskytovatele dle této Smlouvy budou považována za poskytnutá po akceptaci jejich výsledků v souladu s tímto článkem VIII. Včasnou akceptací výsledků všech řádně poskytnutých plnění Poskytovatelem dle této Smlouvy se předmětný závazek Poskytovatele stanovený touto Smlouvou považuje za splněný.

IX. ODPOVĚDNOST ZA ŠKODU, ODPOVĚDNOST ZA VADY, ZÁRUKA

9.1 Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a této Smlouvy. Poskytovatel odpovídá za škodu rovněž v případě, že část Služeb poskytuje prostřednictvím subdodavatele.

9.2 Žádná ze Smluvních stran není odpovědná za škodu nebo prodlení způsobené okolnostmi vylučujícími odpovědnost ve smyslu ObčZ. Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost a bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.

9.3 Poskytovatel se zavazuje, že bude mít po celou dobu účinnosti této Smlouvy sjednánu pojistnou smlouvu, která se vztahuje na plnění předmětu této Smlouvy o poskytování služeb a jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem třetí osobě s limitem pojistného plnění na jednu škodnou událost minimálně 10.000.000,- Kč (slovy: deset milionů korun českých) s výší spoluúčasti maximálně 10 % (slovy: deset procent). Poskytovatel je povinen předložit kopii pojistné smlouvy na vyžádání Objednateli.

9.4 V případě, že činností případně nečinností Poskytovatele dojde ke způsobení škody Objednateli nebo třetím osobám, která nebude kryta pojištěním odpovědnosti dle odst. 9.3 této Smlouvy, bude Poskytovatel povinen škodu uhradit z vlastních prostředků.

9.5 Poskytovatel je odpovědný za to, že poskytnuté Služby jsou v souladu se Zadávací dokumentací a touto Smlouvou, a že po dobu záruční doby budou mít dohodnuté vlastnosti, úroveň a charakteristiky. Záruční doba na Služby dle odst. 3.1 Smlouvy činí 90 (slovy: devadesát) dnů ode dne jejich poskytnutí.

9.6 Poskytovatel je povinen plnit Služby v nejvyšší dostupné kvalitě a odpovídá za to, že případné vady plnění poskytnutého dle této Smlouvy zjištěné v záruční době řádně odstraní, případně nahradí plněním bezvadným, v souladu s touto Smlouvou.

9.7 Pokud Objednatel zjistí vady poskytovaného plnění dle této Smlouvy, je povinen oznámit takové vady Poskytovateli způsobem stanoveným v této Smlouvě a Poskytovatel takové vady odstraní v souladu s touto Smlouvou.

9.8 Pokud v důsledku porušení povinností Poskytovatele stanovených touto Smlouvou nebude Objednateli uhrazen finanční podíl operačního programu věcně příslušného této aktivitě na Projektu, případně bude Objednateli v důsledku porušení povinností Poskytovatele zkrácena výše této dotace, bude Poskytovatel povinen uhradit Objednateli takto vzniklou škodu (celý podíl z operačního programu na Projektu, případně zkrácenou výši dotace, kterou Objednatel písemně sdělí Poskytovateli) a to do 30 (slovy: třiceti) kalendářních dnů ode dne doručení písemného sdělení Poskytovateli nebude-li Smluvními stranami dohodnuto jinak.

X. VLASTNICKÉ PRÁVO A PRÁVO UŽITÍ

10.1 V případě, že součástí plnění Poskytovatele podle této Smlouvy budou movité věci předávané Objednateli, nabývá Objednatel vlastnické právo k těmto věcem dnem převzetí takového plnění Objednatelem na základě písemného protokolu podepsaného oprávněnými osobami obou smluvních stran. Nebezpečí škody na předaných věcech přechází na Objednatele okamžikem jejich faktického převzetí do dispozice Objednatele, o takovémto převzetí musí být sepsán písemný záznam podepsaný oprávněnými osobami stran. Do nabytí vlastnického práva uděluje Poskytovatel Objednateli právo tyto věci užívat v rozsahu a způsobem, který vyplývá z účelu této Smlouvy.

10.2 Bude-li součástí výstupu (Služeb) nebo výsledkem činnosti Poskytovatele prováděné dle této Smlouvy předmět požívající ochrany autorského díla podle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „***autorské dílo***“), nabývá Objednatel dnem poskytnutí autorského díla Objednateli k užívání nevýhradní právo užít

takovéto autorské dílo všemi způsoby nezbytnými k naplnění účelu vyplývajícímu z této Smlouvy, a to po celou dobu trvání autorského práva k autorskému dílu, resp. po dobu autorskoprávní ochrany, bez omezení rozsahu množstevního, technologického, teritoriálního (dále jen „***Licence***"). Součástí Licence je rovněž neomezené právo Objednatele poskytnout třetím osobám podlicenci k užití autorského díla v rozsahu shodném s rozsahem Licence, souhlas Poskytovatele k postoupení Licence na třetí osoby a souhlas Poskytovatele udělený Objednateli k provedení jakýchkoliv změn nebo modifikací autorského díla, a to i prostřednictvím třetích osob. Licence se automaticky vztahuje i na všechny nové verze, aktualizované verze, i na úpravy a překlady autorského díla dodané Poskytovatelem. Poskytovatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorskému dílu a že má souhlas autorů k uzavření těchto licenčních ujednání a že toto prohlášení zahrnuje i taková práva autorů, která by vytvořením autorského díla teprve vznikla.

10.3 Poskytuje-li Poskytovatel Licenci k počítačovým programům vyvíjeným Poskytovatelem, vztahuje se ve stejném rozsahu k počítačovým programům ve zdrojovém a strojovém kódu, jakož i ke koncepčním přípravným materiálům. Poskytovatel se zavazuje v případě, že se Licence vztahuje k počítačovým programům, poskytnout Objednateli zdrojové kódy s komentáři takových počítačových programů a koncepční přípravné materiály (zahrnující zejména analýzy a technické designy) a tyto v případě změny průběžně aktualizovat a poskytovat i dokumentaci provedených změn. Poskytovatel se dále zavazuje předat Objednateli aktuální dokumentované zdrojové kódy a koncepční přípravné materiály všech počítačových programů do třiceti (30) kalendářních dnů od skončení účinnosti této Smlouvy.

10.4 Smluvní strany výslovně prohlašují, že pokud při poskytování plnění dle této Smlouvy vznikne činností Poskytovatele a Objednatele dílo spoluautorů a nedohodnou-li se smluvní strany výslovně jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Poskytovatel udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena Služeb (odměna Poskytovatele) je stanovena se zohledněním tohoto ustanovení a Poskytovateli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.

10.5 Poskytovatel je povinen postupovat tak, aby udělení Licence k autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci zabezpečil, a to bez újmy na právech třetích osob. Nebude-li možné po Poskytovateli spravedlivě požadovat udělení Licence v rozsahu dle článku 10.2 výše, zejména proto, že se jedná o tzv. standardní počítačové programy, je Poskytovatel povinen na to písemně Objednatele upozornit spolu s náležitým odůvodněním a poskytnout Objednateli nebo zajistit pro Objednatele poskytnutí licence či podlicence v nejširším možném rozsahu. Postup dle předchozí věty

je možný jen s výslovným písemným souhlasem Objednatele, přičemž se Objednatel zavazuje, že tento souhlas neodmítne poskytnout bez vážného důvodu.

10.6 Bude-li autorské dílo vytvořeno činností Poskytovatele, smluvní strany činí nesporným, že jakékoliv takovéto autorské dílo vzniklo z podnětu a pod vedením Objednatele.

10.7 Práva získaná v rámci plnění této Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Poskytovatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Poskytovatelem Objednateli.

10.8 Odměna za poskytnutí, zprostředkování nebo postoupení Licence k autorskému dílu je zahrnuta v ceně Služeb, při jejichž poskytnutí došlo k vytvoření autorského díla.

XI. OCHRANA OSOBNÍCH ÚDAJŮ A DŮVĚRNÝCH INFORMACÍ

11.1 Ochrana osobních údajů a důvěrných informací je upravena samostatnou „Smlouvou o dodržování bezpečnostních opatření v rámci spolupráce“, kterou uzavřely Smluvní strany před podpisem této Smlouvy. Smluvní strany se vzájemně zavazují udržovat „Smlouvu o dodržování bezpečnostních opatření v rámci spolupráce“ platnou a účinnou po celou dobu trvání účinnosti této Smlouvy.

11.2 Vzhledem k veřejnoprávnímu charakteru Objednatele Poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen, že žádné z ustanovení této Smlouvy ani jejích příloh nepodléhá z jeho strany obchodnímu tajemství a souhlasí se zveřejněním smluvních podmínek obsažených v této Smlouvě včetně příloh v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zák. č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a ustanovení § 147a ZVZ.

XII. OZNÁMENÍ A KOMUNIKACE

12.1 Veškerá oznámení, tj. jakákoliv komunikace na základě této Smlouvy, bude probíhat v souladu s tímto článkem Smlouvy. Jakékoli oznámení, žádost či jiné sdělení, jež má být učiněno či dáno Smluvní straně dle této Smlouvy, bude učiněno či dáno písemně. Kromě jiných způsobů komunikace dohodnutých mezi Smluvními stranami se za účinné považují osobní doručování, doručování doporučenou poštou, kurýrní službou či datovou schránkou, a to na adresy Smluvních stran uvedené v záhlaví Smlouvy, nebo na takové adresy, které si Smluvní strany vzájemně písemně oznámí.

12.2 Oznámení správně adresovaná se považují za doručená:

12.2.1 dnem, o němž tak stanoví zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále jen

„***ZDS***“), je-li oznámení zasíláno prostřednictvím datové zprávy do datové schránky ve smyslu ZDS; nebo

12.2.2 dnem fyzického předání oznámení, je-li oznámení zasíláno prostřednictvím kurýra nebo doručováno osobně; nebo

12.2.3 dnem doručení potvrzeným na doručence, je-li oznámení zasíláno doporučenou poštou; nebo

12.2.4 dnem, kdy bude, v případě, že doručení výše uvedeným způsobem nebude z jakéhokoli důvodu možné, oznámení zasláno doporučenou poštou na adresu Smluvní strany, avšak k jeho převzetí z jakéhokoli důvodu nedojde, a to ani ve lhůtě tří (3) pracovních dnů od jeho uložení na příslušné pobočce pošty.

12.3 Informace a materiály, které obsahují osobní údaje či důvěrné informace, budou doručovány buď osobně, nebo zasílány elektronicky a budou zabezpečeny proti zneužití. Způsob zabezpečení elektronické komunikace bude určen před zahájením realizace plnění této Smlouvy.

XIII. OPRÁVNĚNÉ OSOBY

13.1 Každá ze smluvních stran jmenuje oprávněnou osobu, popř. zástupce oprávněné osoby. Oprávněné osoby budou zastupovat smluvní stranu ve smluvních, obchodních a technických záležitostech souvisejících s plněním této Smlouvy.

13.2 Oprávněné osoby budou oprávněny činit rozhodnutí závazná pro Smluvní strany ve vztahu ke Smlouvě. Oprávněné osoby, nejsou-li statutárními orgány, však nejsou oprávněny provádět změny ani zrušení Smlouvy, nebude-li jim udělena speciální plná moc.

13.3 Každá ze Smluvních stran má právo změnit jí jmenované oprávněné osoby, musí však o každé změně vyrozumět písemně druhou Smluvní stranu ve lhůtě tří (3) dnů. Změna oprávněných osob je vůči druhé Smluvní straně účinná okamžikem, kdy o ní byla písemně vyrozuměna. Písemné zmocnění oprávněné osoby musí být s uvedením rozsahu zmocnění.

13.4 Existencí oprávněné osoby není dotčeno právo Objednatele komunikovat a kontaktovat pracovníky Poskytovatele dle komunikační matice, která bude stanovena při zahájení plnění.

13.5 Pokud má Poskytovatel formu sdružení, v souladu s obchodními podmínkami dle čl. 12 Zadávací dokumentace (Příloha č. 3 této Smlouvy) zavazuje jednání oprávněné osoby všechny členy sdružení společně a nerozdílně.

13.6 Oprávněnými osobami dle této Smlouvy jsou:

13.6.1 Na straně Objednatele:

Jméno, příjmení:	RNDr. Blanka Fischerová
Funkce:	Ředitelka Odboru správy monitorovacího systému MMR
Adresa:	Staroměstské náměstí 6, Praha 1, PSČ 110 15
Telefon:	[redacted]
Email:	

13.6.2 Na straně Poskytovatele:

Jméno, příjmení:	Ing. Vladimír Brenkuš
Funkce:	Manažer prodeje klíčovým zákazníkům
Adresa:	Tomíčkova 2144/1, 148 00 Praha 4
Telefon:	[redacted]
Email:	

XIV. KREDITACE A SANKCE

V případě, že ve kterémkoliv Vyhodnocovacím období dané Služby dle této Smlouvy nejsou Služby poskytovány v souladu se SLA uvedenými v Příloze č. 1, má Objednatel nárok na slevu z paušální ceny (dále jen „Kredity“), která bude stanovena v souladu s mechanismem uvedeným v Příloze č. 1 této Smlouvy, a to maximálně do výše 60% odměny za poskytování dané Služby za dané Vyhodnocovací období.

14.2 Slevy dle odst. 14.1 shora se uplatní pouze v případě, že Příloha č. 1 této Smlouvy nestanoví pro konkrétní typ prodlení zvláštní slevu z ceny.

14.3 V případě, že je Poskytovatel v prodlení s plněním povinnosti dle odst. 4.1 této Smlouvy (tj. nedodržení termínu zahájení plnění Služeb), aniž by ze strany Objednatele došlo ke změně termínu zahájení plnění, je Poskytovatel povinen Objednateli zaplatit smluvní pokutu ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý den prodlení s plněním této smluvní povinnosti.

14.4 V případě, že Poskytovatel poruší povinnosti dle odst. 6.3 a nebo 6.4 této Smlouvy je Poskytovatel povinen Objednateli zaplatit za každý takový případ smluvní pokutu ve výši 100.000,- Kč (slovy: jednosto tisíc korun českých) a to za každý započatý kalendářní měsíc, ve kterém k porušení povinnosti dle uvedených odstavců této Smlouvy došlo.

14.5 V případě, že je Poskytovatel v prodlení s plněním povinnosti dle odst. 6.1.15 této Smlouvy, je Poskytovatel povinen Objednateli zaplatit smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každý den prodlení s plněním této smluvní povinnosti.

14.6 V případě, že je Poskytovatel v prodlení s plněním povinnosti dle odst. 6.16 této Smlouvy, je Poskytovatel povinen Objednateli zaplatit smluvní pokutu ve výši 1.000,- Kč (slovy: jeden tisíc korun českých) za každý den prodlení s plněním této smluvní povinnosti.

14.7 V případě porušení povinností k ochraně důvěrných informací či ochraně osobních údajů dle článku XI. této Smlouvy je Objednatel oprávněn po Poskytovateli požadovat zaplacení smluvní pokuty za podmínek definovaných samostatnou „Smlouvou o dodržování bezpečnostních opatření v rámci spolupráce".

14.8 V případě porušení jakékoliv povinnosti Poskytovatele uvedené v odst. 6.6 až 6.12 této Smlouvy, je Poskytovatel povinen zaplatit Objednateli smluvní pokutu ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý případ takového porušení.

14.9 V případě, že Poskytovatel poruší povinnosti dle odst. 6.17 této Smlouvy je Poskytovatel povinen Objednateli zaplatit za každý takový případ smluvní pokutu ve výši 10.000.000,- Kč (slovy: deset miliónů korun českých) a to za každý započatý kalendářní měsíc, ve kterém k porušení povinnosti dle uvedeného odstavce této Smlouvy došlo.

14.10 Pro případ prodlení se zaplacením ceny plnění dle příslušné Faktury je Poskytovatel oprávněn po Objednateli požadovat zaplacení úroku z prodlení ve výši stanovené právními předpisy.

14.11 Smluvní pokutu je Objednatel oprávněn započíst formou jednostranného zápočtu proti jakékoliv pohledávce Poskytovatele za Objednatelem z titulu úhrady ceny Služeb dle této Smlouvy, kterou Poskytovatel uplatnil nebo uplatní vystavením Faktury.

14.12 Smluvní pokuty v souladu s odst. 5.8 této Smlouvy splatné do třiceti (30) dní ode dne doručení písemné výzvy oprávněné smluvní strany k jejich úhradě povinnou smluvní stranou, není-li ve výzvě uvedena lhůta delší.

14.13 Zaplacením smluvní pokuty není dotčen nárok Objednatele na náhradu škody v plné výši.

XV. DOBA TRVÁNÍ A ZÁNIK SMLOUVY

15.1 Tato Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma Smluvními stranami. Smlouva je uzavřena na dobu neurčitou.

15.2 Smlouva zaniká mimo další možnosti definované zákonem rovněž:

15.2.1 Dohodou Smluvních stran.

15.2.2 Jednostranným odstoupením Objednatele od Smlouvy pro její podstatné porušení Poskytovatelem, přičemž podstatným porušením Smlouvy se rozumí zejména:

- opakované (alespoň třikrát za tři po sobě jdoucí měsíce) prodlení na straně Poskytovatele s dodržením stanovené lhůty pro vyřešení incidentů typu A dle Přílohy č. 1 této Smlouvy s dobou vyřešení delší než 12 (slovy: dvanáct) hodin; nebo
- dostupnost Služeb, tj. SLA parametr "Minimální dostupnost" pro jednotlivé tyto Služby, je během tří po sobě jdoucích měsíců nižší než 90 % (slovy: devadesát procent); nebo
- porušení povinností dle odst. 6.17 této Smlouvy; nebo
- další případy, o kterých tak stanoví tato Smlouva;
- porušení jakékoliv jiné povinnosti Poskytovatele vyplývající ze Smlouvy a její nesplnění ani v dodatečné přiměřené lhůtě, kterou k tomu Objednatel poskytne (nevylučuje-li to charakter porušené povinnosti); v pochybnostech se má za to, že dodatečná lhůta je přiměřená, pokud činila alespoň pět pracovních dní.

15.2.3 Poskytovatel je oprávněn od této Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Objednatelem, za což se považuje prodlení Objednatele s úhradou ceny za plnění předmětu dle této Smlouvy o více než 30 (slovy: třicet) dní, pokud Objednatel nezjedná nápravu ani do 30 (slovy: třiceti) dnů od doručení písemného oznámení Poskytovatele o takovém prodlení se žádostí o jeho nápravu.

15.2.4 Smluvní strany se dále dohodly, že Objednatel je oprávněn od této Smlouvy odstoupit, pokud nebude schválena částka ze státního rozpočtu následujícího roku, která je potřebná k úhradě za plnění poskytované podle této Smlouvy v následujícím roce. Objednatel prohlašuje, že do třiceti (30) dnů po vyhlášení zákona o státním rozpočtu ve sbírce zákonů oznámí Poskytovateli, pokud nebyla schválena částka ze státního rozpočtu následujícího roku, která je potřebná k úhradě za plnění poskytované dle této Smlouvy v následujícím roce.

15.2.5 Objednatel je rovněž oprávněn odstoupit od této Smlouvy, pokud je na majetek Poskytovatele vedeno insolvenční řízení nebo byl insolvenční návrh zamítnut pro nedostatek majetku Poskytovatele, dle zákona č. 182/2006 Sb., o úpadku

a způsobech jeho řešení, ve znění pozdějších předpisů, nebo pokud Poskytovatel vstoupí do likvidace.

15.2.6 Objednatel je rovněž oprávněn odstoupit od této Smlouvy, pokud dojde ke zrušení zadávacího řízení na "Pořízení HW platformy a Infrastruktury serverovny pro MS2014+", uvedeného na profilu Objednatele (https://ezak.mmr.cz), které je klíčové pro vytvoření Prostředí a tedy je nezbytné pro poskytování Služeb dle této Smlouvy.

15.2.7 Písemnou výpovědí Objednatele i bez udání důvodu. Výpovědní doba činí 3 (slovy: tři) měsíce a začíná běžet prvním dnem měsíce následujícího po měsíci, v němž byla výpověď doručena Poskytovateli.

15.2.8 Písemnou výpovědí Poskytovatele i bez udání důvodu. Výpovědní doba činí 6 (slovy: šest) měsíců a začíná běžet prvním dnem měsíce následujícího po měsíci, v němž byla výpověď doručena Poskytovateli. Poskytovatel je oprávněn podat písemnou výpověď Smlouvy dle tohoto odst. 15.2.8 nejdříve po uplynutí 2 (slovy: dvou) let trvání účinnosti Smlouvy.

15.3 Předčasným ukončením této Smlouvy nejsou dotčena ustanovení o odpovědnosti za škodu (škoda může spočívat i v nákladech vynaložených Objednatelem na realizaci nového výběrového/zadávacího řízení), nároky na uplatnění smluvních pokut, o ochraně důvěrných informací a ostatních práv a povinností založených touto Smlouvou, která mají podle zákona, této Smlouvy či dle své povahy trvat i po jejím zrušení.

XVI. ZÁVĚREČNÁ USTANOVENÍ

16.1 Tato Smlouva představuje úplnou dohodu Smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných oprávněnými zástupci obou Smluvních stran.

16.2 Poskytovatel se zavazuje bez předchozího výslovného písemného souhlasu Objednatele nepostoupit ani nepřevést jakákoliv práva či povinnosti vyplývající ze Smlouvy na třetí osobu či osoby.

16.3 Poskytovatel se zavazuje, že jakoukoliv změnu ovládání ve smyslu § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů (dále jen ***„ZOK“)*** písemně oznámí Objednateli.

16.4 Je-li nebo stane-li se jakékoli ustanovení této Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení této Smlouvy. Smluvní strany se tímto zavazují nahradit jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.

16.5 Jednacím jazykem mezi Objednatelem a Poskytovatelem bude pro veškerá plnění vyplývající z této Smlouvy výhradně jazyk český.

16.6 Práva a povinnosti vzniklé na základě Smlouvy nebo v souvislosti s ní se řídí českým právním řádem, zejména pak ObčZ, ZOK, ZVZ a Autorským zákonem. Veškeré případné spory ze Smlouvy budou v prvé řadě řešeny smírem. Pokud smíru nebude dosaženo během 30 (slovy: třiceti) dnů, všechny spory z této Smlouvy a v souvislosti s ní budou řešeny věcně a místně příslušným soudem v České republice. Smluvní strany se dohodly, že místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.

16.7 Poskytovatel není bez předchozího písemného souhlasu Objednatele oprávněn po dobu účinnosti Smlouvy a 12 (slovy: dvanáct) měsíců po ukončení trvání Smlouvy zaměstnat zaměstnance Objednatele přímo nebo i nepřímo, a to ani v subjektech, v nichž má rozhodující finanční, majetkovou nebo jinou účast. Za zaměstnance Objednatele se považuje osoba, která byla v pracovním poměru k Objednateli v době účinnosti Smlouvy a přímo se podílela na plnění předmětu této Smlouvy nebo o něm rozhodovala.

16.8 Tato Smlouva je vyhotovena v 7 vyhotoveních, z nichž Objednatel obdrží 5 vyhotovení a Poskytovatel 2 vyhotovení.

16.9 Nedílnou součástí Smlouvy jsou následující přílohy:

- Příloha č. 1 – Katalog služeb a podmínky poskytování Bezpečnostního dohledu;

- Příloha č. 2 – Seznam subdodavatelů;
- Příloha č. 3 - Zadávací dokumentace;
- Příloha č. 4 - Popis způsobu poskytování služeb Bezpečnostního dohledu;
- Příloha č. 5 - Bezpečnostní tým;

16.10 Smluvní strany shodně prohlašují, že si Smlouvu před jejím podpisem přečetly a že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, a že se dohodly o celém jejím obsahu, což stvrzují svými podpisy.

V Praze dne 16.7. 2015

Za Objednatele

[redacted]

Česká republika – Ministerstvo pro místní rozvoj
RNDr. Blanka Fischerová
Ředitelka Odboru správy monitorovacího systému

V Praze dne 16.7. 2015

Za Poskytovatele

[redacted]

Ing. Petr Malimánek, na základě pověření

[redacted]

[redacted]adě pověření

T-Mobile Czech Republic a.s.
Tomíčkova 2144/1
Praha 4
DIČ CZ64949681
122

Číslo v CES: 5390

Příloha č. 1 Smlouvy o poskytování služeb

Katalog služeb a podmínky poskytování bezpečnostního dohledu

1 Obsah

1 OBSAH 2

2 DEFINICE SLUŽEB 3

3 SEZNAM SLUŽEB 5

3.1 SLUŽBA „BS01_INFORMAČNÍ BEZPEČNOST“ 5
3.2 SLUŽBA „BS02_OCHRANA OSOBNÍCH ÚDAJŮ“ 12
3.3 SLUŽBA „BS03_BEZPEČNOSTNÍ MONITORING“ 16
3.4 SLUŽBA „BS04_KONTROLA KVALITY POSKYTOVANÝCH SLUŽEB“ 23
3.5 SLUŽBA „BS05_AUDIT PROSTŘEDÍ“ 27

4 MATICE ZODPOVĚDNOSTÍ 33

5 PODMÍNKY POSKYTOVÁNÍ SLUŽEB 34

5.1 VYMEZENÍ POJMŮ 34
5.2 VYMEZENÍ SLA 36
5.3 HODNOCENÍ SLUŽEB 37
5.4 MAXIMÁLNÍ DOBA VÝPADKU 38
5.5 MAXIMÁLNÍ DOBA SERVISNÍ ODEZVY 38
5.6 ODSTRANĚNÍ INCIDENTU – A, B A C 39
5.7 DALŠÍ POŽADOVANÉ ČINNOSTI MIMO SLEDOVANÉ PARAMETRY SLA 39
5.8 STATISTIKA (EXPORTY) SERVICEDESKU 40
5.9 PARAMETRY SNÍŽENÍ PAUŠÁLNÍ CENY - KREDITACE 41

2 Definice služeb

Katalog služeb je detailní formulací předmětu plnění Poskytovatele a specifikuje pro Poskytovatele veškeré činnosti, provozní podmínky a další náležitosti Služeb, které bude nad Prostředím vykonávat.

Následující tabulka uvádí souhrnný přehled Služeb a jejich jednotlivých klíčových činností:

Označení	Služba	Činnosti
BS01	Informační bezpečnost	Definice procesů, zásad, politik a metodik ISMS
		Tvorba bezpečnostní dokumentace ISMS
		Řízení bezpečnostních incidentů
BS02	Ochrana osobních údajů	Metodická a legislativní podpora Objednatele
		Definice metodik, procesů a postupů ochrany osobních údajů a jejich prosazení do bezpečnostní dokumentace ISMS
		Kontrola zpracování osobních údajů
BS03	Bezpečnostní monitoring	Poskytnutí služby HW/SW vyhodnocovacího centra bezpečnostního monitoringu
		Provádění průběžného monitoringu
		Vyhledávání slabých míst
		Stanovování provozních, technických a konfiguračních parametrů bezpečnostních prvků celého prostředí MS2014+
BS04	Kontrola kvality poskytovaných služeb	Kontrola a vyhodnocení parametrů poskytovaných služeb
		Dohled nad poskytovateli služeb a dodržováním závazných smluvních parametrů služeb
BS05	Audit prostředí	Penetrační testy
		Kontroly dodržování pravidel informační bezpečnosti
		Součinnost při auditech a kontrolách
		Součinnost při certifikacích

Detailní obsah, popis, parametry a způsob vyhodnocení jednotlivých Služeb stanovuje kap. 3 tohoto dokumentu. Podmínky poskytování těchto Služeb vymezuje kap. 5 tohoto dokumentu.

Vymezení prostředí:

Označení	Název prostředí	Pozn.
PR1	Produkční	
PR2	Testovací /školící	

Vymezení lokalit:

Označení	Název lokality	Adresa
DC1	Primární	Datové centrum Poskytovatele služeb Prostředí na adrese Jeremenkova 40b, Olomouc.

DC2	Zálohovací / Záložní	Datové centrum v sídle Objednatele. Datové centrum nemá zajištěnu možnost fyzického přístupu do DC v režimu 24x7, ale pouze v režimu 5x8 na vyžádání.

Vymezení rolí:

Název role	Popis role
Vedoucí týmu informační bezpečnosti	Role odpovědná za výkon, koordinaci a poskytování služeb s důrazem na řešení systému řízení informační bezpečnosti a ochrany osobních údajů. Vedoucí týmu informační bezpečnosti je zároveň projektovým manažerem celého projektu, odpovědným za fungování a výkon činností a služeb celého bezpečnostního týmu.
Bezpečnostní specialista	Role odpovědná za výkon činností a poskytování služeb s důrazem na implementaci systému řízení informační bezpečnosti a provádění kontrolních a auditních činností. Role je podřízená Vedoucímu týmu informační bezpečnosti.
Bezpečnostní konzultant	Role odpovědná za výkon činností a poskytování služeb s důrazem na řešení systému řízení kontinuity činností, návrh a řešení disaster recovery plánů a postupů. Role je podřízená Vedoucímu týmu informační bezpečnosti.
Vedoucí týmu monitoringu a testování	Role odpovědná za výkon činností a koordinaci poskytování služeb s důrazem na služby bezpečnostního monitoringu a ověřování informační bezpečnosti. Role je podřízená Vedoucímu týmu informační bezpečnosti.
Specialista - bezpečnostní monitoring	Role odpovědná za výkon činností a poskytování služeb s důrazem na řešení bezpečnostního monitoringu a vyhodnocovacího centra bezpečnostního monitoringu. Role je podřízená Vedoucímu týmu monitoringu a testování.
Specialista - monitoring	Role odpovědná za výkon činností a poskytování služeb s důrazem na řešení auditních nástrojů a způsobu sběru auditních informací z dohledovaného řešení. Role je podřízená Vedoucímu týmu monitoringu a testování.
Operátor - monitoring	Role odpovědná za výkon činností operátora (obsluhy) vyhodnocovacího centra bezpečnostního monitoringu. Role je podřízená Vedoucímu týmu monitoringu a testování.
Specialista - tester	Role odpovědná za výkon činností a poskytování služeb s důrazem na provádění bezpečnostních a penetračních testů a ověřování kvality. Role je podřízená Vedoucímu týmu monitoringu a testování.

Pro tyto role platí kvalifikace, která je definována Zadávací dokumentací (viz Příloha č. 3 Smlouvy).

3 Seznam služeb

3.1 Služba „BS01_Informační bezpečnost“

3.1.1 Parametry služby

Označení	Název služby		
BS01	**Informační bezpečnost**		
Vymezení služby			
Lokalita	DC1, DC2	**Prostředí**	PR1, PR2
Zkrácený popis služby	Služby související s řízení bezpečnosti informací v souladu se zásadami pro Systém řízení bezpečnosti informací (ISMS) dle norem řady ČSN ISO/IEC 27000		
Klíčové činnosti v rámci služby	1. Definice procesů, zásad, politik a metodik ISMS 2. Tvorba bezpečnostní dokumentace ISMS 3. Řízení bezpečnostních incidentů		
Minimální rozsah služeb	**Klíčová činnost**	**Minimální rozsah v hodinách**	**Periodicita činnosti**
	Definice procesů, zásad, politik a metodik ISMS	744	Jednorázově
	Tvorba bezpečnostní dokumentace ISMS	68	Vyhodnocovací období
	Řízení bezpečnostních incidentů	64	Vyhodnocovací období
Požadované role obsazované Poskytovatelem	**Název role**	**Požadovaný rozsah alokace (z provozní doby)**	
	Vedoucí týmu informační bezpečnosti	11,04 *(rozsah alokace jednorázovýh činností je zahrnut jako poměrná část (1/48) do alokace za vyhodnocovací období)	
	Bezpečnostní specialista	49,46 *(rozsah alokace jednorázovýh činností je zahrnut jako poměrná část (1/48) do alokace za vyhodnocovací období)	
	Bezpečnostní konzultant	50,29 *(rozsah alokace jednorázovýh činností je zahrnut jako poměrná část (1/48) do alokace za vyhodnocovací období)	
	Specialista - bezpečnostní monitoring	18,35 *(rozsah alokace jednorázovýh činností je zahrnut jako poměrná část (1/48) do alokace za vyhodnocovací období)	
	Specialista - tester	18,35 *(rozsah alokace jednorázovýh činností je zahrnut jako poměrná část (1/48) do alokace za vyhodnocovací období)	
SLA parametry služby			

Vyhodnocovací období	1 kalendářní měsíc		
Provozní doba	08.00 - 16.00 (5x8)		
Parametr	**Jednotka**	**Hodnota**	**Max počet za období**
Minimální dostupnost	[%/období]	99,5	-
Lhůty při vyřizování požadavku/incidentu			
Lhůta pro potvrzení přijetí	[min]	5	-
Lhůta pro informování o způsobu a odhadu délky řešení	[min]	15	-
Garantovaná doba zahájení řešení	[min]	15	-
Lhůty při řešení požadavku/incidentu			
Kategorie A	[hod]	4	1
Kategorie B	[hod]	8	2
Kategorie C	[dny]	NBD[1]	5

Cena služby			
Položka	**Cena v Kč bez DPH**	**DPH 21%**	**Cena v Kč s DPH**
Paušální cena za vyhodnocovací období	78 893,90 Kč	16 567,72 Kč	95 461,61 Kč

Poskytovatel je povinen cenu za jednorázovou klíčovou činnost č. 1 zohlednit v rámci Paušální ceny za Vyhodnocovací období. Objednatel bude Službu hradit pouze formou úhrady paušální ceny.

3.1.1.1 Vysvětlivky

Minimální rozsah služeb - tento oddíl tabulky specifikuje minimální rozsah poskytnutých kapacit Poskytovatele pro zajištění požadované činnosti pro danou periodu. Výsledný rozsah stanoví Poskytovatel na základě svých znalostí a zkušeností tak, aby odpovídal legislativním předpisům, odborným doporučením a požadavkům na kvalitu a SLA. Rozsah plnění ze strany Poskytovatele nebude v rámci této klíčové činnosti omezen a to i v takovém případě, pokud množství aktuálně provedených činností (v návaznosti na předmět činností) bude vyšší, než Objednatelem deklarovaný minimální rozsah Služby a není důvodem pro změnu výše paušální ceny za poskytovanou Službu.

Požadované role obsazované Poskytovatelem - Poskytovatel uvede v položce **Rozsah alokace (z provozní doby)** pro danou roli očekávaný rozsah hodin, které bude pro výkon dané činnosti alokovat tak, aby byly garantovány požadované SLA parametry příslušné činnosti/služby. Výsledný rozsah hodin za všechny role pro danou činnost musí být roven nebo větší minimálnímu rozsahu služby uvedenému v předcházející části tabulky. Rozsah alokace pro jednotlivé role musí odpovídat povaze dané činnosti.

Paušální cenu za vyhodnocovací období uvede Poskytovatel s přesností na dvě (2) desetinná místa.

[1] NBD (Next Business Day) - následující pracovní den

3.1.2 Popis a parametry činností

Objednatel požaduje zajistit řízení bezpečnosti informací. Jedná se o služby související s řízením bezpečnosti informací v souladu se zásadami pro Systém řízení bezpečnosti informací (ISMS) dle norem řady ČSN ISO/IEC 27000 a to v rozsahu pokrývajícím celý systém MS2014+.

V definované oblasti Objednatel požaduje zajistit zejména Služby uvedené v rámci dále uvedených klíčových činností.

3.1.2.1 Definice procesů, zásad, politik a metodik ISMS

Objednatel požaduje vytvoření systému ISMS pro potřeby a v podmínkách MS2014+ způsobem, který nastaví a prosadí Informační bezpečnost v rozsahu požadovaném standardy řady ČSN ISO/IEC 27000 napříč celým systémem MS2014+. Celé řešení MS2014+ (Prostředí i Aplikace MS2014+) je zároveň informačním systémem dle zákona 365/2000 Sb., o informačních systémech veřejné správy (ISVS), v aktuálním znění, navržené bezpečnostní procesy a zásady musí být s tímto zákonem a jeho požadavky v plném souladu.

Objednatel v informační koncepci stanovil dlouhodobé cíle, kterých chce dosáhnout v oblasti řízení bezpečnosti informačních systémů veřejné správy, mezi které patří systém MS2014+. Těmito cíli jsou:

- bezpečnost dat, která jsou v MS2014+ vytvářena, zpracovávána, ukládána a archivována,
- bezpečnost technických a programových prostředků (Prostředí a Aplikace MS2014+),
- bezpečnost služeb systému MS2014+.

S přihlédnutím k těmto cílům provede Poskytovatel detailní analýzu systému MS2014+, platné Informační koncepce a Bezpečnostní politiky Objednatele a navazujících dokumentů EK, národní legislativy a dalších dokumentů relevantních pro prostředí MS2014+ a navrhne:

- **procesy bezpečnosti informací a řízení bezpečnosti informací**, které je nezbytné uplatnit a prosadit v rámci systému MS2014+
- **klíčové cíle a hlavní zásady bezpečnosti informací**, které budou navrženými procesy pokryty. Cíle ISMS MS2014+ budou zpracovány na období 4 let, přičemž cíle na 1. rok poskytování služeb budou rozpracovány detailně.
- **implementační plán vytvoření systému ISMS MS2014+**, který přehledným způsobem navrhne detailní harmonogram prací a služeb pro vytvoření Systému řízení bezpečnosti informací MS2014+ (ISMS MS2014+). Implementační plán musí zohlednit dále stanovené termíny pro přípravu dokumentace a musí být koncipován tak, aby byl Objednatel schopen **certifikovat ISMS MS2014+ u akreditovaného certifikačního orgánu v horizontu 10 kalendářních měsíců** od data účinnosti této Smlouvy.

Veškeré dokumenty potřebné pro výše popsaný návrh (např. Bezpečnostní politika Objednatele) budou Objednatelem poskytnuty Provozovateli formou součinnosti a to při zahájení poskytování Služeb.

V rámci zpracovávané dokumentace budou zohledněny minimálně následující **právní normy**:

- zákon č. 101/2000 Sb., o ochraně osobních údajů v platném znění,
- zákon č. 227/2000 Sb., o elektronickém podpisu v platném znění,
- zákon č. 365/2000 Sb., o informačních systémech veřejné zprávy v platném znění,
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění,
- zákon č.151/2000 Sb., o telekomunikacích a o změně dalších zákonů v platném znění,

- zákon č. 121/2000 Sb., o právu autorském, a o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění,
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů v platném znění.
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

V rámci zpracovávané dokumentace budou zohledněny minimálně následující **odborné standardy**:

- ČSN ISO/IEC 27000 – „Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník“.
- ČSN ISO/IEC 27001 „Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky“
- ČSN ISO/IEC 27002 – „Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací“.
- ISO/IEC 27003 – “Information technology – Security techniques – Information security management system implementation guidance“ (Informační technologie – Bezpečnostní techniky – Příručka zavedení systému managementu bezpečnosti informací –).
- ISO/IEC 27004 – „Information technology – Security techniques – Information security management – Measurement“ (Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Měření).
- ČSN ISO/IEC 27005 – „Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací“.
- ČSN ISO/IEC 27006 – „Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací“.
- ISO/IEC 27033-1 – „Information technology — Security techniques — Network security — Part 1: Overview and concepts“ (Informační technologie – Bezpečnostní techniky – Síťová bezpečnost – Úvod a pojetí).
- ČSN ISO 22301 - Ochrana společnosti - Systémy managementu kontinuity podnikání - Požadavky
- ISO/IEC 15408-1 „Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model“ (informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model).
- ČSN ISO/IEC 15408-2 – „Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty“.
- ČSN ISO/IEC 15408-3 – „Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk“
- ISO/IEC 18043 Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (případně pokud již bude vydána norma ISO/IEC 27039 — Information technology — Security techniques — Selection, deployment and operations of Intrusion Detection [and Prevention] Systems, která bude 18043 nahrazovat)

V rámci zpracovávané dokumentace budou zohledněny minimálně následující **dokumenty a z nich vyplývající závazky Objednatele a dalších třetích stran**:

- platná smlouva Provozovatele Aplikace MS2014+ a z ní vyplývající procesy, postupy a činnosti ve vztahu k Aplikaci MS2014+;
- platná smlouva Poskytovatele služeb Prostředí a z ní vyplývající procesy, postupy a činnosti ve vztahu k Prostředí systému MS2014+;

Procesy a postupy navržené Poskytovatelem v rámci ISMS MS2014+ musí být připravené a koncipované tak, aby byly v souladu s postupy pro správu, provoz, servis a rozvoj Aplikace MS2014+ a Prostředí.

Implementační plán vytvoření systému ISMS MS2014+ musí v této fázi respektovat zejména ustavení systému ISMS a vytvoření základních předpokladů pro vytváření celého systému ISMS MS2014+, tedy:

a) Stanovení předběžného rozsahu systému řízení pro MS2014+, výstupem bude dokument **Rozsah ISMS MS2014+,** který bude v závěru této klíčové činnosti zpřesněn a finalizován v návaznosti na získané výsledky ostatních činností.
b) Provedení identifikace aktiv systému MS2014+ a identifikace vlastníků aktiv/informací. Výstupem bude **Registr aktiv MS2014+.**
c) Zpracování **Směrnice pro klasifikaci a řízení aktiv MS2014+** a následné provedení hodnocení aktiv podle této směrnice. Hodnocení aktiv bude spolu s registrem aktiv základními dokumenty pro provedení analýzy rizik.
d) Stanovení komplexních zásad pro provedení analýzy rizik prostředí MS2014+, výstupem bude **Směrnice pro hodnocení rizik MS2014+**
e) Provedení analýzy rizik a zpracování jejích výsledků do dokumentu **Zpráva o hodnocení rizik MS2014+**.
f) V návaznosti na výsledky analýzy rizik budou vybrána opatření pro jejich minimalizaci, resp. eliminaci. Vybraná bezpečnostní opatření budou uvedena v **Prohlášení o aplikovatelnosti**. Spolu s tímto prohlášení budou vymezena zbytková rizika a ta zpracována v dokumentu **Souhlas s navrhovanými zbytkovými riziky**.
g) V návaznosti na předchozí činnosti a jejich výstupy bude zpracována **Bezpečnostní politika MS2014+** jako dokument, který formuluje základní strategie, cíle, postoje, role, zodpovědnosti a zásady týkající se činností spojených s informační bezpečností v systému MS2014+.
h) Posledním bodem bude zpracování **Návrhu řídící struktury (výboru) pro ISMS MS2014+** a zpracování **Jednacího řádu výboru**.

Poskytovatel provede výše uvedené činnosti a předá stanovené dokumenty ke schválení do **2 kalendářních měsíců** od data účinnosti této Smlouvy.

3.1.2.2 Tvorba bezpečnostní dokumentace ISMS

Navržený **Implementační plán vytvoření systému ISMS MS2014+** bude v návaznosti na výsledky předcházející klíčové činnosti obsahovat vytvoření detailní dokumentace systému ISMS MS2014+. Tato dokumentace bude zpracována v souladu se zásadami a procesy zakotvenými v základních dokumentech ISMS MS2014+ (viz kap. 3.1.2.1) a to minimálně v následujícím rozsahu:

- **Směrnice k řízení bezpečnosti informací MS2014+,**
- **Směrnice k systému řízení dokumentace MS2014+,**
- **Směrnice k bezpečnosti lidských zdrojů MS2014+,**
- **Směrnice pro budování bezpečnostního povědomí MS2014+,**
- **Směrnice fyzické bezpečnosti a bezpečnosti prostředí MS2014+,**
- **Směrnice k bezpečnosti informačních a komunikačních technologií MS2014+,**
- **Směrnice k řízení incidentů MS2014+,**
- **Směrnice pro řízení kontinuity činností MS2014+,**
- **Směrnice k zajištění shody s bezpečnostními požadavky v rámci MS2014+,**
- **Plán zvládání rizik MS2014+,**
- **Metodika k provádění interních auditů ISMS MS2014+,**
- **Bezpečnostní směrnice pro činnost bezpečnostního správce MS2014+,**
- **Bezpečnostní směrnice administrátora Prostředí a Infrastruktury serverovny,**

- **Bezpečnostní směrnice uživatele MS2014+.**

Součástí výše uvedených směrnic, metodik a plánů budou i veškeré **relevantní a potřebné formuláře** pro evidenci, hlášení, záznamy a další činnosti, vyplývající ze stanoveného rozsahu ISMS a potřebné pro fungování tohoto systému na denní bázi.

Uvedené dokumenty budou zpracovány **do 2 kalendářních měsíců od akceptace výstupů klíčové činnosti dle kap. 3.1.2.1** a předloženy Objednateli k akceptaci. Dokumenty budou pokrývat veškeré oblasti stanovené normou ČSN ISO/IEC 27002 a v budou zpracovány v detailu umožňujícím ověření naplnění vybraných bezpečnostních opatření dle ČSN ISO/IEC 27001 a dostatečném pro návrh technického řešení bezpečnostních mechanismů, které mají být implementovány do jednotlivých prvků Prostředí a Aplikace MS2014+.

V návaznosti na Směrnici pro řízení kontinuity zpracuje Poskytovatel kompletní **Havarijní plány systému MS2014+** a to v minimálně v následujícím rozsahu:

- plány pro zvládání krizových situací
- dílčí havarijní scénáře
- dispečerské povinnosti
- krizový tým
    - definice členů týmů a definice jejich kompetencí
    - postupy a dokumentace činností při zvládání krizových situací
- náhradní a dočasné řešení kontinuity služeb
    - definice zbytných a nezbytných služeb v návaznosti na klasifikaci aktiv
    - stanovení pravidel zajištění náhradního a dočasného provozu

V rámci řešení havarijních plánů provede Poskytovatel **posouzení Zálohovacího plánu a Plánu obnovy**, které budou zpracovány Poskytovatelem služeb Prostředí v rámci zadávacího řízení „Pořízení HW platformy a Infrastruktury serverovny pro MS2014+“. Výstupem posouzení bude doporučení pro Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí, na jejichž základě uvedené subjekty dopracují dokument tak, aby byl v souladu s nastaveným systém ISMS MS2014+ a jeho postupy pro řízení kontinuity a havarijními plány.

Havarijní plány a aktualizovaný Zálohovací plán a Plán obnovy budou předloženy Objednateli k **akceptaci do 2 kalendářních měsíců** od akceptace směrnic ISMS uvedených výše v rámci této klíčové činnosti.

Poskytovatel zároveň zajistí pravidelnou **aktualizaci celé dokumentační základny ISMS MS2014+** a to s periodou 1x za 6 měsíců. V rámci aktualizace budou zapracovávány zejména dílčí změny v prováděcích postupech a bezpečnostních mechanismech v návaznosti na běžné změny provozního Prostředí a Aplikace MS2014+. Perioda aktualizace dokumentace je shodná s prováděním Interního auditu ISMS MS2014+ (viz 3.5.2.2) tak, aby bylo možné výsledky interních auditů promítnout v rámci aktualizace dokumentační základny.

Poskytovatel je zároveň (formou mimořádné aktualizace) povinen upravit a aktualizovat systém ISMS v celém dotčeném rozsahu v případě, že Objednateli budou uloženy povinnosti v oblasti kybernetické bezpečnosti dle zákona č. 181/2014 Sb.

Jedenkrát ročně provede Poskytovatel přezkoumání **Rozsahu ISMS MS2014+** s důrazem na posouzení:

- Klíčové charakteristiky MS2014+,
- Procesy zahrnuté do ISMS MS2014+,

- Přehled informačních aktiv zahrnutých do ISMS MS2014+,
- Přehled lokalit zahrnutých do ISMS MS2014+,
- Role a odpovědnosti v rámci ISMS MS2014+,
- Zdůvodnění vyjmutí aktiv z rozsahu ISMS MS2014+.

V rámci přezkoumání Rozsahu ISMS MS2014+ zároveň provede Poskytovatel **vyhodnocení splnění cílů ISMS MS2014+**, zejména naplnění cílů za uplynulý rok, rozpracování dlouhodobých cílů (ze 4 letého plánu) do detailních cílů na následující období.

Výstupem přezkoumání bude aktualizovaný Rozsah ISMS MS2014+. V návaznosti na aktualizaci Rozsahu ISMS MS2014+ je Poskytovatel povinen do 2 kalendářních měsíců od akceptace aktualizovaného Rozsahu ISMS MS2014+ provést doplňkovou analýzu rizik, posouzení dopadů, návrh bezpečnostních opatření a následně aktualizovat celou dokumentační základnu ISMS MS2014+.

3.1.2.3 Řízení bezpečnostních incidentů

Poskytovatel bude na denní bázi provádět **řízení bezpečnostních incidentů systému MS2014+**. Detailní postupy a procesy řízení bezpečnostních incidentů budou vycházet ze schválené Směrnice k řízení incidentů MS2014+ (viz kap. 3.1.2.2). Poskytovatel bude vůči Objednateli v oblasti řízení bezpečnostních incidentů primární odpovědnou osobou za řešení bezpečnostně relevantních incidentů, událostí a slabin MS2014+.

Poskytovatel v rámci této Služby bude využívat formuláře pro hlášení a řešení bezpečnostních incidentů a událostí MS2014+ (zpracované v rámci dokumentace ISMS) a bude vykonávat veškeré relevantní činnosti vyplývající ze stanovených odpovědností a postupů reakce na incidenty, shromažďování důkazů a ponaučení se z těchto incidentů.

Pro řešení bezpečnostních incidentů bude Poskytovateli zajištěn přístup na ServiceDesk MS2014+ v potřebném rozsahu.

3.1.3 Vyhodnocení služby

O poskytnutí všech služeb bude připraven ze strany Poskytovatele tzv. "**Protokol o poskytnuté službě**" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující:

- Výkaz činností v rámci ISMS
- Výkaz stavu bezpečnostní dokumentace s přehledem platné a akceptované dokumentace ISMS
- Výkaz za oblast bezpečnostních incidentů s detailním popisem stavu a problému při šetření jednotlivých incidentů.

3.2 Služba „BS02_Ochrana osobních údajů“

3.2.1 Parametry služby

Označení	**Název služby**				
BS02	**Ochrana osobních údajů**				
Vymezení služby					
Lokalita	DC1, DC2	**Prostředí**	PR1, PR2		
Zkrácený popis služby	Služby související s prováděním ochrany osobních údajů v souladu s požadavky zákona č. 101/2000 Sb., o ochraně osobních údajů				
Klíčové činnosti v rámci služby	1. Metodická a legislativní podpora Objednatele 2. Definice metodik, procesů a postupů ochrany osobních údajů a jejich prosazení do bezpečnostní dokumentace ISMS 3. Kontrola zpracování osobních údajů				
Minimální rozsah služeb	**Klíčová činnost**	**Minimální rozsah v hodinách**	**Periodicita činnosti**		
	Metodická a legislativní podpora Objednatele	24	Vyhodnocovací období		
	Definice metodik, procesů a postupů ochrany osobních údajů a jejich prosazení do bezpečnostní dokumentace ISMS	48			
	Kontrola zpracování osobních údajů	24			
Požadované role obsazované Poskytovatelem	**Název role**	**Požadovaný rozsah alokace (z provozní doby)**			
	Vedoucí týmu informační bezpečnosti	6			
	Bezpečnostní specialista	35			
	Bezpečnostní konzultant	37			
	Specialista - bezpečnostní monitoring	18			
SLA parametry služby					
Vyhodnocovací období	1 kalendářní měsíc				
Provozní doba	08.00 - 16.00 (5x8)				
Parametr	**Jednotka**	**Hodnota**	**Max počet za období**		
Minimální dostupnost	[%/období]	99,5	-		
Lhůty při vyřizování požadavku/incidentu					

Lhůta pro potvrzení přijetí	[min]	5	-
Lhůta pro informování o způsobu a odhadu délky řešení	[min]	15	-
Garantovaná doba zahájení řešení	[min]	15	-
Lhůty při řešení požadavku/incidentu			
Kategorie A	[hod]	4	1
Kategorie B	[hod]	8	2
Kategorie C	[dny]	NBD	5

Cena služby			
Položka	**Cena v Kč bez DPH**	**DPH 21%**	**Cena v Kč s DPH**
Paušální cena za vyhodnocovací období	52 208,00 Kč	10 963,68 Kč	63 171,68 Kč

3.2.1.1 Vysvětlivky

Minimální rozsah služeb - tento oddíl tabulky specifikuje minimální rozsah poskytnutých kapacit Poskytovatele pro zajištění požadované činnosti pro danou periodu. Výsledný rozsah stanoví Poskytovatel na základě svých znalostí a zkušeností tak, aby odpovídal legislativním předpisům, odborným doporučením a požadavkům na kvalitu a SLA. Rozsah plnění ze strany Poskytovatele nebude v rámci této klíčové činnosti omezen a to i v takovém případě, pokud množství aktuálně provedených činností (v návaznosti na předmět činností) bude vyšší, než Objednatelem deklarovaný minimální rozsah Služby a není důvodem pro změnu výše paušální ceny za poskytovanou Službu.

Požadované role obsazované Poskytovatelem - Poskytovatel uvede v položce **Rozsah alokace (z provozní doby)** pro danou roli očekávaný rozsah hodin, které bude pro výkon dané činnosti alokovat tak, aby byly garantovány požadované SLA parametry příslušné činnosti/služby. Výsledný rozsah hodin za všechny role pro danou činnost musí být roven nebo větší minimálnímu rozsahu služby uvedenému v předcházející části tabulky. Rozsah alokace pro jednotlivé role musí odpovídat povaze dané činnosti.

Paušální cenu za vyhodnocovací období uvede Poskytovatel s přesností na dvě (2) desetinná místa.

3.2.2 Popis a parametry činností

3.2.2.1 Metodická a legislativní podpora Objednatele

Objednatel je z pohledu ochrany osobních údajů (dále též "***OOÚ***") **správcem** a **zpracovatelem** osobních údajů v souladu se zněním zákona č. 101/2000 Sb., o ochraně osobních údajů. Tyto osobní údaje fyzických osob budou shromažďovány, zpracovávány a ukládány i v systému MS2014+ a budou nedílnou součástí jeho dat a informací.

Poskytovatel zajistí Objednateli v rámci této klíčové činnosti metodickou a legislativní podporu vycházející z následujících znalostí a zkušeností Poskytovatele:

- detailní znalost zákona č. 101/2000 Sb., o ochraně osobních údajů v aktuálním znění a navazující legislativy a prováděcích předpisů,

- znalost legislativy EU v oblasti OOÚ s důrazem na Směrnici Evropského parlamentu a Rady 2002/58/ES (ve znění pozdějších doplňků) a Nařízení Komise (EU) č. 611/2013.
- znalost pravidel a postupů při provádění OOÚ z pohledu správce a zpracovatele,
- znalost rozhodovací praxe Úřadu na ochranu osobních údajů
- znalost pravidel a postupů při implementaci a provozu mechanismů na OOÚ s důrazem na prostředí informačních a komunikačních systémů
- zkušenosti s implementací OOÚ v rozsáhlých informačních a komunikačních systémech s více jak 3.000 uživateli
- zkušenosti s odborným vzděláváním pracovníků správce a zpracovatele v oblasti OOÚ.

Poskytovatel bude zajišťovat zejména následující činnosti:

- informovat Objednatele o připravovaných či aktuálních změnách v oblasti OOÚ a navazující legislativy s důrazem na posouzení a identifikaci dopadů těchto změn do podmínek MS2014+. Jedná se o schopnost Poskytovatele proaktivně informovat Zadavatele o všech skutečnostech v oblasti OOÚ, které budou mít dopad na schválené metodiky, procesy a postupy OOÚ v rámci MS2014+. Poskytovatel k tomu bude disponovat znalostmi potřebných veřejných zdrojů informací (např. na národní úrovni zejména Sbírku zákonů a dále webové stránky Poslanecké sněmovny a vlády ČR; na evropské úrovni pak informace z Úředního věstníku Evropské unie, řady L (právní předpisy) a dále tzv. Zelené a bílé knihy Komise EU). Uvedené zdroje nejsou taxativně vymezeny, naopak je, v souladu se stanoveným rozsahem plnění v oblasti OOÚ, schopnost vymezit zdroje a jejich znalost očekávána od Poskytovatele.
- příprava návrhů, procesů a metodických postupů na základě legislativních změn v oblasti OOÚ s návrhem postupu jejich implementace do systému MS2014+,
- návrh metodických postupů a odpovědí na metodické dotazy Objednatele, Provozovatele Aplikace MS2014, Poskytovatele služeb Prostředí a uživatelů systému MS2014+.

Alokace zdrojů Poskytovatele pro činnosti v rámci Metodické a legislativní podpory Objednatele bude prováděna pouze na základě žádosti (písemné, přes ServiceDesk, atd.). Žádost je oprávněn vystavit Objednatel.

Poskytovatel je povinen vést **přehled čerpání hodin** v oblasti Metodické a legislativní podpory Objednatele a **nevyčerpané hodiny převádět** vždy do následujícího vyhodnocovacího období a to po celou dobu účinnosti Smlouvy.

3.2.2.2 Definice metodik, procesů a postupů ochrany osobních údajů a jejich prosazení do bezpečnostní dokumentace ISMS

Poskytovatel v rámci této klíčové činnosti zpracuje veškeré potřebné metodiky, procesy a postupy OOÚ formou rozšíření bezpečnostní dokumentace ISMS vytvořené v rámci Služby BS01 (viz kap. 3.1). Cílem je stanovení podmínek pro bezpečné zpracování, uchovávání a likvidaci osobních údajů (dále jen "***OÚ***") v podmínkách systému MS2014+.

Činnosti Poskytovatele musí zajistit zejména:

- Identifikaci a popis účelu zpracování osobních údajů v systému MS2014+,
- Identifikaci a vymezení prostředků zpracování OÚ v rámci MS2014+ a stanovení přesných způsobů a podmínek zpracování OÚ v těchto prostředcích,
- Stanovení kategorií OÚ, kategorií subjektů, jejichž OÚ jsou zpracovávány a kategorie příjemců, kterým bude systém MS2014+ tyto údaje poskytovat,
- Stanovení přesné identifikace zdrojů OÚ, ze kterých bude systém MS2014+ čerpat.
- Stanovit místa zpracování a délku trvání shromažďování OÚ v rámci MS2014+,

- Identifikovat a vymezit propojení MS2014+ na jiné správce nebo zpracovatele OÚ
- Definovat způsob poskytnutí souhlasu a zajištění přístupu subjektu, jehož OÚ jsou zpracovávány a shromažďovány, k těmto OÚ,
- Identifkovat a definovat předpokládané přenosy OÚ mimo ČR
- Vymezit způsob vedení přehledu o zpracování osobních údajů uživatelů systému MS2014+,
- Stanovit odpovědnosti za zpracování a ochranu OÚ v rámci systému MS2014+,
- Provést analýzu rizik souvisejících se zpracováním OÚ v systému MS2014+, vyhodnocení dopadů a návrh opatření na eliminaci identifikovaných hrozeb,
- Stanovit způsob zpracování, uchovávání a likvidace OÚ v podmínkách MS2014+,
- Určit a zdokumentovat vhodná technická a organizační opatření k OOÚ s důrazem na zabezpečení automatizovaného zpracování OÚ v systému M2014+.

Objednatel požaduje, aby činnosti v rámci této klíčové činnosti byly prováděny paralelně s přípravou systému ISMS a nedocházelo ke zbytečnému opakování činností (např. analýza rizik) a zvýšené zátěži pracovníků Objednatele a dalších subjektů na straně Objednatele, zejména Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí.

Vzhledem k tomu, že dokumentace OOÚ bude rozšířením dokumentace ISMS, platí pro její vytvoření stejné termíny a aktualizační postupy, jako pro dokumentaci ISMS.

3.2.2.3 Kontrola zpracování osobních údajů

Poskytovatel bude na denní bázi provádět kontrolní činnost v oblast dodržování zásad OOÚ v systému MS2014+. Kontroly budou zaměřeny zejména na:

- dodržování postupů zpracování, uchovávání a likvidace OÚ v podmínkách MS2014+,
- dostatečnost a adekvátnost technických a organizačních opatření OOÚ v systému MS2014+,
- úplnost kategorií, zdrojů a odběratelů OÚ v systému MS2014+,
- dodržování rozsahu zpracovávaných OÚ.

Z výsledků kontrolní činnosti bude Poskytovatel na měsíční bázi zpracovávat souhrnné reporty (specifikované v části Vyhodnocení služby) a překládat je Objednateli.

3.2.3 Vyhodnocení služby

O poskytnutí všech služeb bude připraven ze strany Poskytovatele tzv. "**Protokol o poskytnuté službě**" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující:

- Výkaz činností za oblast OOÚ
- Protokoly o provedených kontrolách OOÚ
- Přehled čerpání hodin v oblasti Metodické a legislativní podpory Objednatele

3.3 Služba „BS03_Bezpečnostní monitoring“

3.3.1 Parametry služby

Označení	Název služby		
BS03	**Bezpečnostní monitoring**		
Vymezení služby			
Lokalita	DC1, DC2	**Prostředí**	PR1, PR2
Zkrácený popis služby	Služby provádění a vyhodnocování bezpečnostního monitoringu Aplikace MS2014+		
Klíčové činnosti v rámci služby	1. Poskytnutí služby HW/SW vyhodnocovacího centra bezpečnostního monitoringu 2. Provádění průběžného monitoringu 3. Vyhledávání slabých míst 4. Stanovování provozních, technických a konfiguračních parametrů bezpečnostních prvků celého prostředí MS2014+		
Minimální rozsah služeb	**Klíčová činnost**	**Minimální rozsah v hodinách**	**Periodicita činnosti**
	Poskytnutí služby HW/SW vyhodnocovacího centra bezpečnostního monitoringu	Není relevantní	Jednorázově
	Provádění průběžného monitoringu	304	Vyhodnocovací období
	Vyhledávání slabých míst	60	Vyhodnocovací období
	Stanovování provozních, technických a konfiguračních parametrů bezpečnostních prvků celého prostředí MS2014+	56	Vyhodnocovací období
Požadované role obsazované Poskytovatelem	**Název role**	**Požadovaný rozsah alokace (z provozní doby)**	
	Bezpečnostní specialista	37	
	Bezpečnostní konzultant	22	
	Vedoucí týmu monitoringu a testování	8	
	Specialista - bezpečnostní monitoring	68	
	Specialista - monitoring	56	
	Operátor - monitoring	142	
	Specialista - tester	87	
SLA parametry služby			
Vyhodnocovací období	1 kalendářní měsíc		

Provozní doba	Poskytnutí služby HW/SW vyhodnocovacího centra bezpečnostního monitoringu	24x7x365
	Provádění průběžného monitoringu	08.00 - 16.00 (5x8) + pohotovost mimo tuto dobu
	Vyhledávání slabých míst	08.00 - 16.00 (5x8)
	Stanovování provozních, technických a konfiguračních parametrů bezpečnostních prvků celého prostředí MS2014+	08.00 - 16.00 (5x8)

Parametr	**Jednotka**	**Hodnota**	**Max počet za období**
Minimální dostupnost	[%/období]	99,7	-
Lhůty při vyřizování požadavku/incidentu			
Lhůta pro potvrzení přijetí	[min]	5	-
Lhůta pro informování o způsobu a odhadu délky řešení	[min]	15	-
Garantovaná doba zahájení řešení	[min]	15	-
Lhůty při řešení požadavku/incidentu			
Kategorie A	[hod]	2	1
Kategorie B	[hod]	4	2
Kategorie C	[dny]	ND[2]	5

Cena služby			
Položka	**Cena v Kč bez DPH**	**DPH 21%**	**Cena v Kč s DPH**
Paušální cena za vyhodnocovací období	282 084,47 Kč	59 237,74 Kč	341 322,21 Kč

Poskytovatel je povinen cenu za jednorázovou klíčovou činnost č. 1 zohlednit v rámci Paušální ceny za Vyhodnocovací období. Objednatel bude Službu hradit pouze formou úhrady paušální ceny.

3.3.1.1 Vysvětlivky

Minimální rozsah služeb - tento oddíl tabulky specifikuje minimální rozsah poskytnutých kapacit Poskytovatele pro zajištění požadované činnosti pro danou periodu. Výsledný rozsah stanoví Poskytovatel na základě svých znalostí a zkušeností tak, aby odpovídal legislativním předpisům, odborným doporučením a požadavkům na kvalitu a SLA. Rozsah plnění ze strany Poskytovatele nebude v rámci této klíčové činnosti omezen a to i v takovém případě, pokud množství aktuálně provedených činností (v návaznosti na předmět činností) bude vyšší, než Objednatelem deklarovaný minimální rozsah Služby a není důvodem pro změnu výše paušální ceny za poskytovanou Službu.

[2] ND (Next Day) - následující den

Požadované role obsazované Poskytovatelem - Poskytovatel uvede v položce **Rozsah alokace (z provozní doby)** pro danou roli očekávaný rozsah hodin, které bude pro výkon dané činnosti alokovat tak, aby byly garantovány požadované SLA parametry příslušné činnosti/služby. Výsledný rozsah hodin za všechny role pro danou činnost musí být roven nebo větší minimálnímu rozsahu služby uvedenému v předcházející části tabulky. Rozsah alokace pro jednotlivé role musí odpovídat povaze dané činnosti.

Paušální cenu za vyhodnocovací období uvede Poskytovatel s přesností na dvě (2) desetinná místa.

3.3.2 Popis a parametry činností

3.3.2.1 Poskytnutí služby HW/SW vyhodnocovacího centra bezpečnostního monitoringu

Poskytovatel **formou služby** zajistí instalaci, implementaci, provoz a správu **HW/SW vyhodnocovacího centra bezpečnostního monitoringu** včetně potřebných HW komponent, licencí SW a licencí podpory výrobců HW/SW. Vyhodnocovacím centrem bezpečnostního monitoringu je myšlen HW/SW nástroj na provádění aktivního a proaktivního monitoringu, sběr, analýzu, korelace a kontroly auditních dat a informací shromažďovaných systémem MS2014+. Zadavatel výslovně upozorňuje, že nemá zájem na nákupu vyhodnocovacího centra bezpečnostního monitoringu a tedy se nejedná o dodávku předmětných komponent.

Objednatel a Poskytovatel služeb Prostředí ve spolupráci s Provozovatelem Aplikace MS2014+ zajistí v systému MS2014+ nastavení a implementaci komplexní funkcionality pro vytváření auditních záznamů a to jak provozních, tak bezpečnostně relevantních událostí na všech vrstvách systému MS2014+. Poskytovatel služeb Prostředí zároveň implementuje řadu bezpečnostních mechanismů (např. FW ochrana systému MS2014+ nebo IDS/IPS systém). Systém MS2014+ bude mít zajištěn nepřetržitý provozní monitoring a základní bezpečnostní monitoring, s centrálním managementem řešeným komponentou HP ArcSight AE-7506.

Účelem HW/SW vyhodnocovacího centra a cílem služeb Poskytovatele je **zajištění aktivního sledování, preventivního bezpečnostního dohledu a proaktivního monitoringu systému MS2014+** a to na základě zpracování a vyhodnocení auditních informací vytvářených systémem MS2014+.

Objednatel stanovil na HW/SW vyhodnocovací centrum následující požadavky a podmínky:

- řešení HW/SW vyhodnocovacího centra bude zajištěno specifickou HW/SW apliancí pokrývající a zajišťující zejména služby označované jako SIEM (Security Information and Event Management a navazující služby v oblasti Threat Management, resp. Unified Threat Management (UTM).
- z důvodů bezpečnostních požadavků Objednatel nepřipustí zasílání a zpracování auditních logů mimo prostředí MS2014+,
- řešení vyhodnocovacího centra proto musí být formou HW apliance s dostatečnou diskovou kapacitou pro ukládání a operace nad auditními záznamy. Čistá disková kapacita HW apliance, určená a vyhrazená pro vlastní ukládání auditních zaznámů, bude minimálně 6 TB. Objednatel požaduje, aby HW apliance byla schopná ukládat veškeré auditní záznamy minimálně po dobu 2 kalendářních měsíců a získané výsledky (výstupy analytických činností, korelované záznamy a identifikované hrozby a zranitelnosti) musí být ukládány minimálně pod dobu 1 kalendářního roku).
- Apliance bude určena pro montáž do 19" racku a bude mít maximální výšku 4U (nebo 2x2U). Pro zařízení této velikosti má Objednatel připravený a vyčleněný prostor v rámci rackových

skříní Prostředí MS2014+ a pro zařízení bude zajištěno potřebné napájení, chlazení a konektivita,
- zařízení musí být určeno pro nepřetržitý provoz v režimu 24x7x365 a bude obsahovat redundantní napájecí zdroje a další klíčové komponenty,
- součástí bude SW centrum pro nastavování požadovaných operací nad auditními záznamy, nastavení sledovaných parametrů chování (tresholdů) a robustní reporting,
- k zařízení bude Poskytovatel přistupovat pomocí vzdáleného přístupu, Objednatel nepřipouští (s výjimkou instalace nebo servisního zásahu u vyhodnocovacího centra) přístup pracovníků Poskytovatele do režimové zóny serverovny MS2014+ v rámci datového centra. Poskytovatel za tímto účelem poskytne Poskytovateli služeb Prostředí kompletní přehled komunikačních protokolů, portů a potřebných síťových služeb, které bude pro vzdálený přístup k vyhodnocovacímu centru nebytně potřebovat. Na základě tohoto přehledu Poskytovatel služeb Prostředí zajistí konfiguraci nezbytných komunikačních prostupů pro přístup Poskytovatele do datového centra za účelem vzdálené správy vyhodnocovacího centra.
- řešení musí být škálovatelné tak, aby v případě potřeby bylo možné vyhodnocovací centrum posílit (kapacitně i výkonově),
- řešení musí být schopné zpracovat vstupní tok auditních záznamů v rozsahu minimálně 5000 EPS (Events per Second),
- schopnost pracovat s různými typy auditních záznamů (SYSLOG, EventLog, SNMP trapy),
- součástí řešení budou veškeré potřebné SW licence,
- Poskytovatel bude mít pro řešení zajištěnu technickou podporu HW a SW u výrobce v rozsahu 24x7x365 s SLA 99,8% a dobou reakce do 6h od nahlášení on-site. Součástí podpory musí být i nezbytné SW licence podpory, např. pro pravidelnou aktualizaci databáze zranitelností a další.
- zařízení musí být schopné provádět monitoring a dohled v pasivním i aktivním režimu. Pasivním režimem jsou primárně myšleny analytické činnosti nad databází auditních záznamů, kterou bude vytvářet MS2014+. Aktivním režimem je myšlena schopnost provádění automatizovaného sběru auditních záznamů z jednotlivých komponent MS2014+, jejich ukládání do interní databáze HW/SW vyhodnocovacího centra s následným prováděním analytických činností nad touto databází. V aktivním režimu musí být zařízení schopné provádět proaktivní monitoring ve formě řízení a provádění akcí nad jednotlivými zařízeními (např. změna FW pravidel v návaznosti na zjištěný počítačový útok, blokace IP adres, apod) v návaznosti na detekované hrozby a zranitelnosti. Zadavatel primárně předpokládá nasazení HW/SW vyhodnocovacího centra v režimu aktivního monitoringu.
- Za účelem aktivního monitoringu a schopnosti provádět akce v proaktivním režimu musí mít navržené zařízení HW/SW vyhodnocovacího centra podporovat HW a SW komponenty, ze kterých se řešení MS2014+ skládá, přičemž podporou je zde myšlena schopnost integrace HW/SW vyhodnocovacího centra přímo na komponenty MS2014+, např. formou rozhraní pro sběr auditních záznamů, existencí agenta monitorovacího systému, atd.

Pro správné pochopení rozsahu prostředí, technického řešení, použitých HW a SW komponent a platforem, datových toků na úrovni jednotlivých vrstev systému MS2014+ tak, aby byl Poskytovatel schopen navrhnout optimální a vhodné řešení, vyjde Poskytovatel:
- z technických informací uvedených v rámci zadávacího řízení "Pořízení HW platformy a Infrastruktury serverovny pro MS2014+", uveřejněného na profilu Objednatele (https://ezak.mmr.cz/contract_display_823.html) s důrazem na Přílohu č. 1 Smlouvy o dílo a Přílohu č. 1 Servisní smlouvy.
- z technických informací uvedených v rámci zadávacího řízení "HW a SW vybavení pro záložní pracoviště Aplikace MS2014+", v rámci kterého bude zálohovací lokalita povýšena na lokalitu záložní s předpokladaným výkonem a sizingem na úrovni 50% lokality primární. Toto zadávací

řízení je rovněž zveřejněno na profilu Objednatele (viz https://ezak.mmr.cz/contract_display_868.html).

Poskytovatel bude při návrhu kapacitních a výkonových parametrů HW/SW vyhodnocovacího centra vycházet z celkového rozsahu prostředí MS2014+ daného oběma uvedenými zadávacími řízeními.

Vzhledem k rozdělení odpovědností subjektů zúčastněných v řešení systému MS2014+ není přípustné, aby Poskytovatel Bezpečnostního dohledu jakýmkoliv způsob modifikoval a doplňoval provozní prostředí systému MS2014+ (např. formou instalace vlastních monitorovacích agentů nebo sond) bez schvalovacího procesu na straně Objednatele. Každá modifikace MS2014+ bude posuzována z hlediska dopadů na danou komponentu (např. vliv instalace monitorovacího agenta, požadovaný rozsah a četnost vytváření auditních záznamů, atd.) a Objednatel tuto modifikaci schválí na základě souhlasného stanoviska Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí. Poskytovatel Bezpečnostního dohledu proto bude řešení bezpečnostního monitoringu připravovat vždy v úzké součinnosti s těmito subjekty.

Objednatel požaduje, aby vyhodnocovací centrum bezpečnostního monitoringu bylo funkční, tedy implmentované v datovém centru, instalované a propojené na úrovni komunikační infrastruktury a datových toků a s vazbou na ServiceDesk systému MS2014+, nejpozději **1 kalendářní měsíc** od data účinnosti této Smlouvy.

Nejpozději **do 3 kalendářních měsíců** od data účinnosti této Smlouvy musí Poskytovatel zajisitit plnou funkcionalitu vyhodnocovacího centra bezpečnostního monitoringu v rozsahu definovaném touto Službou BS03, zejména pak službami nezbytnými pro klíčové činnosti 2 až 4.

Činnosti zajišťované Poskytovatelem v rámci Vyhodnocovacího centra a této Služby jsou specifikovány v rámci následujících klíčových činností.

3.3.2.2 Provádění průběžného bezpečnostního monitoringu

Poskytovatel bude zajišťovat a provádět průběžný bezpečnostní monitoring systému MS2014+ za účelem poskytnutí nepřetržitého dohledu nad stavem bezpečnosti systému MS2014+, zajištění schopnosti proaktivní, včasné reakce na bezpečnostně relevantní události a shromažďování důkazů a podkladů pro řešení bezpečnostních incidentů.

Poskytovatel bude zajišťovat zejména následující činnosti:

- analytickou činnost nad bezpečnostními událostmi v systému MS2014+, hledání a nalezení příčin událostí, anomálních chování, bezpečnostních hrozeb a podobně - v současnosti komplexně označováno jako Threat Management,
- sledování anomálií běžného provozu Aplikace MS2014+ a Prostředí a jejich vyhodnocování,
- průběžná optimalizace parametrů chování sledovacích systémů (tresholdů), označování false positive incidentů,
- kontrola vlastních bezpečnostních pravidel, systémů bezpečnostní infrastruktury,
- detekce úspěšných i neúspěšných pokusů o narušení bezpečnosti,
- průběžný bezpečnostní audit logů (korelace, agregace, vyhodnocování a uchovávání).

Prováděný bezpečnostní monitoring musí být schopen komplexním způsobem dokládat aktuální stav prostředí z hlediska bezpečnosti a v detailu umožňujícím provedení adekvátních reakcí (viz následující klíčové činnosti v částech 3.3.2.3 a 3.3.2.4 a činnosti vyplývající z povinností v rámci řešení bezpečnostních incidentů dle části 3.1.2.3)

Z hlediska zajištění této klíčové činnosti stanovuje Objednatel následující požadavky:

- vyhodnocovací centrum (viz kap. 3.3.2.1) bude provozováno nepřetržitě,
- Objednatel nepožaduje v rámci klíčové činnosti průběžného bezpečnostního monitoringu u vyhodnocovacího centra nepřetržitou obsluhu operátorem v režimu 24x7x365. Obsluha bude zajištěna pouze v pracovní dny v režimu 5x8 (08.00-16.00), mimo tuto dobu bude Poskytovatel zajišťovat pouze pohotovost tak, aby byl schopen zareagovat a aktivovat procesy podpory systému MS2014+ v případě detekce bezpečnostně relevantních incidentů (např. kybernetický útok).

3.3.2.3 Vyhledávání slabých míst

Poskytovatel musí být schopen na základě prováděného průběžného bezpečnostního monitoringu identifikovat slabá místa v systému MS2014+ a posoudit je z pohledu vhodnosti a dostatečnosti implementovaných bezpečnostních opatření.

Poskytovatel bude sledovat aktuální trendy v oblasti bezpečnosti (nové hrozby, reakce výrobců, způsoby jejich eliminace, atd.) a to v rozsahu technologií a služeb systému MS2014+. V souvislosti se získanými informacemi bude provádět proaktivní ověřování aktuálního stavu prostředí MS2014+ s cílem odhalit slabá a nezabezpečená místa minimálně v těchto oblastech:

- porovnávání aktuálního stavu hardware a software s přehledem známých zranitelností, týkajících se těchto systémů a jejich konkrétních verzí a patchů,
- kontrola provedených aktualizací firmware, operačních systémů, databázových a aplikačních platforem a antivirových řešení s důrazem na implementaci dostupných bezpečnostních update, patchů, hotfixů, servicepacků a virových databází
- kontrola provedených změn v konfiguracích systémů a jejich verifikace,
- doporučení k odstranění nepoužívaných nebo nadbytečných síťových služeb, služeb operačních systémů a aplikací za účelem snížení možných zranitelných míst, nadbytečné komunikace, otevřených portů a provedení hardeningu jednotlivých komponent systému MS2014+.

V návaznosti na tyto skutečnosti bude vydávat doporučení Provozovateli Aplikace MS2014+ a Poskytovateli služeb Prostředí s cílem zajistit instalaci, implementaci nebo rekonfiguraci určených prvků, komponent, konfiguračních položek, případně jiných oblastí.

Poskytovatel bude zajišťovat Služby v oblasti vyhledávání slabých míst **na denní bázi v pracovní dny**.

3.3.2.4 Stanovování, schvalování a kontrola provozních, technických a konfiguračních parametrů bezpečnostních prvků celého Prostředí a Aplikace MS2014+

Poskytovatel bude po celou dobu poskytování Služeb nedílnou součástí nastavených procesů řízení IT služeb, implementovaných v provozním Prostředí a Aplikaci MS2014+ a zastřešených v rámci ServiceDesku MS2014+. Jde zejména o procesy:

- Incident a Request Management.
- Change a Release Management.
- Problem Management.
- Configuration Management.
- Service Level Management.

V rámci uvedených procesů bude Poskytovatel zařazen do eskalačních procedur a bude se podílet na řešení jednotlivých požadavků a incidentů a stanovování, schvalování a kontrole provozních, technických a konfiguračních parametrů bezpečnostních prvků celého Prostředí a Aplikace MS2014+.

Objednatel požaduje zajištění zejména následujících činností:

- zpracování stanovisek ke změnovým požadavkům z pohledu dopadů navrhovaných změn do bezpečnostních parametrů MS2014+,
- schvalování bezpečnostních pravidel, konfigurací bezpečnostních mechanismů a jejich změn u jednotlivých komponent systému MS2014+,
- koordinace činností, změny rozsahu funkcionality, návrh optimalizace a nápravných opatření u bezpečnostních prvků systému MS2014+ (FW, IDS/IPS, atd.),
- řešení bezpečnostních incidentů v souladu s klíčovou činností dle kap. 3.1.2.3,
- verifikace provedení změn v systému MS2014+.

Poskytovatel bude v rámci této klíčové činnosti úzce spolupracovat se správci a administrátory Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí, kteří budou vlastní zásahy a změny na komponentách systému MS2014+ provádět. Poskytovatel je povinen v případě potřeby poskytnout nezbytnou součinnost a odbornou pomoc i v průběhu vlastní implementace schválené změny nebo opatření.

3.3.3 Vyhodnocení služby

O poskytnutí všech služeb bude připraven ze strany Poskytovatele tzv. "**Protokol o poskytnuté službě**" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující:

- Zpráva o průběhu bezpečnostního monitoringu a stavu vyhodnocovacího centra
- Přehled identifikovaných slabých míst a doporučení pro jejich odstranění včetně termínu, kdy bylo doporučení implementováno nebo odůvodněně zamítnuto.

3.4 Služba „BS04_Kontrola kvality poskytovaných služeb“

3.4.1 Parametry služby

Označení	**Název služby**			
BS04	**Kontrola kvality poskytovaných služeb**			
Vymezení služby				
Lokalita	DC1, DC2	**Prostředí**	PR1, PR2	
Zkrácený popis služby	Služby kontroly a vyhodnocování kvality služeb (SLA) všech subjektů podílejících se na realizaci, provozu, správě a podpoře Aplikace MS2014+			
Klíčové činnosti v rámci služby	1. Kontrola a vyhodnocení parametrů poskytovaných služeb 2. Dohled nad poskytovateli služeb a dodržováním závazných smluvních parametrů služeb			
Minimální rozsah služeb	**Klíčová činnost**	**Minimální rozsah v hodinách**	**Periodicita činnosti**	
	Kontrola a vyhodnocení parametrů poskytovaných služeb	32	Vyhodnocovací období	
	Dohled nad poskytovateli služeb a dodržováním závazných smluvních parametrů služeb	16		
Požadované role obsazované Poskytovatelem	**Název role**	**Požadovaný rozsah alokace (z provozní doby)**		
	Vedoucí týmu informační bezpečnosti	5		
	Bezpečnostní specialista	9		
	Bezpečnostní konzultant	7		
	Vedoucí týmu monitoringu a testování	7		
	Specialista - bezpečnostní monitoring	10		
	Specialista - monitoring	10		
SLA parametry služby				
Vyhodnocovací období	1 kalendářní měsíc			
Provozní doba	08.00 - 16.00 (5x8)			
Parametr	**Jednotka**	**Hodnota**	**Max počet za období**	

Minimální dostupnost	[%/období]	99,5	-
Lhůty při vyřizování požadavku/incidentu			
Lhůta pro potvrzení přijetí	[min]	5	-
Lhůta pro informování o způsobu a odhadu délky řešení	[min]	15	-
Garantovaná doba zahájení řešení	[min]	15	-
Lhůty při řešení požadavku/incidentu			
Kategorie A	[hod]	4	-
Kategorie B	[hod]	8	-
Kategorie C	[dny]	NBD	-

Cena služby			
Položka	**Cena v Kč bez DPH**	**DPH 21%**	**Cena v Kč s DPH**
Paušální cena za vyhodnocovací období	26 300,00 Kč	5 523,00 Kč	31 823,00 Kč

3.4.1.1 Vysvětlivky

Minimální rozsah služeb - tento oddíl tabulky specifikuje minimální rozsah poskytnutých kapacit Poskytovatele pro zajištění požadované činnosti pro danou periodu. Výsledný rozsah stanoví Poskytovatel na základě svých znalostí a zkušeností tak, aby odpovídal legislativním předpisům, odborným doporučením a požadavkům na kvalitu a SLA. Rozsah plnění ze strany Poskytovatele nebude v rámci této klíčové činnosti omezen a to i v takovém případě, pokud množství aktuálně provedených činností (v návaznosti na předmět činností) bude vyšší, než Objednatelem deklarovaný minimální rozsah Služby a není důvodem pro změnu výše paušální ceny za poskytovanou Službu.

Požadované role obsazované Poskytovatelem - Poskytovatel uvede v položce **Rozsah alokace (z provozní doby)** pro danou roli očekávaný rozsah hodin, které bude pro výkon dané činnosti alokovat tak, aby byly garantovány požadované SLA parametry příslušné činnosti/služby. Výsledný rozsah hodin za všechny role pro danou činnost musí být roven nebo větší minimálnímu rozsahu služby uvedenému v předcházející části tabulky. Rozsah alokace pro jednotlivé role musí odpovídat povaze dané činnosti.

Paušální cenu za vyhodnocovací období uvede Poskytovatel s přesností na dvě (2) desetinná místa.

3.4.2 Popis a parametry činností

V rámci Služby BS04 bude Poskytovatel vykonávat ve prospěch Objednatele roli nezávislého dozoru a kontroly a vyhodnocování kvality plnění služeb (SLA) všech subjektů podílejících se na realizaci, provozu, správě a podpoře Aplikace MS2014+.

3.4.2.1 Kontrola a vyhodnocení parametrů poskytovaných služeb

Kontrolní činnost Poskytovatele bude zaměřena zejména na kvalitu plnění služeb Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí. Oba uvedené subjekty mají v rámci svých služeb

povinnost provádět a dokládat Objednateli pravidelný reporting vyhodnocování a dodržování SLA jednotlivých služeb a činností za Vyhodnocovací období, v průběhu kterého byly služby poskytovány nebo zajišťovány.

Poskytovatel bude v rámci této klíčové činnosti povinen:

- **provést** kontrolu výkazů, protokolů o poskytnuté službě, reportů a dalších relevantních dokumentů, předkládaných Provozovatelem Aplikace MS2014+ a Poskytovatelem služeb Prostředí v rámci doložení splnění SLA Objednateli,
- **porovnat** uvedené dokumenty s výsledky vlastního monitoringu (viz Služba BS03), provedených šetření a kontrol, závěry v oblasti Change Managementu a Incident Managementu,
- **formulovat** zjištění z provedené kontroly a porovnání a upozornit Objednatele na možné neshody, rozpory či nedostatky. Mimo jednotlivá zjištění je Poskytovatel povinen sdělit Objednateli **celkový závěr v oblasti dodržení SLA** ze strany jednotlivých kontrolovaných subjektů. Závěr musí jednoznačně potvrdit nebo vyvrátit výkazy předkládané Provozovatelem Aplikace MS2014+ a Poskytovatelem služeb Prostředí.

Objednatel pro účely této klíčové činnosti v rámci součinnosti zajistí Poskytovateli přístup ke všem relevantním výkazům, reportům a dalším dokumentům, které budou předmětem kontrolní činnosti Poskytovatele a to zejména cestou ServiceDesku MS2014+, v rámci kterého budou tyto dokumenty primárně ukládány.

Na základě získaných informací z kontrol kvality a vyhodnocení parametrů služeb bude Poskytovatel zajišťovat podporu Objednatele v rámci řešení sporů kontrolovaných subjektů při stanovování odpovědností za zjištěný stav, způsobení incidentu nebo odpovědností za provedení nápravy zjištěného stavu. Poskytovatel bude arbitrem zejména mezi Provozovatelem Aplikace MS2014+ a Poskytovatelem služeb Prostředí.

Poskytovatel je povinen kontrolní činnost provést a předkládat Objednateli její výsledky vždy do **5-ti pracovních dní** od předání výkazů a reportingu SLA za dané Vyhodnocovací období Provozovatelem Aplikace MS2014+ a Poskytovatelem služeb Prostředí Objednateli.

3.4.2.2 Dohled nad poskytovateli služeb a dodržováním závazných smluvních parametrů služeb

Cílem činností Poskytovatele je podpora Objednatele prováděním dohledu nad jednotlivými subjekty podílejícími se na řešení, provozu a rozvoji systému MS2014+. Rozsah služeb dohledu a vyhodnocování je doplněním činností v oblasti kontroly kvality (úzce navazuje na činnosti uvedené v kap. 3.4.2.1) a je zaměřen na plnění předmětu smluvních ujednání mezi Objednatelem a ostatními subjekty v rámci systému MS2014+ s důrazem na Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí.

Poskytovatel bude v rámci této klíčové činnosti zajišťovat:

- **Posouzení výsledků a závěrů z kontroly kvality** (viz kap. 3.4.2.1) vůči znění smluvně stanovených požadavků na SLA u jednotlivých kontrolovaných subjektů a identifikace oblastí smluv, v rámci kterých nebyly smluvně zajištěné SLA parametry dodrženy v kontrolovaném Vyhodnocovacím období,
- **Kontrolu dodržování závazných smluvních parametrů** s důrazem na:
    - naplňování smluvních cílů a rozsahu předmětu plnění,

- dodržování stanovených harmonogramů, milníků, časových lhůt a dalších parametrů vymezujících postup plnění projektů, provozních a rozvojových činností v závislosti na čase,
- úroveň organizace lidských zdrojů a komunikace v rámci plnění, včetně dodržování plnění smluvně stanovenými pracovníky, dodržování komunikačních matic a požadavků na ochranu dat a informací MS2014+ při výměně informací s a mezi třetími stranami,

- **Posouzení dopadů změn do smluvních vztahů** s cílem upozornit Objednatele na možná rizika vyplývající ze schválených změn a jejich vlivu na předmět plnění, jeho rozsah a kvalitu, harmonogram a milníky jednotlivých projektů a zdroje,
- **Dostatečnost akceptačních postupů a kritérií** pro přebírání plnění Objednatelem s důrazem na vhodnost a úplnost akceptačních scénářů a testů z hlediska jejich schopnosti ověřit předmět akceptace.

Poskytovatel bude poskytovat tuto Službu průběžně dle potřeb a postupu plnění jednotlivých dohledovaných subjektů. U činnosti "Posouzení výsledků a závěrů z kontroly kvality" (viz první odrážka výše) je Poskytovatel povinen předkládat její výsledky spolu se závěry z klíčové činnosti dle kap. 3.4.2.1 vždy do **5-ti pracovních dní** od předání výkazů a reportingu SLA za dané Vyhodnocovací období Provozovatelem Aplikace MS2014+ a Poskytovatelem služeb Prostředí Objednateli.

3.4.3 Vyhodnocení služby

O poskytnutí všech služeb bude připraven ze strany Poskytovatele tzv. "**Protokol o poskytnuté službě**" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující:

- Zpráva o posouzení výsledků a závěrů z kontroly kvality
- Stav dodržování smluvních parametrů služeb u kontrolovaných subjektů
- Návrhy a doporučení pro řešení zjištěných negativních výsledků

3.5 Služba „BS05_Audit prostředí“

3.5.1 Parametry služby

Označení	Název služby		
BS05	**Audit prostředí**		
Vymezení služby			
Lokalita	DC1, DC2	**Prostředí**	PR1, PR2
Zkrácený popis služby	Služby provádění auditních činností a součinnosti při provádění auditů Aplikace MS2014+		
Klíčové činnosti v rámci služby	1. Penetrační testy 2. Kontroly dodržování pravidel informační bezpečnosti 3. Součinnost při auditech a kontrolách 4. Součinnost při certifikacích		
Minimální rozsah služeb	**Klíčová činnost**	**Minimální rozsah v hodinách**	**Periodicita činnosti**
	Penetrační testy	56	Vyhodnocovací období
	Kontroly dodržování pravidel informační bezpečnosti	56	
	Součinnost při auditech a kontrolách	160	Ročně
	Součinnost při certifikacích	80	Ročně
Požadované role obsazované Poskytovatelem	**Název role**	**Požadovaný rozsah alokace (z provozní doby)**	
	Vedoucí týmu informační bezpečnosti	5,67 *(rozsah alokace ročních činností je zahrnut jako poměrná část (1/12) do alokace za vyhodnocovací období)	
	Bezpečnostní specialista	39,17 *(rozsah alokace ročních činností je zahrnut jako poměrná část (1/12) do alokace za vyhodnocovací období)	
	Bezpečnostní konzultant	22,33 *(rozsah alokace ročních činností je zahrnut jako poměrná část (1/12) do alokace za vyhodnocovací období)	
	Vedoucí týmu monitoringu a testování	5,67 *(rozsah alokace ročních činností je zahrnut jako poměrná část (1/12) do alokace za vyhodnocovací období)	
	Specialista - bezpečnostní monitoring	12,25 *(rozsah alokace ročních činností je zahrnut jako poměrná část (1/12) do alokace za vyhodnocovací období)	
	Specialista - tester	46,92 *(rozsah alokace ročních činností je zahrnut jako poměrná část (1/12) do alokace za vyhodnocovací období)	
SLA parametry služby			

Vyhodnocovací období	1 kalendářní měsíc		
Provozní doba	08.00 - 16.00 (5x8) Poskytovatel je povinen upravit pracovní dobu dle potřeb a podmínek pro penetrační testování nebo kontrolních a certifikačních orgánů		
Parametr	**Jednotka**	**Hodnota**	**Max počet za období**
Minimální dostupnost	[%/období]	99,5	-
Lhůty při vyřizování požadavku/incidentu			
Lhůta pro potvrzení přijetí	[min]	5	-
Lhůta pro informování o způsobu a odhadu délky řešení	[min]	15	-
Garantovaná doba zahájení řešení	[min]	15	-
Lhůty při řešení požadavku/incidentu			
Kategorie A	[hod]	4	1
Kategorie B	[hod]	8	2
Kategorie C	[dny]	NBD	5

Cena služby			
Položka	**Cena v Kč bez DPH**	**DPH 21%**	**Cena v Kč s DPH**
Paušální cena za vyhodnocovací období	67 905,92 Kč	14 260,24 Kč	82 166,16 Kč

Poskytovatel je povinen cenu za roční klíčové činnosti č. 3 a 4 zohlednit v rámci Paušální ceny za Vyhodnocovací období. Objednatel bude Službu hradit pouze formou úhrady paušální ceny.

3.5.1.1 Vysvětlivky

Minimální rozsah služeb - tento oddíl tabulky specifikuje minimální rozsah poskytnutých kapacit Poskytovatele pro zajištění požadované činnosti pro danou periodu. Výsledný rozsah stanoví Poskytovatel na základě svých znalostí a zkušeností tak, aby odpovídal legislativním předpisům, odborným doporučením a požadavkům na kvalitu a SLA. Rozsah plnění ze strany Poskytovatele nebude v rámci této klíčové činnosti omezen a to i v takovém případě, pokud množství aktuálně provedených činností (v návaznosti na předmět činností) bude vyšší, než Objednatelem deklarovaný minimální rozsah Služby a není důvodem pro změnu výše paušální ceny za poskytovanou Službu.

Požadované role obsazované Poskytovatelem - Poskytovatel uvede v položce **Rozsah alokace (z provozní doby)** pro danou roli očekávaný rozsah hodin, které bude pro výkon dané činnosti alokovat tak, aby byly garantovány požadované SLA parametry příslušné činnosti/služby. Výsledný rozsah hodin za všechny role pro danou činnost musí být roven nebo větší minimálnímu rozsahu služby uvedenému v předcházející části tabulky. Rozsah alokace pro jednotlivé role musí odpovídat povaze dané činnosti.

Paušální cenu za vyhodnocovací období uvede Poskytovatel s přesností na dvě (2) desetinná místa.

3.5.2 Popis a parametry činností

3.5.2.1 Penetrační testy

Poskytovatel bude zajišťovat komplexní a detailní ověření aktuálního stavu bezpečnosti systému MS2014+ formou provedení **penetračních testů**.

Objednatel požaduje v rámci této klíčové činnosti **naplnění následujících cílů**:

- ověření stavu informační bezpečnosti systému MS2014+ z hlediska existence zranitelností a slabých míst,
- detekce nezabezpečených míst, nadbytečných nebo nepoužívaných služeb a konfiguračních parametrů na všech vrstvách systému,
- vytvoření podkladů pro návrh vylepšení technických a konfiguračních parametrů systému MS2014+ (viz Služba BS03, kap. 3.3.2.4).

Při provádění penetračních testů bude Poskytovatel vycházet z předem definované **Metodiky provádění penetračních testů MS2014+**, která bude založena na mezinárodních standardech a doporučeních pro provádění testů ICT (např. OSSTMM – Open Source Security Testing Methodology Manual). Objednatel požaduje, aby metodika byla navržená důsledně se zohledněním následujících cílů:

- bude řešit **postupy a metody pro ověření systému** MS2014+ formou:
    - bezpečnostních testů z vnějšího prostředí
    - bezpečnostních testů z vnitřního prostředí
    - konfiguračních testů
- navržené metody budou vycházet ze situace, kdy **má tester stejná práva jako běžný uživatel**,
- navržené metody budou obsahovat postupy a bezpečnostní testy pro **ověření webové části MS2014+** dle metodiky OWASP (www.owasp.org - Open Web Application Security Project) s využitím OWASP projektu pro 10 nejznámějších zranitelností - **OWASP TOP TEN 2013** (vždy v aktuálním znění při provádění předmětných testů webových aplikací - detailně viz https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project), kdy Poskytovatel zajistí ověření zranitelnosti systému MS2014+ na následující zranitelnosti:
    - A1 Injection - Chyby na bázi vkládání
    - A2 Broken Authentication and Session Management - Chybná správa sezení a autentizace
    - A3 Cross-Site Scripting (XSS)
    - A4 Insecure Direct Object References - Nezabezpečený přímý odkaz na objekt
    - A5 Security Misconfiguration - Chyby v konfiguraci
    - A6 Sensitive Data Exposure - Vystavení citlivých dat
    - A7 Missing Function Level Access Control - Chybějící funkce pro řízení přístupu
    - A8 Cross-Site Request Forgery (CSRF)
    - A9 Using Components with Known Vulnerabilities - Využití komponent se známými zranitelnostmi
    - A10 Unvalidated Redirects and Forwards - Neošetřené přesměrování
- bude obsahovat **přehled nástrojů**, které bude Poskytovatel využívat, přičemž Objednatel požaduje uvést důsledné rozlišení na komerční nástroje a nástroje vyvinuté Poskytovatelem. U nástrojů (podléhajících licenčním, autorským a jiným právům) musí být součástí závazek Poskytovatele o tom, že použití těchto nástrojů, jejich reporting a další využití pro potřeby testování MS2014+ neznamená žádné další náklady pro Objednatele.
- Volbu nástrojů musí Poskytovatel přizpůsobit skutečnosti, že Objednatel **nepřipustí využití** jakýchkoliv nástrojů, které vyžadují k provedení testů a stanovení výsledků **odesílání dat k analýze na externí servery a zařízení mimo systém MS2014+**,

- Objednatel **nebude akceptovat metodiku, která je založena výhradně na použití automatizovaných nástrojů** s předvolenými sadami testů výrobcem těchto nástrojů a to z důvodu vysokého rizika false-pozitive výsledků. Využití automatizovaných nástrojů může být v celkovém objemu testů maximálně 50%.

Návrh metodiky bude doplněn o návrh sady testů v rozsahu, který komplexně pokrývá celý systém MS2014+. Testy musí být koncipovány tak, aby byly opakovatelné za účelem ověření odstranění jednotlivých zjištění nebo jako důkaz v případě potřeby důkazního materiálu na straně Objednatele, Poskytovatel je povinen provést opakování testu vždy po provedení nápravy zjištěného stavu za účelem ověření úspěšnosti opravy.
Za tímto účelem bude návrh metodiky obsahovat návrh harmonogramu provádění penetračních testů na období 4 let, přičemž Poskytovatel bude vycházet z požadavku Objednatele, který stanoví, že systém MS2014+ musí být v průběhu 1 kalendářního roku komplexně prověřen penetračními testy ve všech stanovených formách (testy z vnějšího a vnitřního prostředí a konfigurační testy). Přitom nebude připuštěno jednorázové provedení penetračních testů všech částí a vrstev systému MS2014+ z důvodu neakceptovatelné zátěže systému v případě tohoto provedení. Harmonogram provádění penetračních testů bude 1x ročně, vždy po provedení celé sady testů plánovaných na daný rok, Poskytovatelem aktualizován tak, aby plán na další roky postihoval výsledky a možné posuny v testech vyplývající z již provedených testů, jejich výsledků a časových nároků na odstranění zjištění.

Poskytovatel je povinen metodiku, vloženou na základě nabídky Poskytovatele jako Příloha č. 4 Smlouvy o poskytování služeb, doplnit a rozpracovat na základě seznámení se se skutečným stavem systému MS2014+ a předložit ji, včetně detailního harmonogramu, k akceptaci Objednateli a to do **2 kalendářních měsíců** ode dne zahájení poskytování Služeb.

3.5.2.2 Kontroly dodržování pravidel informační bezpečnosti

Poskytovatel bude provádět **pravidelné kontroly dodržování pravidel informační bezpečnosti** formou **výkonu interního auditu ISMS** a prováděním **kontrol stavu informační bezpečnosti MS2014+**.

Interní audit je procesem systematického a nezávislého ověřování, zda je ISMS v souladu s požadavky platných právních předpisů a požadavky norem řady ČSN ISO/IEC 27000.

Audit ISMS tvoří soustava organizačních a technických opatření, která zajišťují shromáždění a vyhodnocení informací o stavu bezpečnosti informací dle předem stanoveného rozsahu. Cílem interního auditu ISMS je zejména:

- získání informací o současném stavu ISMS MS2014+;
- odhalení slabých míst a nedostatků ISMS MS2014+;
- navržení doporučení, resp. nápravných, případně preventivních opatření;
- prověření splnění doporučení a účinnosti realizovaných nápravných a preventivních opatření;
- zlepšování a zvyšování efektivity ISMS MS2014+;
- prověření, zda procesy a postupy ISMS MS2014+ vyhovují požadavkům normy;
- prověření, zda procesy a postupy ISMS vyhovují určeným požadavkům na Informační bezpečnost MS2014+.

Poskytovatel bude **interní audit ISMS provádět 2x ročně** v souladu s metodickými postupy, které stanoví dokumentace ISMS (viz 3.1.2.2).

Kontroly stavu informační bezpečnosti MS2014+ budou Poskytovatelem prováděné kontroly jednotlivých oblastí ISMS a způsobu jejich implementace, prosazení a dodržování v rámci běžného provozu systému MS2014+. **Kontroly budou prováděny 1x měsíčně v rozsahu, který zajistí, že 1x za 6 měsíců dojde ke kontrole všech oblastí ISMS MS2014+**. Plán kontrol ISMS MS2014+ navrhne Poskytovatel do 1 měsíce od vytvoření dokumentační základny ISMS MS2014+ na dobu 1 roku. Měsíc před uplynutím této doby je Poskytovatel povinen předložit Objednateli ke schválení Plán kontrol ISMS MS2014+ na další rok. Z každé kontroly bude zpracován protokol o kontrole, který bude obsahovat minimálně následující informace:

- Identifikátor kontroly
- Identifikace kontrolované oblasti s uvedením přesných částí a komponent systému MS2014+ a případně dotčených subjektů a třetích stran,
- Identifikace pracovníků provádějících kontrolu za Poskytovatele
- Přesný popis (vymezení) testů a kontrolních postupů, které byly spuštěny nebo provedeny,
- Popis získaných výsledků,
- Návrh opatření k nápravě včetně návrhu subjektů/třetích stran odpovědných za jejich provedení,
- Místo pro vyjádření kontrolovaných/odpovědných subjektů k oblastem nebo výsledkům kontroly,
- Schvalovací doložku, na které Objednatel akceptuje výsledky provedené kontroly.

Obsah kontroly včetně návrhu testů nebo postupů, které budou spouštěny nebo ověřovány, je Poskytovatel povinen předložit Objednateli ke schválení nejpozději 14 dní před vlastním provedením kontroly. Dotčené/kontrolované subjekty nebo třetí strany mají právo se k rozsahu kontroly vyjádřit.

3.5.2.3 Součinnost při auditech a kontrolách

Poskytovatel bude poskytovat **součinnost při auditech a kontrolách systému MS2014+**, které budou prováděny ze strany národních nebo evropských kontrolních orgánů, vnitřních kontrolních orgánů Objednatele a případně dalších oprávněných subjektů.

Poskytovatel bude tuto součinnost poskytovat v rámci všech poskytovaných Služeb (dle oblasti, která bude předmětem auditu nebo kontroly) nebo formou poskytnutí specialistů pro poradenství Objednateli dle zaměření kontroly nebo auditu, případně formou účasti na auditech a kontrolách a spolupráce s kontrolními orgány dle potřeb kontrolních orgánů.

Poskytovatel bude počítat se součinností při auditech a kontrolách v rozsahu **20 MD ročně**. Způsob, termín a formu součinnosti Poskytovateli vždy stanoví Objednatel v návaznosti na předmět a rozsah auditu nebo kontroly, případně na základě požadavků kontrolních orgánů.

3.5.2.4 Součinnost při certifikacích

Celé řešení MS2014+ (Prostředí i Aplikace MS2014+) je informačním systémem dle zákona 365/2000 Sb. o informačních systémech veřejné správy (ISVS) v aktuálním znění. Objednatel požaduje, aby Poskytovatel zajistil **součinnost při atestu** Aplikace MS2014+ a Prostředí dle podmínek ISVS a součinnost při případné certifikaci systému řízení bezpečnosti informací (ISMS) dle normy ISO/IEC 27001. V rámci součinnosti bude Poskytovatel zajišťovat zejména:

- Účast pracovníků Poskytovatele při provádění atestu za účelem spolupráce s atestačním orgánem dle jeho potřeby.

- Přípravu aktuální verze bezpečnostní dokumentace a dokumentace ISMS ve struktuře požadované zákonem 365/2000 Sb. a na základě navazující vyhlášky 529/2006 Sb.
- Přípravu aktuální verze bezpečnostní dokumentace a dokumentace ISMS v rozsahu potřebném pro certifikaci ISMS dle ISO/IEC 27001,
- Plnění požadavků Objednatele oblasti služeb, přípravy podkladů, případně jiných výstupů či dokladů za účelem získání atestu, certifikátu ISMS nebo doplnění požadovaných informací na základě požadavků atestačního nebo certifikačního orgánu.

Poskytovatel bude počítat se součinností při certifikacích (atestech) v rozsahu **10 MD ročně**.

3.5.3 Vyhodnocení služby

O poskytnutí všech služeb bude připraven ze strany Poskytovatele tzv. "**Protokol o poskytnuté službě**" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující:

- Zpráva o provedeném penetračním testu s detailním vymezením získaných výsledků, závěrů a doporučení pro nápravu.
- Zpráva o provedených kontrolách dodržování pravidel informační bezpečnosti.
- Zpráva o poskytnutí součinnosti při auditech, kontrolách a certifikacích.

4 Matice zodpovědností

R - Responsible / Zodpovědný – Organizace je vrcholově zodpovědná za danou službu.
A - Assists / Spolupracuje – Organizace má povinnost spolupracovat a poskytovat součinnost (definovanou jejím katalogem služeb).
C - Consulted / Konzultuje –Zodpovědná organizace konzultuje způsob řešení s danou organizací, a zohledňuje obdržené informace.
I - Informed / Na vědomí – Organizace je při aktivitách v dané oblasti vždy podrobně informována Zodpovědnou organizací.

Upozorňujeme, že je použito alternativní vymezení pojmů RACI, které se oproti většinovému vymezení liší ve vymezení kompetencí R a A.

Téma	Zodpovědnost Poskytovatele	Zodpovědnost dalších dodavatelů	Zodpovědnost Zadavatele
BS01_Informační bezpečnost	R	C	A
BS02_Ochrana osobních údajů	R	C	A
BS03_Bezpečnostní monitoring	R	A	I
BS04_Kontrola kvality poskytovaných služeb	R	A	I
BS05_Audit prostředí	R	A	A

5 Podmínky poskytování služeb

5.1 Vymezení pojmů

5.1.1 Definice vad

Vada / incident kategorie A – Služby Poskytovatele nejsou použitelné ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující činnost a řádné užití Služeb Poskytovatele. Tento stav ohrožuje nebo znemožňuje výkon činnosti Bezpečnostního dohledu, případně může Objednateli a dalším subjektům způsobit větší finanční nebo jiné škody.

Vada / incident kategorie B - Rozsah Služeb Poskytovatele je ve svých funkcích degradován tak, že tento stav omezuje řádné užití Služeb Poskytovatele.

Vada / incident kategorie C - Ostatní - drobné vady, které nespadají do kategorií A a/nebo B.

		Vliv na Služby či Prostředí		
		Vysoký	Střední	Nízký
Závažnost	Vysoká	**A**	**A**	**B**
	Střední	**A**	**B**	**B**
	Nízká	**B**	**B**	**C**

5.1.2 Definice lhůt

Lhůta pro potvrzení přijetí je chápána jako doba od přijetí události (tj. žádosti / dotazu / požadavku / apod.) od uživatele systému po odeslání potvrzení o jejím přijetí pracovníky zajišťujícími službu Servicedesku tomuto uživateli (žadateli). Potvrzení o přijetí musí být odesláno systémem pro zasílání zpráv v rámci ServiceDesku. Do lhůty o informování o vyřešení události se počítá pouze provozní doba.

Lhůta pro informování o způsobu a odhadu délky řešení je doba, jejímž začátkem je čas zaslání potvrzení o přijetí události žadateli a koncem je vlastní zaslání informací o způsobu řešení a odhadu délky vyřešení/vyřízení události zpět žadateli. V této době musí být od odpovědných pracovníků provozu nebo odpovědného subjektu získána základní informace o způsobu vyřešení/vyřízení události a rámcovém odhadu délky řešení. Do lhůty o informování o vyřešení události se počítá pouze provozní doba.

Garantovaná doba zahájení řešení je doba od informování o způsobu a odhadu délky řešení po vlastní zahájení prací na řešení požadavku žadatele. Do garantované doby zahájení řešení se počítá pouze provozní doba.

Lhůty při řešení požadavku/incidentu jsou termíny od zaslání potvrzení přijetí požadavku do finálního vyřešení požadavku/incidentu.

Vyhodnocovací období je doba, v rámci které se počítají stanovené SLA parametry a vyhodnocuje jejich splnění.

Konkrétní hodnoty a parametry jednotlivých lhůt jsou stanoveny v rámci specifikace Služeb Poskytovatele v Příloze č. 1 Servisní smlouvy - Katalogu služeb.

5.1.3 Definice dob

Obvyklá **Provozní doba je doba od 08:00 do 16:00 hod.** každý pracovní den v roce s výjimkou dnů víkendu (sobota, neděle), státních svátků a ostatních svátků (dle definice zákona č. 245/2000 Sb., o státních svátcích, o ostatních svátcích, o významných dnech a o dnech pracovního klidu, ve znění pozdějších předpisů).
Objednatel může provozní dobu upřesnit či omezit v rámci specifikace Služeb Poskytovatele v tomto dokumentu.

Zaručenou provozní dobou je míněna Provozní doba, v průběhu které je Objednatelem požadovaná a současně Poskytovatelem garantovaná plná nebo omezená dostupnost služby, a to včetně podpory ze strany Poskytovatele. Zaručená provozní doba je měřena/vyhodnocována v jednotkách času (v hodinách).
Parametr slouží společně s parametrem Vyhodnocovacího období (1 měsíc, případně jiné období) k určení a vyhodnocení dostupnosti služby.

Servisní okno je čas vymezený pro provádění servisních činností, údržby, profylaxe, zálohování a dalších činností, které neumožňují běžný provoz Vyhodnocovacího centra Bezpečnostního dohledu. V rámci Prostředí a Aplikace MS2014+ jsou rozlišena následující servisní okna:

- pro Provozovatele Aplikace MS2014+ v čase mimo provozní dobu (00:00 až 04:00);
- pro Poskytovatele služeb Prostředí:
  - v čase **00:00 až 04:00**, využití tohoto času je podmíněno souhlasem Provozovatele Aplikace MS2014+.
  - v čase **od soboty 18:00 do neděle 08:00 každý 1. víkend v měsíci**, využití tohoto času je podmíněno souhlasem Objednatele a uveřejněním oznámení na veřejné uživatelské části Aplikace MS2014+.
- Poskytovatel bude v rámci služeb Bezpečnostního dohledu využívat stejná servisní okna za stejných podmínek jako Poskytovatel služeb Prostředí

Plánovaná odstávka je doba, kdy budou Prostředí a Aplikace MS2014+ a tedy i vyhodnocovací centrum Bezpečnostního dohledu uvedeny do stavu mimo provoz. Plánovaná odstávka musí být projednána a schválena Objednatelem nejméně 1 kalendářní měsíc před odstavením Prostředí.

5.1.4 Definice dalších pojmů

Protokol o poskytnuté službě je sada výkazů, zpráv, návrhů a dalších dokumentů sestavovaných Poskytovatelem za vyhodnocovací období v ServiceDesku. Rozsah Protokolu a jeho náležitosti jsou vymezeny v rámci specifikace jednotlivých služeb v tomto dokumentu. Poskytovatel zodpovídá za to, že Protokol o poskytnuté službě bude zpracován v detailu umožňujícím kvalitativní a kvantitativní vyhodnocení každé Služby s důrazem na dodržení SLA.
Protokol o poskytnuté službě je předkládán Objednateli ke schválení a slouží jako podklad pro uplatnění sankcí a fakturaci Poskytovatele.

MD je jednotka kapacity, která definuje vynaloženou práci jednoho pracovníka za jeden pracovní den, který je tvořen 8 hodinami.

ServiceDesk je jednotný systém pro evidenci a řízení všech záznamů (Incidentů, Požadavků, Konfigurační databáze, Vad,…) souvisejících s provozem a rozvojem aplikace MS2014+ včetně Prostředí. ServiceDesk provozuje Provozovatel Aplikace MS2014+.

1. úroveň podpory = pracoviště ServiceDesk zabezpečuje příjem resp. vstupní zpracování všech incidentů, požadavků od autorizovaných interních uživatelů (tj. pracovníků Objednatele, řídících orgánů (resp. dalších subjektů tzv. Implementační struktury) a dodavatelů, jejich prvotní kontrolu, klasifikaci a předání řešitelům na základě stanovených eskalačních procedur.
Pozn.: první úroveň podpory pro externí uživatele (tj. např. žadatele, atp.) budou zajišťovat pracovníci řídících orgánů.

2. úroveň podpory = označuje první vrstvu řešitelů přijetého požadavku, incidentu. Typicky se jedná o pracovníky Provozovatele Aplikace MS2014+, Poskytovatele služeb Prostředí a Poskytovatele.

3. úroveň podpory = označuje druhou vrstvu řešitelů, kteří provádějí vysoce specializované činnosti, např. metodicko-technické analýzy složitých problémů. Jedná se zejména o výrobce/dodavatele SW a HW, případně jejich specializované servisní partnery. Řešitel 3. úrovně podpory je vždy specifikován smlouvou o podpoře, nebo v rámci zakoupené licence podpory a to včetně kontaktních informací a způsobů alokace.
Všechny záznamy procházející 1. až 3. úrovní podpory budou vedeny v systému ServiceDesk. Způsob řešení na 3. úrovni podpory je povinen do ServiceDesku zaznamenat řešitel 2. úrovně podpory, který 3. úroveň aktivoval.

Online centrální knihovna dokumentů MS2014+ = centrální knihovna dokumentů pro systém MS2014+ napojená na ServiceDesk MS2014+. Poskytovatel je povinen veškeré výstupy a jednotlivé verze těchto výstupů vytvořených v rámci Služeb definovaných v tomto dokumentu ukládat do Online centrální knihovny dokumentů MS2014+.

5.2 Vymezení SLA

Poskytovatel garantuje, že předmět plnění (Služby) bude v požadované provozní době vykazovat **spolehlivost a dostupnost lepší než je stanovená hodnota parametru „Minimální dostupnost**“ v rámci specifikace jednotlivých Služeb v tomto dokumentu.

Splnění SLA parametru „Dostupnost“ se počítá z provozní doby. Předmět plnění je považován za **nedostupný v případě výskytu vady/incidentu kategorie A**. Objednatel stanovuje, že **maximální počet** vad/incidentů kategorie A za vyhodnocovací období je stanoven hodnotou SLA parametru "**Maximální počet za období**" definovaném pro každou Službu v tomto dokumentu.

Přitom platí následující zásady:

- Poskytovatel má povinnost vhodným způsobem informovat Objednatele o míře ztrát dat a informací v důsledku nedostupnosti jeho Služeb.
- Pokud prokazatelně dojde k nenávratné ztrátě dat Prostředí nebo Aplikace MS2014+ v důsledku porušení smluvních povinností Poskytovatele, je Poskytovatel odpovědný za vznik a úhradu škody poškozeným subjektům. Pokud Objednatel uhradí takto vzniklou škodu poškozenému subjektu místo Poskytovatele, je Objednatel oprávněn uspokojit vzniklou pohledávku z regresního nároku vůči Poskytovateli započtením proti peněžitým pohledávkám

Poskytovatele vůči Objednateli; a to zejména proti peněžitým pohledávkám z titulu nároku na odměnu za poskytnutí Služeb dle Servisní smlouvy.

- Pokud prokazatelně dojde k nenávratné ztrátě dat v důsledku pochybení třetí strany, je tato strana odpovědná za případný vznik a úhradu škody Poskytovateli a všem ostatním dotčeným subjektům.
- Pokud dojde k nenávratné ztrátě dat v důsledku okolnosti, jež nastala aniž by Poskytovatel porušil své smluvní povinnosti nebo nezávisle na vůli třetích stran, je odpovědnost za škodu vyloučena.

Nedostupnost Služeb Poskytovatele (např. Vyhodnocovacího centra Bezpečnostního dohledu) způsobená Provozovatelem Aplikace MS2014+, Poskytovatelem služeb Prostředí, Objednatelem nebo třetími stranami na straně Objednatele (např. ve smluvním vztahu s Objednatelem) se **nezapočítává do výpočtu dostupnosti Služeb Poskytovatele**.

O předání řešení incidentu na třetí stranu musí být neprodleně informován rovněž Objednatel. V případě, kdy bude po předání řešení provozního incidentu Provozovateli Aplikace MS2014+, Poskytovateli služeb Prostředí nebo 3. úrovni podpory zpětně **prokázáno, že k incidentu došlo chybou na straně Poskytovatele**, je do doby pro vyřešení incidentu započítávaná celá doba od nahlášení incidentu (tj. včetně doby, kterou analýzou příčin provozního incidentu strávil Provozovatel Aplikace MS2014+, Poskytovatel služeb Prostředí nebo 3. úroveň podpory).

5.3 Hodnocení služeb

Hodnocení SLA na základě předaných Protokolů o poskytnuté službě (pro každou Službu samostatně) provádí Objednatel.

V případech, kdy Poskytovatel v rámci plnění definovaných SLA Služeb a/nebo v rámci provozních činností, jejichž předmět je smluvně vymezen specifikací příslušné Služby, nedosáhne stanovené (dohodnuté) úrovně plnění během Vyhodnocovacího období, vzniká tímto Objednateli nárok na **jednorázové snížení paušální ceny** za odebírání Služeb pro příští Vyhodnocovací období (tzv. kreditace). Za nedosažení stanovené (dohodnuté) úrovně plnění se nepočítá doba schváleného servisního okna nebo plánované odstávky. Výše jednorázové slevy bude stanovena dle příslušného SLA parametru, který byl porušen a dle úrovně porušení (specifikované jednotlivě pro každý SLA parametr).

V případě, že v důsledku výpadku jedné Služby dojde k výpadku i dalších Služeb, platí, že kreditace se uplatní pouze pro tu Službu, která způsobila výpadek i ostatních Služeb.

V případě, že dojde k nedodržení více dílčích SLA parametrů v rámci jedné Služby, platí, že kreditace se uplatní ke všem nedodrženým dílčím SLA parametrům.

5.3.1 Dostupnost služby

Podkladem vyhodnocení **dostupnosti Služby** je zejména Protokol o poskytnuté službě odpovídající Vyhodnocovacímu období, z něhož jsou relevantní všechny Poskytovatelem vyřešené a Objednatelem uzavřené incidenty kategorie A a údaje ze ServiceDesku Provozovatele Aplikace MS2014+. U incidentů kategorie A se určí pouze časová období spadající do zaručené provozní doby,

a to dle příslušného známého času zjištění daného incidentu a známého času jeho vyřešení. Takto určená časová období (období nedostupnosti služby) se sečtou a celkový součet vyjádřený v procentech se vyhodnotí (porovná) proti hodnotě smluvně sjednaného SLA parametru "**Minimální dostupnost**".
Kreditace se uplatní v daném Vyhodnocovacím období, ve kterém došlo k porušení (nedodržení) SLA parametru "Dostupnost".

5.4 Maximální doba výpadku

Maximální dobou výpadku je míněno maximální časové období, po které je v rámci zaručené provozní doby přípustná jednorázová nedostupnost služby. Maximální doba výpadku je vyhodnocována v jednotkách času (v hodinách).

Podkladem vyhodnocení maximální doby výpadku Služby je zejména Protokol o poskytnuté službě odpovídající Vyhodnocovacímu období, z něhož jsou relevantní všechny Poskytovatelem vyřešené a Objednatelem uzavřené incidenty kategorie A a údaje ze ServiceDesku Provozovatele Aplikace MS2014+. U incidentů kategorie A se určí doba výpadku jako absolutní hodnota rozdílu mezi časem vzniku nedostupnosti a časem, kdy byla služba po vyřešení/odstranění incidentu obnovena v plném rozsahu a je dále dostupná v plném rozsahu.

Maximální doba výpadku se vyhodnotí (porovná) proti hodnotě smluvně sjednaného SLA parametru "**Lhůty při řešení požadavku/incidentu**", a to individuálně pro každý incident a výpadek zvlášť.

V případech, u kterých bude prokázáno, že byl výpadek jedné Služby způsoben nedostupností jiné Služby Poskytovatele nebo jich dat, bude od času doby výpadku Služby odečten čas řešení nedostupnosti této jiné služby nebo jejich dat.

5.5 Maximální doba servisní odezvy

Dobou servisní odezvy se rozumí doba, do které je Poskytovatel povinen zareagovat na nový záznam v ServiceDesku, který byl založen v rámci zaručené provozní doby. Maximální doba servisní odezvy je vyhodnocována v jednotkách času (v minutách).

Podkladem vyhodnocení **maximální doby servisní odezvy** je zejména Protokol o poskytnuté službě odpovídající Vyhodnocovacímu období, z něhož jsou relevantní všechny Poskytovatelem vyřešené a Objednatelem uzavřené incidenty kategorie A, B, C a údaje ze ServiceDesku Provozovatele Aplikace MS2014+. U incidentů kategorie A, B, C se určí doba servisní odezvy jako absolutní hodnota rozdílu mezi časem vzniku nového záznamu v ServiceDesku a časem první reakce Poskytovatele.

Maximální doba servisní odezvy se vyhodnotí (porovná) proti hodnotě smluvně sjednaného SLA parametru "**Lhůty při vyřizování požadavku/incidentu**", a to individuálně pro každý incident a výpadek zvlášť. Kreditace se uplatní jednotlivě za každý incident, u kterého došlo k porušení (překročení) SLA parametru "Lhůty při vyřizování požadavku/incidentu".

Případy, kdy je záznam vložen do ServiceDesku v čase spadajícím do zaručené provozní doby a zároveň čas reakce (odvozen jako čas vložení záznamu plus maximální doba servisní odezvy) již spadá do časového období mimo zaručenou provozní dobu, jsou posuzovány z hlediska výpočtu servisní odezvy shodně jako případy, kdy oba časy (založení záznamu do helpdeskového systému a čas servisní odezvy) spadají do zaručené provozní doby.

V případech, kdy je záznam vložen mimo časové období zaručené provozní doby, je za čas založení záznamu považován čas zahájení nejbližší příští zaručené provozní doby.

5.6 Odstranění incidentu – A, B a C

Jednotlivé kategorie incidentů jsou uvedeny v tomto dokumentu. Odstranění incidentu je měřeno/vyhodnocováno v jednotkách času (v hodinách pro kategorie A a B a ve dnech pro kategorii C).

Podkladem vyhodnocení odstranění incidentu A, B a C je zejména Protokol o poskytnuté službě odpovídající Vyhodnocovacímu období, z něhož jsou relevantní všechny Poskytovatelem vyřešené a Objednatelem uzavřené incidenty kategorie A, B, C a údaje ze ServiceDesku Provozovatele Aplikace MS2014+ s tím, že:

a) pro každý incident se určí čas odstranění jako absolutní hodnota rozdílu mezi časem vzniku příslušného záznamu v ServiceDesku a časem, kdy byla služba po vyřešení/odstranění incidentu obnovena v plném rozsahu a je dále dostupná v plném rozsahu;
b) pro každou kategorii incidentů A, B a C se určí počet příslušných incidentů.

Ad a) Maximální doba odstranění výpadku se vyhodnotí (porovná) proti příslušné hodnotě smluvně sjednaného SLA parametru "**Lhůta při řešení požadavku/incidentu – Kategorie A**" (resp. "**Lhůta při řešení požadavku/incidentu – Kategorie B**", "**Lhůta při řešení požadavku/incidentu - Kategorie C**"), a to dle kategorie daného incidentu a individuálně pro každý incident či výpadek. Kreditace se uplatní jednotlivě za každý incident, u kterého došlo k porušení (překročení) SLA parametru.
V případech, kdy je záznam vložen mimo časové období zaručené provozní doby, je za čas založení záznamu považován čas zahájení nejbližší příští zaručené provozní doby.

Ad b) Maximální počet incidentů se vyhodnotí (porovná) proti příslušné hodnotě smluvně sjednaného SLA parametru "**Maximální počet za období**", a to individuálně pro každou kategorii incidentů. Kreditace se uplatní jednotlivě za každou kategorii incidentu, u které došlo k porušení (překročení) SLA parametru "Maximální počet za období".
Překročení SLA parametru "Maximální počet za období" u incidentu kategorie A znamená, že každá další vada/incident kategorie A, bez ohledu na lhůty vyřizování nebo řešení, považována **nedostupnost systému** po celou dobu do úplného vyřešení tohoto incidentu.

5.7 Další požadované činnosti mimo sledované parametry SLA

Jedná se zejména o provozní činnosti specifikované rozsahem požadovaných činností v rámci příslušné Služby. Jednotlivá jednorázová porušení povinnosti Poskytovatele poskytovat tyto činnosti budou posuzována jako jednotlivá porušení SLA parametru s nárokem na jednorázovou paušální kreditaci s tím, že je povinností Poskytovatele zjištěnou závadu do doby stanovené Objednatelem odstranit. Při nesplnění této doby je Objednatel oprávněn opakovaně uplatnit kreditaci.

5.8 Statistika (exporty) ServiceDesku

Z hlediska exportu/reportu generovaného ze ServiceDesku za Vyhodnocovací období pro posouzení jednotlivých SLA parametrů platí, že:

- relevantní jsou pouze záznamy Poskytovatelem vyřešené a Objednatelem uzavřené, které byly přiřazeny Poskytovateli s tím, že byla prokázána příčinná souvislost mezi porušením smluvních povinností Poskytovatele a vznikem incidentu, resp. nebyla prokázána příčina vzniku incidentu u jiné Služby. V případě, že by vyhodnocení a následné uzavření incidentu přesáhlo do dalšího Vyhodnocovacího období, je Poskytovatel povinen zpětně přepočítat SLA po uzavření všech incidentů a stanovit výši neuplatněné kreditace, ke které došlo na základě doby trvání uzavření incidentu. Neuplatněná kreditace bude Poskytovatelem započtena do fakturace za Vyhodnocovací období, v rámci kterého byl incident uzavřen. Případným průtahem a prodloužením vyřešení a uzavření incidentu tak není dotčen nárok Objednatele uplatnit kreditaci a další smluvní sankce i zpětně.
- záznamy odmítnuté Poskytovatelem s tím, že jejich příčina nebyla prokázána provozu příslušné Služby (např. nefunkčnost jiného/podřízeného systému nebo chyba integrity dat způsobená uživatelem systému) nejsou do statistik zahrnuty. Takovéto záznamy musí být v ServiceDesku Poskytovatelem doplněny řádným odůvodněním a Objednatelem na základě doplněného odůvodnění Poskytovatele uzavřeny jako neplatné.

Níže uvedená tabulka zobrazuje výčet parametrů SLA s příslušnými kreditacemi a způsobem výpočtu.

5.9 Parametry snížení paušální ceny - kreditace

	Název parametru	Kredity*)	Způsob výpočtu
1.	**Dostupnost služby**	3,0%	Za každých započatých 0,1% pod stanovenou hodnotu parametru
2.	**Max. doba výpadku**	3,0%	Za každou započatou 1 hodinu nad stanovenou hodnotu parametru
3.	**Max. doba servisní odezvy**	1,0%	Za každých započatých 15 minut nad stanovenou hodnotu parametru
4.	**Doba odstranění závady kategorie A**	2,0%	Za každých započatých 15 minut nad stanovenou hodnotu parametru
5.	**Maximální počet za období (kat. A)**	3,0%	Za každý 1 incident nad stanovenou hodnotu parametru
6.	**Doba odstranění závady kategorie B**	2,0%	Za každou 1 provozní hodinu služby nad stanovenou hodnotu parametru
7.	**Maximální počet za období (kat. B)**	2,0%	Za každý 1 incident nad stanovenou hodnotu parametru
8.	**Doba odstranění závady kategorie C**	0,5%	Za každých 8 provozních hodin služby nad stanovenou hodnotu parametru
9.	**Maximální počet za období (kat. C)**	0,5%	Za každé 2 incidenty nad stanovenou hodnotu parametru
10.	**Neplnění provozní činnosti specifikované v části "Popis a parametry činností" v rámci příslušné služby (neměřitelné parametry SLA)**	10.000,- Kč	Jednotlivá jednorázová porušení povinnosti Poskytovatele poskytovat tyto činnosti budou posuzována jako jednotlivá porušení SLA parametru s nárokem na jednorázovou paušální kreditaci s tím, že je povinností Poskytovatele zjištěnou závadu do doby stanovené Objednatelem odstranit. Při nesplnění této doby je Objednatel oprávněn opakovaně uplatnit kreditaci.

*U procentuálních hodnot je míněno dané procento z ceny stanovené za provoz Služby ve Vyhodnocovacím období.

Číslo v CES: 5390

Příloha č. 2 Smlouvy o poskytování služeb

Seznam subdodavatelů

1 Identifikace subdodavatelů

Subdodavateli Poskytovatele v rámci zajištění Služeb budou:

2 Rozsah činnosti subdodavatelů

Číslo v CES: 5390

Příloha č. 3 Smlouvy o poskytování služeb

Zadávací dokumentace

k veřejné zakázce

„Zajištění služby Bezpečnostního dohledu pro MS2014+“

Název veřejného Zadavatele:	Česká republika - Ministerstvo pro místní rozvoj
Sídlo:	Staroměstské nám. 6, 110 15 Praha 1
Zastoupena:	RNDr. Blankou Fischerovou, ředitelkou Odboru správy monitorovacího systému
IČ:	660 02 222

V Praze dne 24. 10. 2014

OBSAH

1. PREAMBULE 3
2. ZÁKLADNÍ ÚDAJE O VEŘEJNÉ ZAKÁZCE 4
3. ZKRATKY A POJMY 6
4. PŘEDMĚT PLNĚNÍ ZAKÁZKY 8
5. DOBA A MÍSTO PLNĚNÍ ZAKÁZKY 9
6. KVALIFIKAČNÍ PŘEDPOKLADY 9
7. POVINNÁ SOUČÁST NABÍDKY (DLE § 68 ODST. 3 ZVZ) 17
8. POŽADAVKY NA ZPŮSOB ZPRACOVÁNÍ NABÍDKY 18
9. LHŮTY A ZPŮSOB PODÁNÍ NABÍDEK 22
10. POŽADAVEK NA ZPŮSOB ZPRACOVÁNÍ NABÍDKOVÉ CENY 22
11. HODNOCENÍ NABÍDEK 24
12. OBCHODNÍ A PLATEBNÍ PODMÍNKY 27
13. OSTATNÍ 28
14. STRUKTUROVANÝ SEZNAM DOKUMENTŮ TVOŘÍCÍCH ZADÁVACÍ PODMÍNKY ..29

1. PREAMBULE

Tato zadávací dokumentace k veřejné zakázce (dále též „***Zadávací dokumentace***“) je souhrn údajů, požadavků a technických podmínek Zadavatele vymezujících předmět veřejné zakázky v podrobnostech nezbytných pro vypracování a podání nabídky (dále též „***Nabídka***“) v otevřeném řízení podle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále též „***ZVZ***“) a ve smyslu § 27 ZVZ, na nadlimitní veřejnou zakázku na služby. Práva a povinnosti Zadavatele a uchazečů resp. dodavatelů (dále pro účely této Zadávací dokumentace „***Uchazeč***“) v rámci zadávacího řízení, která nejsou výslovně uvedena v této Zadávací dokumentaci, se řídí příslušnými ustanoveními zákona.

2. ZÁKLADNÍ ÚDAJE O VEŘEJNÉ ZAKÁZCE

Zadavatel:	Česká republika - Ministerstvo pro místní rozvoj Staroměstské nám. 6 110 15 Praha 1 IČ: 66002222 Zastoupen: RNDr. Blankou Fischerovou ředitelkou Odboru správy monitorovacího systému Kontaktní osoba: Ing. Mgr. Radek Vršecký, Ph.D., Odbor práva veřejných zakázek a koncesí email [redacted] č. účtu pro složení jistoty: 6015-629001/0710, v případě složení na účet zadavatele uchazeč uvede jako variabilní symbol své IČ, popř. své rodné číslo, jde-li o fyzickou osobu, a specifický symbol 368381324. Web zadavatele: www.mmr.cz Profil zadavatele: ezak.mmr.cz (dále jen „***Zadavatel***“ nebo „***MMR***“).
Druh veřejné zakázky:	Nadlimitní veřejná zakázka na služby (dále jen „***Veřejná zakázka***“) zadávaná v otevřeném řízení
CPV kód:	Hlavní předmět: CPV kód: 72223000-4 Hodnocení požadavků informačních technologií Další předměty: CPV kód: 72266000-7 Poradenství v oblasti programového vybavení CPV kód: 72150000-1 Poradenské služby v oblasti počítačových auditů a technického vybavení počítačů CPV kód: 72810000-1 Audity počítačů
Název Veřejné zakázky:	**"Zajištění služby Bezpečnostního dohledu pro MS2014+"**

Předpokládaná hodnota Veřejné zakázky:	**45 000 000 Kč bez DPH** (slovy: čtyřicet pět milionů korun českých).
Nejvyšší přípustná nabídková cena:	Předpokládaná hodnota je zároveň stanovena jako nejvyšší přípustná a maximální nabídková cena (bez DPH). Pokud bude celková nabídková cena vyšší, jedná se o nepřijatelnou nabídku a v souladu s ustanovením § 76 ZVZ bude nabídka vyřazena.
Lhůta pro podání nabídek:	Dle uveřejněného formuláře Oznámení o zakázce
Projekt OPTP:	**název projektu:** "Zajištění služby Bezpečnostního dohledu pro MS2014+" **reg. číslo projektu:** CZ.1.08/2.1.00/13.00167

3. ZKRATKY A POJMY

MS2014+	Monitorovací systém Evropských strukturálních a investičních fondů (dále jen „ESI fondy“) na programové období 2014 - 2020 sestávající se z „Aplikace MS2014+“, „HW platformy a Infrastruktury serverovny pro Aplikaci MS2014+“ a „Bezpečnostního dohledu pro MS2014+“
Aplikace MS2014+	Souhrn programového vybavení, který společně tvoří logický celek Aplikaci MS2014+. Aplikace MS2014+ je dodávána, spravována a provozována Provozovatelem Aplikace MS2014+ na základě jiného smluvního vztahu.
Prostředí	Představuje souhrn Infrastruktury serverovny, HW platformy a veškerého dalšího SW vybavení mimo Aplikace MS2014+ pro potřeby provozování Aplikace MS2014+. Případné výjimky budou Zadavatelem protokolárně schváleny.
HW platforma	Jedná se o veškeré HW vybavení provozované v primární a zálohovací / záložní lokalitě pro potřeby provozování Aplikace MS2014+. Součástí HW platformy jsou i vybrané prvky ze zálohovacího a testovacího / školícího prostředí.
Infrastruktura serverovny	Zajištění příslušných služeb datového centra včetně síťové infrastruktury, konektivity datového centra, housingu HW platformy, řízení a správy provozního prostředí, podpory HW a SW prvků třetích stran a dalších služeb pro Aplikaci MS2014+.
Provozovatel Aplikace MS2014+	Subjekt odpovědný za správu, provoz, rozvoj a údržbu Aplikace MS2014+ v rozsahu stanoveném na základě jiného smluvního vztahu (viz https://ezak.mmr.cz/contract_display_668.html)
Poskytovatel služeb Prostředí	Subjekt odpovědný za zajištění služeb provozu, správy, údržby a podpory Prostředí v rozsahu stanoveném na základě jiného smluvního vztahu (viz https://ezak.mmr.cz/contract_display_823.html)
Technický dozor	Subjekt zajišťující služby technického dozoru nad realizací celého projektu MS2014+ na základě jiného smluvního vztahu (viz https://ezak.mmr.cz/contract_display_730.html)
Bezpečnostní dohled	Subjekt zajišťující služby bezpečnostního dohledu pro MS2014+ na základě této zadávací dokumentace (dále také „***Poskytovatel***“)
Projekt	CZ.1.08/2.1.00/13.00167 - Zajištění služby Bezpečnostního dohledu pro MS2014+

EU	Evropská unie
VZ	Veřejná zakázka
ZVZ	Zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů

4. PŘEDMĚT PLNĚNÍ ZAKÁZKY

4.1. ÚČEL VEŘEJNÉ ZAKÁZKY

Veřejná zakázka je součástí celkového komplexního řešení MS2014+, který zahrnuje tři zadávací řízení (dále ZŘ) následujících technologických celků (přičemž předmětem této zakázky je pouze Zajištění služby Bezpečnostního dohledu pro MS2014+):

1. Pořízení aplikace MS2014+ (včetně provozu a rozvoje),
2. Pořízení HW platformy a Infrastruktury serverovny pro MS2014+,
3. Zajištění služby Bezpečnostního dohledu pro MS2014+.

Proto při plnění této Veřejné zakázky bude Uchazeč spolupracovat kromě Zadavatele i se třetími stranami pověřenými Zadavatelem, zejména s Provozovatelem Aplikace MS2014+, Technickým dozorem a Poskytovatelem služeb Prostředí.

Tato veřejná zakázka představuje poskytování komplexních služeb pro kontrolu zabezpečení provozního prostředí, aplikace a procesního zajištění komplexního řešení MS2014+. Rozsah požadovaných služeb vychází nejen z požadavků EK na standardy bezpečnosti pro systémy monitorující Evropské strukturální a investiční fondy, ale i ze standardů bezpečnosti uplatňovaných pro IT systémy v rámci e-Governmentu České republiky. Definování základních parametrů služeb bude korespondovat s rozsahem požadavků, které na takovéto systémy kladou zejména České národní normy a příslušné normy EK. V přímé souvislosti s výše uvedenými zadávacími řízeními Zadavatel zároveň realizoval zadávací řízení "HW a SW vybavení pro záložní pracoviště Aplikace MS2014+", v rámci kterého je v současnosti budována plnohodnotná záložní lokalita formou rozšíření a povýšení stávající lokality zálohovací.

4.2. SPECIFIKACE PŘEDMĚTU

Předmětem této veřejné zakázky je pořízení nezbytně nutných služeb pro zajištění správného nastavení a dohledu nad provozní bezpečností systému MS2014+ (monitoring bezpečnosti, kontrola procesů, přístupů a postupů, schvalování změnových řízení aplikace, HW a SW prostředí a způsobu jejich řešení z pohledu bezpečnostních norem, kontrola vstupů pro výkon auditů a vlastní provádění pravidelných bezpečnostních auditů, návrhy opravných řešení a tvorba, revize a vedení bezpečnostní dokumentace systému jako celku).

Předmětem této Veřejné zakázky jsou následující služby:

- Informační bezpečnost
- Ochrana osobních údajů
- Bezpečnostní monitoring
- Kontrola kvality poskytovaných služeb
- Audit prostředí

Podrobnější vymezení předmětu Veřejné zakázky pro jednotlivé služby služeb je uvedeno v Příloze č. 1 "Katalog služeb a podmínky poskytování bezpečnostního dohledu" **Smlouvy na zajištění služby Bezpečnostního dohledu pro MS2014+** (dále též „***Smlouva o poskytování služeb***“).

4.3. DRUH VEŘEJNÉ ZAKÁZKY

Tato Veřejná zakázka je Veřejnou zakázkou na služby dle § 10 ZVZ.

4.4. VÝKLADOVÉ USTANOVENÍ

Pokud tyto Zadávací podmínky obsahují v definici předmětu plnění požadavky nebo odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, které platí pro určitou osobu, popřípadě její organizační složku za příznačné, patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, je uchazeč oprávněn nabídnout i jiné kvalitativně a technicky obdobné řešení.

Jiné kvalitativně a technicky obdobné řešení však musí být plně kompatibilní s ostatními částmi Aplikace MS2014+.

Zadavatel pro vyloučení pochybností uvádí, že toto výkladové ustanovení se nevztahuje na mezinárodní normy a standardy, stanovené jako předmět plnění v Příloze č. 1 Smlouvy.

5. DOBA A MÍSTO PLNĚNÍ ZAKÁZKY

5.1. MÍSTO PLNĚNÍ VEŘEJNÉ ZAKÁZKY

Místem plnění Veřejné zakázky bude sídlo Zadavatele, záložní lokalita - datové centrum Zadavatele na adrese Staroměstské nám. 6 (adresa shodná s adresou sídla Zadavatele) a primární lokalita - datové centrum zajišťované Poskytovatelem služeb Prostředí na adrese Jeremenkova 40b, Olomouc.

5.2. DOBA PLNĚNÍ VEŘEJNÉ ZAKÁZKY

Termín zahájení poskytování služeb bude určen Zadavatelem na základě výzvy Zadavatele a k datu, které Zadavatel jednostranně určí, ne však dříve než 7 dní ode dne odeslání výzvy Zadavatelem.

Zadavatel předpokládá podpis smlouvy na veřejnou zakázku bez zbytečného odkladu poté, kdy tak bude moci dle ZVZ učinit. Zadavatel odešle výzvu dle předchozího odstavce bez zbytečného odkladu po uzavření smlouvy na veřejnou zakázku.

Služby budou poskytovány po dobu platnosti a účinnosti smlouvy o poskytování služeb, která se uzavírá na dobu neurčitou a která zároveň upravuje způsob jejího ukončení.

6. KVALIFIKAČNÍ PŘEDPOKLADY

Zadavatel tímto stanovuje požadavky na prokázání základních kvalifikačních předpokladů podle § 53 ZVZ, profesních kvalifikačních předpokladů podle § 54 ZVZ a technických kvalifikačních předpokladů podle § 56 ZVZ.

a) Splnění kvalifikace prokáže Uchazeč, který s poukazem na § 50 odst. 1 ZVZ splní kvalifikační předpoklady uvedené dále. Prokázání splnění kvalifikace podle požadavků Zadavatele je v souladu s § 51 odst. 2 ZVZ předpokladem posouzení a hodnocení Nabídky Uchazeče.

b) Postačí, pokud Uchazeč předloží prosté kopie dokladů prokazujících splnění kvalifikace.

c) Pokud není Uchazeč schopen prokázat splnění určité části kvalifikace požadované Zadavatelem podle § 50 odst. 1 písm. b) a d) ZVZ, v plném rozsahu, je oprávněn splnění kvalifikace v chybějícím rozsahu prokázat prostřednictvím subdodavatele. Uchazeč je v takovém případě povinen veřejnému Zadavateli předložit:
   - doklady prokazující splnění základního kvalifikačního předpokladu podle § 53 odst. 1 písm. j) a profesního kvalifikačního předpokladu podle § 54 písm. a) subdodavatelem a
   - smlouvu uzavřenou se subdodavatelem, z níž vyplývá závazek subdodavatele k poskytnutí plnění určeného k plnění Veřejné zakázky Uchazečem či k poskytnutí věcí či práv, s nimiž bude Uchazeč oprávněn disponovat v rámci plnění Veřejné zakázky, a to alespoň v rozsahu, v jakém subdodavatel prokázal splnění kvalifikace podle § 50 odst. 1 písm. b) a d).

d) Uchazeč není oprávněn prostřednictvím subdodavatele prokázat splnění kvalifikace podle § 54 písm. a) ZVZ.

e) Má-li být předmět Veřejné zakázky plněn několika Uchazeči společně a za tímto účelem podávají či hodlají podat společnou Nabídku, je každý z Uchazečů povinen se řídit ustanovením § 51 odst. 5 a 6 ZVZ.

f) Nevyplývá-li ze zvláštního právního předpisu jinak, prokazuje zahraniční Uchazeč splnění kvalifikace způsobem podle právního řádu platného v zemi jeho sídla, místa podnikání nebo bydliště, a to v rozsahu požadovaném tímto zákonem a veřejným zadavatelem. Pokud se podle právního řádu platného v zemi sídla, místa podnikání nebo bydliště zahraničního Uchazeče určitý doklad nevydává, je zahraniční Uchazeč povinen prokázat splnění takové části kvalifikace čestným prohlášením. Není-li povinnost, jejíž splnění má být v rámci kvalifikace prokázáno, v zemi sídla, místa podnikání nebo bydliště zahraničního Uchazeče stanovena, učiní o této skutečnosti čestné prohlášení. Doklady prokazující splnění kvalifikace předkládá zahraniční Uchazeč v původním jazyce s připojením jejich úředně ověřeného překladu do českého jazyka, pokud Zadavatel v zadávacích podmínkách nebo mezinárodní smlouva, kterou je Česká republika vázána, nestanoví jinak; to platí i v případě, prokazuje-li splnění kvalifikace doklady v jiném než českém jazyce Uchazeč se sídlem, místem podnikání nebo místem trvalého pobytu na území České republiky. Povinnost připojit k dokladům úředně ověřený překlad do českého jazyka se nevztahuje na doklady ve slovenském jazyce, na vysokoškolské diplomy v latinském jazyce a na certifikáty v anglickém jazyce.

g) Je-li Uchazeč zapsán v seznamu kvalifikovaných dodavatelů podle § 125 ZVZ (dále jen „***Seznam kvalifikovaných dodavatelů***“), může prokázat splnění kvalifikace podle § 127 odst. 1 písm. a), b) ZVZ výpisem ze Seznamu kvalifikovaných dodavatelů ne starším než tři měsíce.

h) Je-li Uchazeč zapsán v Systému certifikovaných dodavatelů podle § 133 ZVZ, může prokázat splnění kvalifikace podle § 134 odst. 1 ZVZ certifikátem ne starším než 1 rok.

i) Doklady prokazující splnění základních kvalifikačních předpokladů a výpis z obchodního rejstříku nesmějí být ke dni podání nabídky starší 90 kalendářních dnů.

6.1. ZÁKLADNÍ KVALIFIKAČNÍ PŘEDPOKLADY

Základní kvalifikační předpoklad splní Uchazeč,

a) který nebyl pravomocně odsouzen pro trestný čin spáchaný ve prospěch organizované zločinecké skupiny, trestný čin účasti na organizované zločinecké skupině, legalizace výnosů z trestné činnosti, podílnictví, přijetí úplatku, podplacení, nepřímého úplatkářství, podvodu,

úvěrového podvodu, včetně případů, kdy jde o přípravu nebo pokus nebo účastenství na takovém trestném činu, nebo došlo k zahlazení odsouzení za spáchání takového trestného činu; jde-li o právnickou osobu, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu, a je-li statutárním orgánem Uchazeč či členem statutárního orgánu Uchazeče právnická osoba, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu této právnické osoby; podává-li Nabídku či žádost o účast zahraniční právnická osoba prostřednictvím své organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí Uchazeč splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání či bydliště;

b) který nebyl pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání Uchazeče podle zvláštních právních předpisů nebo došlo k zahlazení odsouzení za spáchání takového trestného činu; jde-li o právnickou osobu, musí tuto podmínku splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu, a je-li statutárním orgánem Uchazeče či členem statutárního orgánu Uchazeče právnická osoba, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu této právnické osoby; podává-li Nabídku či žádost o účast zahraniční právnická osoba prostřednictvím své organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí Uchazeč splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání či bydliště;

c) který v posledních 3 letech nenaplnil skutkovou podstatu jednání nekalé soutěže formou podplácení podle zvláštního právního předpisu;

d) vůči jehož majetku neprobíhá nebo v posledních 3 letech neproběhlo insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh nebyl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo nebyl konkurs zrušen proto, že majetek byl zcela nepostačující nebo zavedena nucená správa podle zvláštních právních předpisů;

e) který není v likvidaci;

f) který nemá v evidenci daní zachyceny daňové nedoplatky, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště Uchazeče;

g) který nemá nedoplatek na pojistném a na penále na veřejné zdravotní pojištění, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště Uchazeče;

h) který nemá nedoplatek na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště Uchazeče;

i) který není veden v rejstříku osob se zákazem plnění veřejných zakázek; a

j) kterému nebyla v posledních 3 letech pravomocně uložena pokuta za umožnění výkonu nelegální práce podle zvláštního právního předpisu.

6.1.1. PROKÁZÁNÍ SPLNĚNÍ ZÁKLADNÍCH KVALIFIKAČNÍCH PŘEDPOKLADŮ

Uchazeč prokazuje splnění základních kvalifikačních předpokladů podle předchozího odstavce předložením:

a) **výpisu z evidence Rejstříku trestů** [odstavec 6.1 písm. a) a b)];

b) **potvrzení příslušného finančního úřadu a ve vztahu ke spotřební dani čestného prohlášení** [odstavec 6.1 písm. f)];

c) **potvrzení příslušného orgánu či instituce** [odstavec 6.1 písm. h)]; a

d) **čestného prohlášení** [odstavec 6.1 písm. c) až e) a g), i) až j) shora]; Zadavatel doporučuje využít vzorové čestné prohlášení, které je uvedeno v Příloze č. 2 této Zadávací dokumentace.

6.2. PROFESNÍ KVALIFIKAČNÍ PŘEDPOKLADY

Splnění profesních kvalifikačních předpokladů prokáže Uchazeč, který předloží:

a) **výpis z obchodního rejstříku**, pokud je v něm zapsán, či výpis z jiné obdobné evidence, pokud je v ní zapsán dle § 54 písm. a) ZVZ;

b) **doklad o oprávnění k podnikání podle zvláštních právních předpisů** v rozsahu odpovídajícím předmětu Veřejné zakázky, zejména doklad prokazující příslušné živnostenské oprávnění či licenci.

6.3. ČESTNÉ PROHLÁŠENÍ O EKONOMICKÉ A FINANČNÍ ZPŮSOBILOSTI SPLNIT VEŘEJNOU ZAKÁZKU

Zadavatel požaduje předložení čestného prohlášení o ekonomické a finanční způsobilosti Uchazeče splnit tuto Veřejnou zakázku.

6.4. TECHNICKÉ KVALIFIKAČNÍ PŘEDPOKLADY

6.4.1. SPLNĚNÍ TECHNICKÝCH KVALIFIKAČNÍCH PŘEDPOKLADŮ

Ke splnění technických kvalifikačních předpokladů požaduje Zadavatel předložení:

a) **Seznamu významných služeb** poskytnutých Uchazečem v posledních 3 letech s uvedením jejich rozsahu a doby poskytnutí (§ 56 odst. 2 písm. a) ZVZ); seznam významných služeb musí být formou čestného prohlášení v následující struktuře, nejlépe ve formě tabulky a s následujícími údaji:

- název objednatele služby,
- odkaz na kvalifikační předpoklad (ustanovení zadávací dokumentace), který významná služba dokládá,
- popis poskytovaných služeb,
- celkový rozsah plnění ve finančním vyjádření v Kč bez DPH (u plnění zasahujících do budoucnosti uvede dodavatel rozsah plnění ve finančním vyjádření v Kč vztahujícím se ke dni podání nabídky, budoucí plnění nebudou uznána), přičemž cena za významnou službu musí být jednoznačně přiřazena k požadované službě, pokud zakázka zahrnovala více služeb v jedné zakázce,
- doba realizace služeb,
- označení, zda objednatelem byl veřejný zadavatel nebo jiná osoba a údaj o tom, zda je přiloženo osvědčení objednatele.

Přílohou tohoto seznamu musí být:

i. osvědčení vydané veřejným zadavatelem, pokud byly služby poskytovány veřejnému zadavateli, nebo

ii. osvědčení vydané jinou osobou, pokud byly služby poskytovány jiné osobě než veřejnému zadavateli, nebo

iii. kopie smlouvy s jinou osobou a doklad o uskutečnění plnění Uchazeče, není-li současně možné osvědčení od této osoby získat z důvodů spočívajících na její straně.

Pro prokázání splnění tohoto kvalifikačního předpokladu Zadavatel určuje minimální úroveň takto:

Uchazeč předloží seznam nejméně 4 významných služeb poskytnutých Uchazečem v posledních 3 letech, a to dle vymezení uvedeného dále v bodech I. až IV.

I. Uchazeč předloží alespoň **jednu významnou službu řízení informační bezpečnosti**.

Za významnou službu se považuje služba **řízení informační bezpečnosti**, jejíž rozsah plnění činil minimálně **1.000.000,- Kč bez DPH** a předmět plnění spočíval v poskytnutí **služby implementace systému řízení informační bezpečnosti dle norem řady ISO 27000**, přičemž předmět plnění spočíval v poskytnutí **služeb zahrnujících analýzu rizik, hodnocení aktiv, výběr a implementaci opatření a návrh a vytvoření celé dokumentační základny systému řízení.**

Významná služba bude splňovat minimální úroveň dle následujících parametrů:

a. V rámci služby došlo k úspěšnému zavedení systému řízení informační bezpečnosti (ISMS). Za úspěšné zavedení je považováno provedení certifikace a získání certifikátu od akreditovaného certifikačního orgánu nebo schválení ISMS ze strany vlastníka provozovaného systému a jeho prosazení do běžného provozu daného informačního systému.

   Kopii certifikátu nebo písemného schválení vlastníka je uchazeč povinen doložit v rámci příloh Seznamu významných služeb.

b. Významná služba byla realizována u zákazníka, který provozuje informační systém, který:

   - zajišťoval komunikaci s externími informačními systémy na úrovni přenosů a validací strukturovaných dat,
   - využívá alespoň 3000 koncových uživatelů, nebo alespoň 20 uživatelských rolí.

II. Uchazeč předloží alespoň **jednu významnou službu řízení kontinuity činností**.

Za významnou službu se považuje služba **řízení kontinuity činností**, jejíž rozsah plnění činil minimálně **300.000,- Kč bez DPH** a předmět plnění spočíval v poskytnutí **služby dle mezinárodně uznávaného standardu v oblasti návrhu systému řízení kontinuity činností (např. ČSN ISO 22301, nebo BS25599) nebo kontinuity služeb (např. dle ISO 20000)**, přičemž služba byla poskytnuta pro informační systém a jeho provoz.

Významná služba bude splňovat minimální úroveň alespoň jednoho z následujících parametrů:

a. Součástí služby byl návrh detailních havarijních plánů, přičemž bude doloženo, že uchazečem navržené havarijní plány prošly úspěšnou implementací a testováním,

b. Součástí služby byla úspěšná implementace a testování havarijních plánů.

III. Uchazeč předloží alespoň **jednu významnou službu bezpečnostního monitoringu ICT**.

Za významnou službu se považuje služba **bezpečnostního monitoringu ICT**, jejíž rozsah plnění činil minimálně **7.000.000,- Kč bez DPH** a předmět plnění spočíval v poskytnutí **služeb bezpečnostního monitoringu, detekci slabých míst a optimalizace technických a konfiguračních parametrů monitorovaného prostředí**, přičemž služba byla poskytována kontinuálně po dobu nejméně 1 kalendářního roku.

Významná služba bude splňovat minimální úroveň dle následujících parametrů:

a. Při poskytování služby bezpečnostního monitoringu bylo součástí vybudování centrálního místa pro dohled a monitoring bezpečnostně relevantních událostí s důrazem na:
   - využití specializovaných SW/HW prostředků pro sběr auditních záznamů (např. agenti, sondy a další),
   - implementace centrálního sledovacího a vyhodnocovacího místa na bázi SW/HW produktu schopného provádět analýzy, korelace a další operace nad získanými záznamy,
   - systém poskytoval aktivní a proaktivní monitoring a řídil operativní změny bezpečnostních parametrů monitorovaného systému s využitím systémů bezpečnostních prvků IDS/IPS, FW a apod.

b. Bezpečnostní monitoring byl zajišťován nad informačním systémem a jeho vrstvami (např. síťovou, HW, datovou, vrstvou OS a aplikační vrstvou). Nedílnou součástí architektury tohoto monitorovaného informačního systému bylo portálové řešení (či jiné ekvivalentní rozhraní pro externí přístup), zpřístupňující koncovým uživatelům služby aplikační vrstvy prostřednictvím veřejné sítě Internet. Monitorovaný informační systém byl provozován v geograficky oddělených lokalitách.

c. V průběhu plnění významné služby nenastaly závažné provozní nebo bezpečnostní incidenty zaviněné ze strany Uchazeče ani vady / incidenty kategorie A zaviněné ze strany Uchazeče spočívající zejména ve výskytu incidentů způsobených nesprávnou implementací a provozem bezpečnostního monitoringu či nastavením nepřiměřené úrovně logování (za „závažný provozní nebo bezpečnostní incident“ a „vada / incident kategorie A“ je Zadavatelem považován incident / vada nejvyššího stupně klasifikace (nejzávažnější) dle metriky, která byla u dané významné služby pro daného objednatele služby použita).

Vzhledem ke skutečnosti, že služby bezpečnostního monitoringu bývají v praxi součástí např. služeb provozu nebo služeb technické podpory, Zadavatel bude akceptovat doložení významné služby jako dílčího plnění v rámci většího projektu. Ze seznamu významných služeb však musí vyplývat splnění všech výše požadovaných parametrů pro službu bezpečnostního monitoringu.

IV. Uchazeč předloží alespoň **jednu významnou službu provedení penetračních testů**.

Za významnou službu se považuje služba **povedení penetračních testů**, jejíž rozsah plnění činil minimálně **300.000,- Kč bez DPH** a předmět plnění spočíval v poskytnutí **služby ověření stavu bezpečnosti a zranitelnosti informačního systému formou penetračních testů**.

Významná služba bude splňovat minimální úroveň dle následujících parametrů:

a. Penetrační testy obsahovaly testy webového rozhraní (webové aplikace) přístupné z prostředí veřejné sítě internet.

b. Testovaný systém byl v době poskytnutí služby využíván alespoň 3000 uživateli (jedná se o celkový počet registrovaných uživatelů v systému, nikoliv o současně pracující uživatele).

c. Prováděné penetrační testy zahrnovaly ad-hoc manuální postupy, nástroje a schopnosti testerů Uchazeče.

d. Penetrační testy byly prováděny podle mezinárodně uznávané metodiky (např. OWASP).

e. Penetrační testy obsahovaly zpracování návrhů doporučení pro odstranění zjištěných skutečností a nedostatků.

f. Penetrační testy byly protokolárně ukončeny a akceptovány ze strany objednatele služby.

b) Seznam techniků a osvědčení o vzdělání a odborné kvalifikaci Uchazeče a osob odpovědných za poskytování služeb (§ 56 odst. 2 písm. b) a e) ZVZ)

Splnění technických kvalifikačních předpokladů prokáže Uchazeč, který předloží požadovaná osvědčení o vzdělání a odborné kvalifikaci Uchazeče.

Pro prokázání splnění tohoto kvalifikačního předpokladu Zadavatel určuje minimální úroveň takto:

Uchazeč předloží formou čestného prohlášení seznam alespoň 8 odborných pracovníků (bezpečnostní tým), kteří budou odpovědní za poskytování plnění této Veřejné zakázky. Čestné prohlášení bude obsahovat prohlášení Uchazeče, že "*veškeré údaje uvedené v profesních životopisech předkládaných v nabídce na veřejnou zakázku "Zajištění služby Bezpečnostního dohledu pro MS2014+" jsou úplné a pravdivé*".

Bezpečnostní tým se musí skládat alespoň z následujících odborných pracovníků:

b1) Vedoucí týmu informační bezpečnosti

- ukončené vysokoškolské vzdělání
- praxe v ICT minimálně 5 let, z toho 3 roky v oblasti informační bezpečnosti
- praktické zkušenosti se zaváděním, implementací a nebo hodnocením systémů ISMS minimálně u 2 služeb s uvedením jejich stručného popisu, z toho alespoň u jedné služby v pozici vedoucího týmu/projektu
- prokazatelná znalost procesů zavádění, implementace a hodnocení systémů ISMS dle mezinárodně uznávané normy (např. ISO 27000 na úrovni ISMS Lead Auditor nebo Lead Implementer nebo obdobné)

b2) Bezpečnostní specialista

- ukončené vysokoškolské vzdělání nebo středoškolské vzdělání
- praxe v ICT minimálně 5 let

- praktické zkušenosti s návrhem a implementací bezpečnostních opatření dle přílohy A normy ČSN ISO/IEC 27001 v ICT systémech minimálně u 2 služeb s uvedením jejich stručného popisu
- prokazatelná znalost systémů řízení bezpečnosti informací dle mezinárodně uznávané normy (např. ISO 27000 na úrovni ISMS Auditor nebo ISMS Internal Auditor nebo obdobné) a, nebo postupů pro auditování informačních systémů v úrovni CISA

b3) Bezpečnostní konzultant

- ukončené vysokoškolské vzdělání nebo středoškolské vzdělání
- praxe v ICT minimálně 5 let
- praktické zkušenosti se zaváděním a implementací systémů kontinuity činností minimálně u 2 služeb s uvedením jejich stručného popisu
- prokazatelná znalost procesů zavádění a implementace systémů řízení kontinuity činností dle některého z mezinárodně uznávaných standardů nebo norem pro řízení kontinuity činností (např. BS25599, ISO 22301) nebo kontinuity služeb (např. ISO 20000)

b4) Vedoucí týmu monitoringu a testování

- ukončené vysokoškolské vzdělání
- praxe v ICT minimálně 5 let
- praktické zkušenosti s prováděním bezpečnostního monitoringu, analýz auditních záznamů a reportování výsledků bezpečnostního monitoringu minimálně u 2 služeb s uvedením jejich stručného popisu
- praktické zkušenosti s řešením informační bezpečnosti v prostředí založeném na produktech Microsoft

b5) Specialista - bezpečnostní monitoring

- ukončené vysokoškolské vzdělání nebo středoškolské vzdělání
- praxe v ICT minimálně 5 let
- prokazatelná znalost vyhodnocovacího centra bezpečnostního monitoringu v rozsahu komponent nabízených Uchazečem v rámci tohoto zadávacího řízení
- praktické zkušenosti s prováděním bezpečnostního monitoringu pomocí technologií nabízených Uchazečem v rámci tohoto zadávacího řízení minimálně u 1 služby s uvedením jejího stručného popisu

b6) Specialista - monitoring

- ukončené vysokoškolské vzdělání nebo středoškolské vzdělání
- praxe v ICT minimálně 5 let
- praktické zkušenosti s řešením informační bezpečnosti a nastavením technických parametrů bezpečnostních služeb a nástrojů v prostředí produktů Microsoft,
- praktické zkušenosti s řešením a konfigurací auditních nástrojů operačních systémů Microsoft Windows a virtualizačních center Hyper-V
- praktické zkušenosti s prováděním bezpečnostního monitoringu/dohledu databázové platformy Oracle minimálně u 1 služby s uvedením jejího stručného popisu

b7) Operátor - monitoring

- ukončené vysokoškolské vzdělání nebo středoškolské vzdělání

- praxe v ICT minimálně 3 roky
- praktické zkušenosti s prováděním bezpečnostního monitoringu pomocí technologií nabízených Uchazečem v rámci tohoto zadávacího řízení minimálně u 1 služby s uvedením jejího stručného popisu
- praktické zkušenosti s řešením nebo prováděním procesů a postupů poskytování technické podpory 2. úrovně.

b8) Specialista - tester

- ukončené vysokoškolské vzdělání nebo středoškolské vzdělání
- praxe v ICT minimálně 3 roky
- praktické zkušenosti s prováděním auditů prostředí informačních a komunikačních systémů s důrazem na kontroly, testování bezpečnosti a penetrační testy těchto systémů
- praktické zkušenosti s prováděním penetračních testů webových aplikací minimálně u 2 služeb s uvedením jejich stručného popisu.

Ve vztahu ke každému odbornému pracovníkovi shora (b1 až b8) předloží Uchazeč:

- **Profesní životopis**, ve kterém bude uvedeno minimálně:

a. jméno, příjmení a titul,

b. dosažené vzdělání,

c. řídící / odborná role v realizačním týmu,

d. zkušenosti / praxe v oblasti bezprostředně související s úlohou v realizačním týmu v souladu s požadavky na členy realizačního týmu,

e. seznam odborných osvědčení vztahujících se k požadované řídící / odborné roli zpracovaný v souladu s dále uvedenými podmínkami,

f. další údaje podstatné pro plnění svěřené role.

Součástí profesního životopisu bude rovněž čestné prohlášení podepsané odborným pracovníkem o úplnosti a pravdivosti údajů uvedených v příslušném profesním životopisu.

V případě, že Zadavatel v této kapitole vyžaduje “dosažené vzdělání” nebo „prokazatelnou znalost“ určité oblasti, musí být možné takovou skutečnost doložit (prokázat) prostřednictvím:

- vysokoškolského diplomu nebo maturitního vysvědčení,
- relevantního mezinárodně uznávaného certifikátu pro danou oblast,
- relevantního certifikátu nebo dokladu o absolvování školení příslušného výrobce HW/SW,

Kompletní výčet dokladů bude uveden u každého odborného pracovníka v profesním životopisu v části Seznam odborných osvědčení.

7. POVINNÁ SOUČÁST NABÍDKY (DLE § 68 ODST. 3 ZVZ)

Uchazeč je v souladu s § 68 odst. 3 ZVZ povinen učinit součástí Nabídky tyto údaje:

a. seznam statutárních orgánů nebo členů statutárních orgánů, kteří v posledních 3 letech od konce lhůty pro podání nabídek byli v pracovněprávním, funkčním či obdobném poměru u Zadavatele,

b. seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10 % základního kapitálu, vyhotovený ve lhůtě pro podání nabídek (pouze pokud má Uchazeč formu akciové společnosti),

c. prohlášení Uchazeče o tom, že neuzavřel a neuzavře v souvislosti se zadávanou Veřejnou zakázkou dohodu zakázanou dle zákona č. 143/2001 Sb., o ochraně hospodářské soutěže, ve znění pozdějších předpisů.

Zadavatel doporučuje využít vzorové čestné prohlášení, které je uvedeno v Příloze č. 2 této Zadávací dokumentace.

8. POŽADAVKY NA ZPŮSOB ZPRACOVÁNÍ NABÍDKY

8.1. POŽADAVKY NA OBSAH, ČLENĚNÍ A ZPRACOVÁNÍ NABÍDKY

Nabídka bude obsahovat:

a. Vyplněný Krycí list (viz Příloha č. 1 této Zadávací dokumentace), který bude vložen jako první list Nabídky.

b. Obsah Nabídky.

c. Identifikační údaje Uchazeče dle §17, písm. d) ZVZ a dále, bankovní spojení, jméno kontaktní osoby, její telefon, fax, poštovní a e-mailová adresa, id datové schránky.

d. Případně plnou moc osoby zmocněné statutárním orgánem Uchazeče k jednání a podepisování za Uchazeče.

e. Doklad o poskytnutí jistoty.

f. Čestné prohlášení prokazující informace dle §68, odst. 3 ZVZ.

g. Doklady prokazující splnění kvalifikačních předpokladů Uchazeče v pořadí:

- Základní kvalifikační předpoklady,
- Profesní kvalifikační předpoklady,
- Čestné prohlášení o ekonomické a finanční způsobilosti splnit Veřejnou zakázku,
- Technické kvalifikační předpoklady,
- Doklady dle § 51 odst. 4 ZVZ,
- Platnou smlouvu o sdružení v případě podání společné nabídky více Uchazečů, která bude v souladu s obchodními podmínkami dle kap. 12.1 této Zadávací dokumentace.

h. Nabídková cena (Cenový list) při dodržení pokynů a ve struktuře tabulky dle článku 10 této Zadávací dokumentace jako jediný a nezbytný údaj pro hodnocení dle dílčího hodnotícího kritéria č. 1 „Výše Celkové ceny nabídky“). Zadavatel v této souvislosti upozorňuje, že Smlouva o poskytování služeb je uzavírána na dobu neurčitou a v čl. 5.1 tedy obsahuje pouze celkovou cenu služeb za 1 vyhodnocovací období (to je za jeden kalendářní měsíc). Výše Celkové ceny Nabídky je však v souladu s čl. 10 této Zadávací dokumentace cena za 48 vyhodnocovacích období.

   Uchazeč v této části nabídky zároveň uvede rozklad paušálních cen v souladu s Přílohou č. 5 této Zadávací dokumentace. Rozklad paušálních cen slouží Zadavateli pro posouzení, zda lze jednoznačně a přesně identifikovat veškeré cenové položky, na jejichž základě Uchazeč kalkuloval Celkovou cenu Nabídky a lze tak jednoznačně identifikovat veškeré náklady Zadavatele na zajištění předmětu plnění tohoto zadávacího řízení.

i. Řádně podepsaný návrh **Smlouvy o poskytování služeb** s doplněnými údaji (návrh smlouvy musí být podepsán osobou oprávněnou Uchazeče zastupovat a podepisovat v souladu se způsobem podepisování uvedeným ve výpisu z obchodního rejstříku nebo zástupcem zmocněným k tomuto úkonu podle právních předpisů).

- Seznam subdodavatelů uvede Uchazeč do **Přílohy č. 2 Smlouvy o poskytování služeb**. Uchazeč je povinen uvést seznam subdodavatelů podílejících se na plnění předmětu Veřejné zakázky (i těch, jejichž prostřednictvím nebude prokazováno splnění části kvalifikace), s uvedením jejich identifikačních údajů a rozsahu dodávek nebo činností, které budou v rámci Veřejné zakázky zajišťovat.
- Popis způsobu realizace Veřejné zakázky uvede Uchazeč do **Přílohy č. 4 Smlouvy o poskytování služeb**. Detailní popis způsobu poskytování všech služeb, popis přístupu k řízení a zajištění požadovaných služeb ve struktuře Přílohy č. 1 "Katalog služeb a podmínky poskytování bezpečnostního dohledu" Smlouvy o poskytování služeb. Uchazeč zde uvede veškeré relevantní informace týkající se poskytovaných služeb, které nejsou uvedeny v Příloze č. 1 Smlouvy o poskytování služeb (Zadavatel nepřipouští duplicitu textů v Příloze č. 1 a v Příloze č. 4 Smlouvy) a to v podrobnosti nezbytné pro hodnocení:
  - subkritéria „Navržený způsob poskytování služeb řízení informační bezpečnosti“ dílčího hodnotícího kritéria č. 2 „Navržený způsob a postup poskytovaných služeb“. Minimálně však:
    - Implementační plán systému řízení informační bezpečnosti, popis jednotlivých kroků s názvy a obsahy jednotlivých výstupů, včetně návrhů termínů realizace navržených kroků,
    - procesy a postupy (metodiky), kterými bude Uchazeč realizovat poskytování služeb,
    - požadavky na součinnost Zadavatele, Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí při realizaci.
  - subkritéria „Navržený způsob poskytování služeb bezpečnostního monitoringu“ dílčího hodnotícího kritéria č. 2 „Navržený způsob a postup poskytovaných služeb“. Minimálně však:
    - detailní návrh řešení bezpečnostního monitoringu Aplikace MS2014+ a Prostředí, tj.:
      - jednotlivé kroky implementace bezpečnostního monitoringu včetně časového průběhu,
      - řešení HW/SW vyhodnocovacího centra bezpečnostního monitoringu, přičemž detail popisu řešení musí umožnit identifikovat veškeré HW/SW komponenty, ze kterých se řešení bude skládat. Zejména se jedná o:
        i. vlastní nástroj bezpečnostního monitoringu včetně identifikace všech modulů a komponent, které budou v rámci řešení nasazeny, potřebných SW licencí a licencí podpory výrobce.
        ii. detailní výčet všech HW komponent (appliancí, serverů, úložišť a případných dalších), které bude Uchazeč v rámci řešení implementovat, včetně licencí podpory výrobce HW,
        iii. v případě implementace serverů musí být dále identifikovány i licence a podpora výrobce souvisejícího serverového SW (operační systémy, databáze, atd.),
        iv. popis škálovatelnosti nabízeného řešení v případě budoucí potřeby výkonového a kapacitního posílení vyhodnocovacího centra.

- procesy a postupy, kterými bude Uchazeč realizovat poskytování služeb bezpečnostního monitoringu,
- nástroje a opatření, kterými Uchazeč hodlá zabránit nebo minimalizovat:
  - možnost vzniku provozních a bezpečnostních incidentů vzniklých na základě činnosti Uchazeče resp. v souvislosti s poskytování služeb Uchazeče;
  - možnost vzniku chyb způsobených lidským faktorem při poskytování služeb, příp. umožní jejich včasnou identifikaci a odstranění,
- požadavky na součinnost Zadavatele, Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí při poskytování služby.

- subkritéria „Navržený způsob poskytování služeb auditu“ dílčího hodnotícího kritéria č. 2 „Navržený způsob a postup poskytovaných služeb“. Minimálně však:
  - popis metodiky penetračních testů,
  - harmonogram provádění penetračních testů
  - nástroje a postupy provádění penetračních testů

Uchazeč, za účelem předložení vhodného způsobu realizace Veřejné zakázky, který bude přizpůsoben specifikům a technickým parametrům Aplikace MS2014+ a Prostředí, využije informace dostupné v rámci souvisejících zadávacích řízení na profilu Zadavatele na adresách:

https://ezak.mmr.cz/contract_display_668.html a

https://ezak.mmr.cz/contract_display_823.html.

- Bezpečnostní tým pro služby Uchazeč uvede **v Příloze č. 5 Smlouvy o poskytování služeb**; Uchazeč je povinen obsadit role v bezpečnostním týmu pracovníky, kterými prokázal kvalifikaci dle bodů b1) až b8) písm. b) kap. 6.4.1 této zadávací dokumentace.

  Uchazeč není oprávněn v rámci nabídky a návrhu smlouvy vytvářet nové role, pouze je oprávněn jmenovat další pracovníky do Zadavatelem stanovených rolí. Počty těchto dalších pracovníků v jednotlivých rolích pro oblast služeb Uchazeč stanoví na základě rozsahu požadovaných služeb a SLA parametrů uvedených k jednotlivým službám v Příloze č. 1 Smlouvy o poskytování služeb. U pracovníků v zaměstnaneckém poměru musí Uchazeč jejich počty stanovit také s ohledem na maximální rozsah pracovní doby dle zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

  Všechny Uchazečem jmenované pracovníky pro nezbytné obsazení jednotlivých rolí je Uchazeč povinen uvést v Příloze č. 5 Smlouvy o poskytování služeb, přičemž pracovníky, kterými není prokazována kvalifikace dle bodů b1) až b8) kap. 6.4.1 písm. b) této zadávací dokumentace, uvede Uchazeč pouze do této Přílohy č. 5 Smlouvy.

j. Řádně podepsaný návrh "**Smlouvy o dodržování bezpečnostních opatření v rámci spolupráce**" s doplněnými údaji (návrh smlouvy musí být podepsán osobou oprávněnou za Uchazeče jednat a podepisovat v souladu se způsobem podepisování uvedeným ve výpisu z obchodního rejstříku nebo zástupcem zmocněným k tomuto úkonu podle právních předpisů);

k. CD s úplnou kopií Nabídky v elektronické podobě.

8.2. DALŠÍ POŽADAVKY NA ZPŮSOB ZPRACOVÁNÍ NABÍDKY

a. Nabídka včetně všech příloh musí být předložena v českém nebo ve slovenském jazyce.

b. Nabídka bude předložena ve 2 listinných vyhotoveních, označených jako "**Výtisk č. 1 – Originál**" a "**Výtisk č. 2 - Kopie**" a v 1 elektronickém provedení na CD nebo DVD (v obecně čitelném formátu DOC, PDF, apod.), označeném "**Elektronická kopie nabídky + název Uchazeče**". Elektronická kopie bude přesnou kopií výtisku č. 1 (včetně dokladů a úředních listin). Uchazeč je povinen dodat elektronické provedení v kvalitě umožňující vyhledávání v textových částech nabídky (s výjimkou částí obsahujících doklady nebo úřední listiny).

c. Nabídka bude kvalitním způsobem vytištěna tak, že bude dobře čitelná a nebude obsahovat opravy a přepisy a jiné nesrovnalosti, které by Zadavatele mohly uvést v omyl.

d. Nabídka bude zabezpečena proti neoprávněné manipulaci s jednotlivými listy, např. provázána šňůrkou s přelepením volných konců a opatřena na přelepu podpisem/razítkem Uchazeče (oprávněné osoby). V případě podání Nabídky v kroužkovém pořadači či podobném technickém provedení, musí být tato zabezpečena proti možné manipulaci s jednotlivými listy, ovšem opět tak, aby bylo možné jednotlivé listy při listování nabídkou bezproblémově obracet. Pokud to je z důvodu rozsahu nabídky nutné, lze nabídku rozdělit na několik částí;

e. Všechny listy Nabídky budou ve spodním okraji listiny očíslovány nepřerušenou vzestupnou číselnou řadou počínající číslem 1 na krycím listu (např. ručně psané). Vkládá-li Uchazeč do Nabídky jako její součást některý samostatný celek (listinu), který má již listy očíslovány vlastní číselnou řadou, Uchazeč očísluje i všechny tyto strany znovu, v rámci nepřerušené číselné řady celé zpracované Nabídky;

f. Předmětem posouzení a hodnocení je výhradně originál, který bude obsahovat všechny doklady v řádné formě. V případě zjištění rozporů mezi jednotlivými výtisky Nabídky, nebo mezi papírovou a elektronickou verzí Nabídky, se považuje za rozhodný text Nabídky označené jako „Originál“.

g. Nabídka bude splňovat pravidla publicity Operačního programu Technická pomoc 2007-2013, publikované na adrese: URL: http://www.strukturalni-fondy.cz/getmedia/b5a1fa9f-c6e5-4802-86fd-2b1c10d5dad8/Logo-manual-OPTP_b5a1fa9f-c6e5-4802-86fd-2b1c10d5dad8.pdf

8.3. VARIANTY NABÍDKY

Zadavatel nepřipouští varianty Nabídky.

8.4. SUBDODÁVKY

V souladu s ustanovením § 44 odst. 6 ZVZ požaduje Zadavatel, aby Uchazeč uvedl seznam subdodavatelů v Příloze č. 2 Smlouvy o poskytování služeb. Podrobné požadavky na jeho obsah jsou uvedeny v článku 8.1 písm. i) této Zadávací dokumentace.

8.5. DODATEČNÉ INFORMACE

Uchazeč je oprávněn po Zadavateli písemně požadovat dodatečné informace k zadávacím podmínkám. Písemné žádosti o dodatečné informace je možné zaslat na adresu kontaktní osoby uvedené v oznámení o zakázce a v článku 2 této Zadávací dokumentace.

Zadavatel má právo poskytnout Uchazečům dodatečné informace k zadávacím podmínkám i bez předchozí žádosti Uchazeče.

Postup při poskytování dodatečných informací se řídí dle § 49 ZVZ.

8.6. DALŠÍ POŽADAVKY ZADAVATELE

Zadavatel neposkytne náhradu nákladů, které Uchazeč vynaložil na účast v zadávacím řízení. Nabídky, kopie nabídek ani jednotlivé součásti nabídek Uchazečů či vyloučených Uchazečů nebudou vráceny.

9. LHŮTY A ZPŮSOB PODÁNÍ NABÍDEK

9.1. LHŮTA PRO PODÁNÍ NABÍDEK

Konec lhůty pro podání nabídek je uveden ve formuláři oznámení o zakázce.

9.2. ZPŮSOB PODÁNÍ NABÍDEK

Nabídka musí být podána v jedné, uzavřené obálce (či jiném obalu) následujícím způsobem:

Obálka (obal) bude na přelepu opatřen razítkem a podpisem Uchazeče (oprávněné osoby). V levé horní části lícní strany obálky (obalu) bude Nabídka označena identifikací Uchazeče, pod ní bude výrazným způsobem uvedeno: „**NEOTEVÍRAT! Veřejná zakázka " Zajištění služby Bezpečnostního dohledu pro MS2014+**“. Na obálce bude dále uvedena adresa, na kterou bude moci zadavatel zaslat vyrozumění dle § 71 odst. 5 ZVZ.

9.3. MÍSTO PRO PODÁNÍ NABÍDEK

Nabídku je třeba doručit na adresu Zadavatele nebo podat osobně v podatelně Zadavatele na adrese Staroměstské náměstí 6, 110 15 Praha 1.

9.4. ZADÁVACÍ LHŮTA

Zadávací lhůta (tj. lhůta, po kterou jsou Uchazeči podle § 43 ZVZ svými nabídkami vázáni) činí 6 měsíců a začíná běžet dnem následujícím po skončení lhůty pro podání nabídek.

9.5. OTEVÍRÁNÍ OBÁLEK

Obálky s nabídkami budou otevírány v sídle Zadavatele, na adrese Staroměstské náměstí 6, 110 15 Praha 1, datum a čas je uveden ve formuláři Oznámení o zakázce.

Otevírání obálek se uskuteční dle údajů uvedených ve formuláři Oznámení o zakázce. Otevírání obálek se mají právo zúčastnit zástupci Uchazečů, jejichž Nabídky byly řádně doručeny do konce lhůty pro doručení nabídek. Z organizačních důvodů je omezen počet zástupců každého Uchazeče na dvě fyzické osoby.

10. POŽADAVEK NA ZPŮSOB ZPRACOVÁNÍ NABÍDKOVÉ CENY (CENOVÉHO LISTU)

Celkovou cenu Nabídky uvede Uchazeč v následující struktuře:

	Položka	Cena v Kč bez DPH	Výše DPH v Kč	Cena v Kč včetně DPH
1	**Cenová nabídka za službu „Informační bezpečnost“** (do řádku 1 Tabulky vyplní Uchazeč položku za Službu BS01 dle odstavce 5.1.2 Smlouvy o poskytování služeb **vynásobenou 48**)	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]
2	**Cenová nabídka za „Ochrana osobních údajů“** (do řádku 2 Tabulky vyplní Uchazeč položku za Službu BS02 dle odstavce 5.1.2 Smlouvy o poskytování služeb **vynásobenou 48**)	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]
3	**Cenová nabídka za „Bezpečnostní monitoring“** (do řádku 3 Tabulky vyplní Uchazeč položku za Službu BS03 dle odstavce 5.1.2 Smlouvy o poskytování služeb **vynásobenou 48**)	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]
4	**Cenová nabídka za „Kontrola kvality poskytovaných služeb“** (do řádku 4 Tabulky vyplní Uchazeč položku za Službu BS04 dle odstavce 5.1.2 Smlouvy o poskytování služeb **vynásobenou 48**)	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]
5	**Cenová nabídka za „Audit prostředí“** (do řádku 5 Tabulky vyplní Uchazeč položku za Službu BS05 dle odstavce 5.1.2 Smlouvy o poskytování služeb **vynásobenou 48**)	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]	[DOPLNÍ UCHAZEČ]
6	**Celková cena Nabídky** (řádek 6 je součtem položek řádků 1 až 5)	**[DOPLNÍ UCHAZEČ]**	**[DOPLNÍ UCHAZEČ]**	**[DOPLNÍ UCHAZEČ]**

Ceny bude Uchazeč, v souladu se zněním Přílohy č. 1 Smlouvy o poskytování služeb, uvádět s přesností na dvě (2) desetinná místa.

Platí, že součástí celkové ceny Nabídky musí být veškeré náklady Uchazeče související poskytováním služeb dle těchto zadávacích podmínek. Součástí nabídkové ceny musí být veškeré náklady Uchazeče včetně dopravy, pracovních pomůcek a všech dalších nákladů.

Uchazeč je povinen podložit cenové nabídky za jednotlivé Služby dle Přílohy č. 1 Smlouvy o poskytování služeb **detailním rozkladem cen v rozsahu stanoveném Přílohou č. 5 této Zadávací dokumentace**.

Uchazeč je povinen stanovit Celkovou cenu Nabídky v Kč bez DPH tak, aby nebyla vyšší než předpokládaná hodnota veřejné zakázky. Pokud bude celková nabídková cena vyšší, jedná se o nepřijatelnou nabídku a v souladu s ustanovením § 76 ZVZ bude nabídka vyřazena.

Zadavatel na tomto místě znovu připomíná, že ceny za jednotlivé položky ve smlouvě na veřejnou zakázku jsou uváděny za 1 vyhodnocovací období (to je za jeden kalendářní měsíc). Naopak ve výše uvedeném cenovém listu jsou ceny za jednotlivé položky uvedeny za 48 vyhodnocovacích období (kalendářních měsíců).

11. HODNOCENÍ NABÍDEK

11.1. ZÁKLADNÍ HODNOTÍCÍ KRITÉRIA

Zadavatel stanovil, v souladu s ustanovením § 78 odst. 1 písm. a) ZVZ, základním hodnotícím kritériem ekonomickou výhodnost Nabídky které rozdělil na dílčí hodnotící kritéria a subkritéria.

Dílčí hodnotící kritérium	váha (%)	Subkritérium	váha (%)
1) Výše Celkové ceny Nabídky	60		
2) Navržený způsob a postup poskytovaných služeb	40	Navržený způsob poskytování služeb řízení informační bezpečnosti	20
		Navržený způsob poskytování služeb bezpečnostního monitoringu	60
		Navržený způsob poskytování služeb auditu	20

Přičemž pro přepočty výše stanovených vah platí, že při veškerých výpočtech a úpravách v rámci hodnocení budou čísla zaokrouhlována na dvě desetinná místa podle matematických pravidel.

11.2. DÍLČÍ HODNOTÍCÍ KRITÉRIUM „VÝŠE CELKOVÉ CENY NABÍDKY“

Předmětem hodnocení bude „Celková cena Nabídky" (v Kč včetně DPH dle tabulky v kap. 10 Zadávací dokumentace), nikoli dílčí ceny, ze kterých je vypočtena.

Pro číselně vyjádřitelné dílčí hodnotící kritérium „Výše Celkové ceny Nabídky“ získá hodnocená nabídka bodovou hodnotu, která vznikne násobkem 100 a poměru hodnoty nejvhodnější nabídky (tj. nabídky s nejnižší celkovou cenou nabídky) k hodnocené Nabídce.

$$\text{Počet bodů hodnocené Nabídky} = 100 * \frac{\text{cena nejvýhodnější nabídky (nejnižší Celková cena Nabídky)}}{\text{cena aktuálně hodnocené nabídky}} = DHK1$$

Takto získané hodnocení je ve výpočtovém vzorci celkového hodnocení nabídky označeno jako DHK1.

11.3. DÍLČÍ HODNOTÍCÍ KRITÉRIUM “ NAVRŽENÝ ZPŮSOB A POSTUP POSKYTOVANÝCH SLUŽEB“

V rámci dílčího hodnotícího kritéria „Navržený způsob a postup poskytovaných služeb“ budou hodnocena následující subkritéria:

a) Subkritérium „Navržený způsob poskytování služeb řízení informační bezpečnosti“

Předmětem hodnocení bude Uchazečem navržený způsob a postup implementace systému řízení informační bezpečnosti dle norem řady ISO 27000 (harmonogram průběhu – Implementační plán) pro systém MS2014+; obsahující popis jednotlivých kroků, názvů a obsahů jednotlivých výstupů; procesů a postupů (metodik) realizace, termínů realizace navržených kroků a požadavky na součinnost ze strany Zadavatele, Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí a jejich zdůvodnění v rámci této VZ.

Jako nejvhodnější bude hodnocena nabídka, ve které Uchazeč nejlépe logicky, věcně a v souladu s požadavky Zadavatele dle těchto zadávacích podmínek zpracuje Implementační plán systému řízení bezpečnosti informací pro systém MS2014 + s důrazem na způsob naplnění požadavků stanovených pro Službu BS01 dle Přílohy č. 1 Smlouvy, zachování vazby na stanovené termíny a logickou posloupnost a souslednost jednotlivých kroků Implementačního plánu. Při hodnocení bude přihlíženo k požadovanému objemu součinnosti Zadavatele, Provozovatele Aplikace MS2014+ a Poskytovatele služeb Prostředí a jeho zdůvodnění s důrazem na ověření, že nedochází k přenesení výkonu požadovaných činností zpět na Zadavatele.

b) Subkritérium „Navržený způsob poskytování služeb bezpečnostního monitoringu“

Předmětem hodnocení bude Uchazečem navržený popis řešení bezpečnostního monitoringu Aplikace MS2014+ a Prostředí; procesy a postupy poskytování služeb bezpečnostního monitoringu; nástroje a opatření minimalizující vznik provozních a bezpečnostních incidentů vzniklých na základě činnosti Uchazeče a možnost vzniku chyb způsobených lidským faktorem při poskytování služeb.

Jako nejvhodnější bude hodnocena nabídka, ve které Uchazeč navrhne způsob, který nejlépe věcně a v souladu s požadavky Zadavatele dle těchto zadávacích podmínek zpracuje návrh technického řešení bezpečnostního monitoringu Aplikace MS2014+ a Prostředí, vymezí schopnosti a parametry nabízeného řešení HW/SW vyhodnocovacího centra v oblasti sběru, vyhodnocování a ukládání auditních informací s důrazem na minimalizaci vzniku provozních a bezpečnostních incidentů a stanoví vhodnou posloupnost jednotlivých kroků vedoucích k zajištění plné funkčnosti bezpečnostního monitoringu Prostředí a Aplikace MS2014+ ve vazbě na stanovené termíny plnění.

c) Subkritérium „Navržený způsob poskytování služeb auditu“

Předmětem hodnocení bude Uchazečem navržený popis způsobu poskytování služeb auditu a technické kontroly s důrazem na oblast penetračních testů (metodiku, harmonogram, nástroje a postupy).

Jako nejvhodnější bude hodnocena nabídka, ve které Uchazeč nejlépe logicky, věcně a v souladu s požadavky Zadavatele dle těchto zadávacích podmínek navrhne metodiku penetračních testů a harmonogram jejich provádění, zdůvodní vhodnost zvolených nástrojů a popíše opatření vedoucí k minimalizaci vzniku provozních a bezpečnostních incidentů činností Uchazeče resp. v souvislosti s poskytování služeb penetračních testů a minimalizuje tak dopad na kvalitu a kvantitu poskytovaných služeb Aplikace MS2014+ a Prostředí.

Společné ustanovení pro hodnocení subkritérií dílčího hodnotícího kritéria „Navržený způsob a postup poskytovaných služeb“:

Pro hodnocení nabídek použije hodnotící komise bodovací stupnici v rozsahu 1 až 100. Každé jednotlivé nabídce bude v rámci hodnoceného subkritéria přidělena bodová hodnota, která odráží úspěšnost předmětné nabídky v rámci hodnoceného subkritéria, přičemž nejlépe hodnocená nabídka obdrží 100 bodů.

Nepřepočtené hodnocení nabídky za dílčí hodnotící kritérium č. 2 „Navržený způsob a postup poskytovaných služeb“ je pak rovno váženému součtu bodů, které hodnocená nabídka získala za všechna subkritéria dle vzorce:

$$NHDHK = \frac{\text{20x body za subkritérium „Navržený způsob poskytování služeb řízení informační bezpečnosti“}}{100} + \frac{\text{60x body za subkritérium „Navržený způsob poskytování služeb bezpečnostního monitoringu“}}{100} + \frac{\text{20x body za subkritérium „Navržený způsob poskytování služeb auditu“}}{100}$$

Nepřepočtená hodnocení nabídek za dílčí hodnotící kritérium č. 2 „Navržený způsob a postup poskytovaných služeb“ (NHDHK) budou následně přepočtena (normalizována) tak, aby nejlépe hodnocená nabídka za dílčí hodnotící kritérium č. 2 „Navržený způsob a postup poskytovaných služeb“ získala 100 bodů:

$$DHK2 = 100 \times \frac{NHDHK}{NHDHK\ MAX}$$

NHDHK = Nepřepočtené hodnocení nabídky za dílčí hodnotící kritérium „Navržený způsob a postup poskytovaných služeb“
NHDHK MAX = Nepřepočtené hodnocení za dílčí hodnotící kritérium „Navržený způsob a postup poskytovaných služeb“ nabídky, která byla v rámci tohoto dílčího hodnotícího kritéria hodnocena nejlépe
DHK2 = hodnocení přepočítávané nabídky za dílčí hodnotící kritérium „Navržený způsob a postup poskytovaných služeb“

Takto získané hodnocení je ve výpočtovém vzorci celkového hodnocení nabídky označeno jako DHK2.

11.4. CELKOVÉ HODNOCENÍ NABÍDKY

Celkové bodové hodnocení („CBH“) nabídky v rámci základního hodnotícího kritéria ekonomická výhodnost nabídky bude tvořit vážený součet bodů, které hodnocená nabídka získala v rámci dílčích hodnotících kritérií „Výše Celkové ceny Nabídky“ a „Navržený způsob realizace veřejné zakázky“ redukovaných příslušnými vahami:

$$CBH = \frac{60 \times DHK1}{100} + \frac{40 \times DHK2}{100}$$

Na základě celkového bodového hodnocení („CBH“) u jednotlivých nabídek hodnotící komise stanoví výsledné pořadí nabídek v rámci základního hodnotícího kritéria ekonomické výhodnosti nabídky tak, že nabídky budou seřazeny dle počtu získaných bodů. Jako nejúspěšnější bude stanovena nabídka, která dosáhne nejvyšší bodové hodnoty.

V případě rovnosti celkového počtu bodů rozhodne o vítězné Nabídce Výše Celkové ceny Nabídky (nabídka s nejnižší Výší Celkové ceny Nabídky bude nabídkou vítěznou).

12. OBCHODNÍ A PLATEBNÍ PODMÍNKY

Obchodní a platební podmínky ve smyslu § 44 odst. 3 písm. a) ZVZ, vymezující budoucí rámec smluvního vztahu mezi Zadavatelem a vybraným Uchazečem, jsou podrobně zapracovány do závazného návrhu Smlouvy o poskytování služeb, která je nedílnou součástí této Zadávací dokumentace a tvoří její Přílohu č. 4.

Uchazeč do návrhu smluv doplní požadované údaje (zejména vlastní identifikaci, údaje vztahující se k hodnotícím kritériím a další údaje, které jsou v návrhu smluv označeny slovy „doplní Uchazeč“, resp. „doplní Poskytovatel“). Takto doplněné obchodní podmínky předloží jako svůj návrh smlouvy. Návrh smlouvy bude řádně podepsán osobou oprávněnou jednat za Uchazeče.

Uchazeč není oprávněn měnit či doplňovat text návrhu smlouvy s výjimkou údajů uvedených v předchozím odstavci. Obchodní a platební podmínky vymezují budoucí rámec smluvního vztahu. Nabídka Uchazeče musí respektovat stanovené obchodní a platební podmínky a v žádné části nesmí obsahovat ustanovení, které by bylo v rozporu s těmito podmínkami.

Uchazeč je v návrhu smlouvy v rámci údajů o ceně a platebních podmínkách povinen uvést údaje, tak aby:

a) byly stanoveny za požadované časové období,
b) byla dodržena podmínka, že Celková cena Nabídky v Kč bez DPH uvedená v cenovém listu nebude vyšší než předpokládaná hodnota veřejné zakázky

Jestliže Uchazeč poruší některý z požadavků Zadavatele, bude Nabídka posouzena tak, že nesplňuje zadávací podmínky a Uchazeč bude vyloučen podle ust. § 76 odst. 6 ZVZ.

12.1. PODÁNÍ SPOLEČNÉ NABÍDKY VÍCE UCHAZEČI

Podá-li společnou nabídku více Uchazečů (sdružení více právních subjektů), jsou povinni předložit v rámci nabídky smlouvu o sdružení, která bude splňovat následující náležitosti:

- bude obsahovat ustanovení, že jsou dodavatelé zavázání společně a nerozdílně v souladu s §51, odst. 6 ZVZ,
- bude obsahovat identifikaci jediného člena sdružení, který je oprávněn jednat za ostatní dodavatele ve věcech spojených s poskytováním plnění dle smlouvy na veřejnou zakázku „Zajištění služby Bezpečnostního dohledu pro MS2014+“ navenek (dále jen „Zastupující člen sdružení“). Kdo jedná za Zastupujícího člena sdružení navenek, se určí dle obecně závazných právních předpisů. Povinností určit Zastupujícího člena sdružení není dotčeno oprávnění Zastupujícího člena sdružení jmenovat jako Oprávněnou osobu dle Smlouvy o poskytování služeb i osobu, která není v zaměstnaneckém či obdobném poměru k Zastupujícímu členu sdružení.

12.2. POJIŠTĚNÍ ODPOVĚDNOSTI ZA ŠKODU

Zadavatel požaduje před podpisem smluv předložení kopie pojistné smlouvy, která se vztahuje na plnění předmětu dle návrhu Smlouvy o poskytování služeb (viz. Příloha č. 4 této zadávací dokumentace) a jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Uchazečem třetí osobě, s minimálním limitem pojistného plnění ve výši nejméně 10.000.000,- Kč (slovy: deset miliónů korun českých) s maximální spoluúčastí Uchazeče ve výši 10 %.

Pojištění je možné doložit i pojistným certifikátem, musí z něj být však zřejmá výše pojistného plnění, míra spoluúčasti a předmět pojištění (pojištění odpovědnosti za škodu způsobenou Uchazečem třetí osobě a typově popsaná činnost, která je kryta pojištěním).

13. OSTATNÍ

13.1. PRÁVA ZADAVATELE

Zadavatel si dále vyhrazuje právo posunout termín předpokládaného zahájení plnění zakázky v souvislosti s termínem ukončení tohoto zadávacího řízení.

13.2. PROHLÍDKA MÍSTA

Zadavatel neorganizuje prohlídku místa plnění.

13.3. JISTOTA

Zadavatel požaduje, aby Uchazeči k zajištění svých povinností vyplývajících z účasti v zadávacím řízení poskytli jistotu ve výši **500.000,- Kč** (slovy: pětset tisíc korun českých).

Pokud se Uchazeč rozhodne poskytnout jistotu formou složení peněžní částky na účet Zadavatele, tak peněžní prostředky složí na účet Zadavatele, jehož číslo je uvedeno v kap. 2 této Zadávací dokumentace. Variabilní symbol a specifický symbol jsou rovněž uvedeny v kap. 2 této Zadávací dokumentace.

Doklad o jistotě poskytnuté formou složení peněžní částky na účet Zadavatele nebo originál záruční listiny budou součástí Nabídky, zadavatel je navrátí za podmínek dle § 67 ZVZ.

14. STRUKTUROVANÝ SEZNAM DOKUMENTŮ TVOŘÍCÍCH ZADÁVACÍ PODMÍNKY

Specifikace dokumentu	Obsah dokumentu	Označení dokumentu
Zadávací dokumentace na Veřejnou zakázku "Zajištění služby Bezpečnostního dohledu pro MS2014+"	Základní dokument zadávacího řízení. V souladu s požadavky ZVZ vymezuje předmět Veřejné zakázky, kvalifikační předpoklady, hodnotící kritéria a další údaje o zadávacím řízení v detailu potřebném pro zpracování Nabídky Uchazeče.	ZD_Bezpečnostní dohled
Přílohy Zadávací dokumentace		
Příloha č. 1: Krycí list	Šablona pro vyplnění základní identifikace Uchazeče	ZD_P1_Krycí list nabídky
Příloha č. 2: Vzorová čestné prohlášení	Šablona čestného prohlášení pro potřeby prokázání základních kvalifikačních předpokladů dle §53, odst. 1 ZVZ a čestného prohlášení dle §68 odst. 3 ZVZ (povinná součást nabídky).	ZD_P2_Vzorová čestné prohlášení
Příloha č. 3: Smlouva o dodržování bezpečnostních opatření v rámci spolupráce	Smlouva upravuje podmínky dodržování bezpečnostních opatření a ochrany důvěrných informací mezi Zadavatelem a Uchazečem.	ZD_P3_NDA smlouva
Příloha č. 4: Smlouva na zajištění služby Bezpečnostního dohledu pro	Vymezení předmětu plnění a podmínek smluvního vztahu mezi Zadavatelem a Uchazečem	ZD_P4_Smlouva o poskytování služeb

Specifikace dokumentu	Obsah dokumentu	Označení dokumentu
MS2014+ (Smlouva o poskytování služeb)	pro oblast služeb	
Příloha č. 5: Rozklad paušálních cen služeb	Příloha slouží k podrobnému rozkladu paušálních cen za Vyhodnocovací období u jednotlivých služeb a jako podklad pro posouzení způsobu tvorby Celkové ceny Nabídky.	ZD_P5_Rozklad cen
Přílohy Smlouvy o poskytování služeb		
Příloha č. 1: Katalog služeb a podmínky poskytování bezpečnostního dohledu	Příloha podrobně vymezuje předmět, podmínky a kvalitu služeb poskytovaných Uchazečem	S_P1_ KS a podmínky poskytování BD
Příloha č. 2: Seznam subdodavatelů	Seznam subdodavatelů Uchazeče, kteří se budou podílet na plnění služeb včetně uvedení rozsahu činností subdodavatele	S_P2_Seznam subdodavatelů
Příloha č. 3: Zadávací dokumentace	Kopie Zadávací dokumentace	S_P3_Zadávací dokumentace
Příloha č. 4: Popis způsobu poskytování služeb Bezpečnostního dohledu	Popis způsobu poskytování služeb Bezpečnostního dohledu v rozsahu stanoveném písm. i) kap. 8.1 Zadávací dokumentace	S_P4_Popis poskytování služeb
Příloha č. 5: Bezpečnostní tým	Složení týmu Uchazeče, který bude zajišťovat plnění služeb	S_P5_Bezpečnostní tým
Standardizovaný formulář „oznámení o zakázce“		
Bude uveřejněn ve Věstníku veřejných zakázek a v Evropském úředním věstníku.		

V Praze dne 24. 10. 2014

Česká republika – Ministerstvo pro místní rozvoj

[redacted]

RNDr. Blanka Fischerová
ředitelka Odboru správy monitorovacího systému

Číslo v CES: 5390

Příloha č. 4 Smlouvy o poskytování služeb

Popis způsobu poskytování služeb Bezpečnostního dohledu

1 Obsah

1 OBSAH 2

2 PŘÍSTUP SPOLEČNOSTI T – MOBILE K ŘEŠENÍ ZAKÁZKY 3

3 POPIS SLUŽEB 5

NAVRŽENÝ ZPŮSOB POSKYTOVÁNÍ SLUŽEB ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI 5

PŘÍSTUP POSKYTOVATELE K REALIZACI INFORMAČNÍ BEZPEČNOSTI 5
3.1 SLUŽBA „BS01_INFORMAČNÍ BEZPEČNOST“ 6
3.2 SLUŽBA „BS02_OCHRANA OSOBNÍCH ÚDAJŮ“ 28

NAVRŽENÝ ZPŮSOB POSKYTOVÁNÍ SLUŽEB ŘÍZENÍ BEZPEČNOSTNÍHO MONITORINGU 46

3.3 SLUŽBA „BS03_BEZPEČNOSTNÍ MONITORING“ 46

NAVRŽENÝ ZPŮSOB POSKYTOVÁNÍ SLUŽEB AUDITU 77

3.4 SLUŽBA „BS04_KONTROLA KVALITY POSKYTOVANÝCH SLUŽEB“ 77
3.5 SLUŽBA „BS05_AUDIT PROSTŘEDÍ“ 80

4 REJSTŘÍK A SEZNAMY 86

2 Přístup společnosti T – Mobile k řešení zakázky

Společnost T-Mobile Czech republic jako Uchazeč předkládá Objednateli tuto nabídku na řešení požadavků zajištění bezpečnosti infrastruktury MS2014+ a zajistí splnění požadavků Objednatele

Práce na projektu budou realizovány v jednotlivých fázích dle požadavků každé ze služeb specifikovaných Objednatelem. Uchazeč bude práce provádět dle nejlepšího vědomí, v souladu se zadáním Objednatele.

Práce na zakázce budou realizovány dle projektové metodiky T-Mobile Česká republika, v případech, kde je vyžadováno použití jiné metodiky v rámci dané služby bude použito příslušné projektové metodiky pro řízení projektu tak, aby bylo zajištěno kontinuální dodání všech specifikovaných výstupních dokumentů a plnění. Výsledky budou průběžně prezentovány řídícímu výboru, složenému ze sponzora obou stran.

V nabídce uchazeče dále bude popsáno zajištění vzniku produktů projektu. Se Objednatelem budou odsouhlasena akceptační kritéria u jednotlivých produktů. Významnou částí bude odsouhlasení mechanismů pro přijetí změn ve smlouvě. Konečně, bude projednán a odsouhlasen proces pro schvalování dokumentů a výstupů. Detailní plán realizace jednotlivých služeb bude respektovat předpokládané termíny plnění jednotlivých fází daných služeb.

Řídící výbor projektu bude navržen tak, aby umožnil efektivní „governance“ jednotlivých služeb. Struktura řídícího výboru je nastavena tak, že přijímá důležitá rozhodnutí a schází se na pravidelných schůzkách během implementace klíčových milníků v rámci dané služby. Za dodávané služby je odpovědný vedoucí týmu jednotlivých oblastí.

Dodavatel předpokládá, že Objednatel disponuje částí relevantní dokumentace, která bude poskytnuta k naplnění cílů realizace zakázky. Seznam požadavků je centrálně shromážděn u projektového manažera dodavatele (popř. vedoucích jednotlivých týmů), který je předá projektovému manažerovi Objednatele - pokud není stanoveno jinak.
Dokumenty jsou shromážděny u dodavatele a je s nimi nakládáno dle klasifikace a pravidel požadovaných Objednatelem. Dodavatel dokumenty a informace analyzuje s ohledem na cíle zakázky a z hlediska nutnosti definovat rizika.

Ze strany dodavatele je komunikace v rámci projektu zajištěna projektovým manažerem nebo vedoucím jednotlivých oblastí (podle reálného nastavení týmu). Jednotliví členové týmu dodavatele mu předávají dílčí a finální verze výstupů. Pro jednotlivé výstupy jsou definována akceptační kritéria tak, aby se předešlo pozdějším nedorozuměním.

Dále bude popsáno zajištění vzniku produktů projektu. Se Objednatelem budou odsouhlasena akceptační kritéria u jednotlivých produktů. Významnou částí bude odsouhlasení mechanismů pro přijetí změn a změnových řízení v souladu se smlouvou. Konečně, bude projednán a odsouhlasen proces pro schvalování dokumentů a výstupů. K vytvoření bude použito technik Ganttova diagramu, metodiky projektového managementu společnosti T-Mobile, metodiky WBS (Work Breakdown Structure).

Schválený řídící výbor bude dalším z výstupů, který vznikne podle nominací ze strany Uchazeče a Objednatele zakázky.

V rámci plnění úkolů jednotlivých služeb uchazeč sestaví komunikační matici pro řídící role a pracovní skupiny. V této oblasti očekáváme od Objednatele maximální součinnost tak abychom získali kontaktní spojení do všech lokalit (GSM, pevná linka, fax, email, poštovní adresa). Pro potřeby této zakázky vyčlení naše společnost servisní číslo, emailový box, fax pro účely projektového dispečinku *(Service Desk, Help Desk, Info Box)* na zaznamenávání splněných úkolů a případných nedostatků, poruch, závad, popřípadě nehod, pracovních úrazů apod. souvisejících s plněním předmětu zakázky. Zde budou poskytování Objednateli všechny informace o konkrétních činnostech v rámci plnění harmonogramu zakázky dle náplně jednotlivých etap, o konkrétní přítomnosti členů našich pracovních skupin v prostředí zákazníka.

V rámci činnosti jednotlivých týmů v jednotlivých etapách, dle jednotlivých úkolů budeme ukládat a chránit informace, které získáme při činnostech spojených s předmětem této zakázky, povedeme záznamy co, kdy, kde a jak a od koho jsme informace, doklady nebo podklady získali. Provoz jednotlivých služeb bude probíhat podle bezpečnostních pravidel, politik a procedur Objednatele, aby byli ve shodě s bezpečným prováděním jednotlivých služeb.

Pro dosažení vysoké kvality tvorby dokumentace vyčleníme z našeho projektového týmu zkušené specialisty, kteří se podílejí jak na auditní činnosti v oblasti bezpečnosti informací a zavádění procesů systému řízení bezpečnosti informací do organizací státní správy ale i zkušené analytiky, procesní specialisty a tvůrce dokumentací, působící v rámci naší společnosti.

3 Popis služeb

Navržený způsob poskytování služeb řízení informační bezpečnosti

Přístup Poskytovatele k realizaci Informační bezpečnosti

Při poskytování služeb řízení informační bezpečnosti budou uplatňovány následující zásady:

- Veškeré výstupy budou v souladu s požadavky standardů řady ISO/IEC 27000 : 2013 a budou zpracovány způsobem, který vytvoří základní předoklady pro úspěšnou certifikaci dle ČSN ISO/IEC 27001:2014
- Navržené, schválené a následně implementované výstupy a závěry budou garantovat stanovené dlouhodobé cíle v Informační koncepci Objednatele a uvedené v bodě 3.1.2.1 Přílohy č. 1 Smlouvy o poskytování služeb.
- Veškeré výstupy budou použitelné pro naplnění požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a jeho avízovaných prováděcích předpisů, dostupných nebo již platných k datu zpracování těchto výstupů.
- Navrhovaná řešení musí být optimální a minimalistická – musí dosahovat maximálních výsledků s minimální zátěží zdrojů Objednatele.
- Bezpečnostní opatření, která jsou již zavedena a fungují, budou zachována.
- Zjistí se, která opatření chybí a stanoví se priorita zavádění těchto opatření.
- Respektuje se zavedená firemní kultura Objednatele.

V souladu s předmětem plnění Smlouvy, se jedná o dodávku klíčových služeb uvedených v Příloze č. 1 Smlouvy, vedené pod názvem „Katalog služeb a podmínky poskytování bezpečnostního dohledu“ jako:

Služba „BS01_Informační bezpečnost“:

a) Služby související s řízení bezpečnosti informací v souladu se zásadami pro Systém řízení bezpečnosti informací (ISMS) dle norem řady ČSN ISO/IEC 27000

Klíčové aktivity:

1. Definice procesů, zásad, politik a metodik ISMS;
2. Tvorba bezpečnostní dokumentace ISMS;
3. Řízení bezpečnostních incidentů.

Služba „BS02_Ochrana osobních údajů“:

b) Služby související s prováděním ochrany osobních údajů v souladu s požadavky zákona č. 101/2000 Sb., o ochraně osobních údajů

3.1 Služba „BS01_Informační bezpečnost“

3.1.1 Implementační plán systému řízení informační bezpečnosti

Tabulka 1: Implementace služby BS_01

Implementační plán - systému řízení informační bezpečnosti (SŘIB)			
Kód	**Aktivita**	**Očekávaný výstup**	**Termín plnění nebo důležitý milník projektu**
1.0	Vyhotovení finální verze Smlouvy, podpis Smlouvy	Podpis Smlouvy	
1.0.1	**Zahajovací schůzka pro ŘV SŘIB:** (prezentace projektových cílů, představení společnosti, projektového týmu, upřesnění harmonogramu plnění, požadavky na součinnost, představení osnovy projektových výstupů, způsob naplňování předmětu Smlouvy, nominace členů Objednatele do řídících a pracovních skupin)	**Prezentace**	Do 2 dnů od podpisu Smlouvy
1.1.0	**Naplňování aktivity BS01/01:** Definice procesů, zásad, politik a metodik ISMS**: Detailní Analýzu systému MS2014+**, platné Informační koncepce a Bezpečnostní politiky Objednatele a navazujících dokumentů EK, národní legislativy a dalších dokumentů relevantních pro prostředí MS2014+, vypracujeme: • **procesy bezpečnosti informací a řízení bezpečnosti informací**, které je nezbytné uplatnit a prosadit v rámci systému MS2014+; • **klíčové cíle a hlavní zásady bezpečnosti informací**, které budou navrženými procesy pokryty (Cíle ISMS MS2014+ budou zpracovány na období 4 let, přičemž cíle na 1. rok poskytování služeb budou rozpracovány detailně); • **upřesnění implementačního plánu vytvoření systému ISMS MS2014+**, který přehledným způsobem navrhne detailní harmonogram prací a služeb pro vytvoření Systému řízení bezpečnosti informací MS2014+ (ISMS MS2014+).	**Pracovní dokumentace aktivity BS01/01**	Max. do 2 měsíců od podpisu Smlouvy, (max. 40 MD)
1.1.1	Stanovení předběžného rozsahu systému řízení pro MS2014+, výstupem bude dokument **Rozsah ISMS MS2014+,** který bude v závěru této klíčové činnosti zpřesněn a finalizován v návaznosti na získané výsledky ostatních činností.	Pracovní dokumentace Analýzy rizik	5 MD
1.1.2	Provedení identifikace aktiv systému MS2014+ a identifikace vlastníků aktiv/informací. Výstupem bude **Registr aktiv MS2014+.**	Pracovní dokumentace Analýzy rizik	5 MD
1.1.3	Zpracování **Směrnice pro klasifikaci a řízení aktiv MS2014+** a následné provedení hodnocení aktiv podle této směrnice. Hodnocení aktiv bude spolu s registrem aktiv základními dokumenty pro provedení analýzy rizik.	Pracovní dokumentace Analýzy rizik	5 MD
1.1.4	Stanovení komplexních zásad pro provedení analýzy rizik prostředí MS2014+, výstupem bude **Směrnice pro hodnocení rizik MS2014+.**	Pracovní dokumentace Analýzy rizik	5 MD
1.1.5	Provedení analýzy rizik a zpracování jejích výsledků do dokumentu **Zpráva o hodnocení rizik MS2014+**.	Pracovní dokumentace Analýzy rizik	5 MD
1.1.6	V návaznosti na výsledky analýzy rizik budou vybrána opatření pro jejich minimalizaci, resp. eliminaci. Vybraná bezpečnostní opatření budou uvedena v **Prohlášení o aplikovatelnosti**. Spolu s tímto prohlášení budou vymezena zbytková rizika a ta zpracována v dokumentu **Souhlas s navrhovanými zbytkovými riziky**.	Pracovní dokumentace výstupy Analýzy rizik	5 MD

1.1.7	V návaznosti na předchozí činnosti a jejich výstupy bude zpracována **Bezpečnostní politika MS2014+** jako dokument, který formuluje základní strategie, cíle, postoje, role, zodpovědnosti a zásady týkající se činností spojených s informační bezpečností v systému MS2014+.	Pracovní dokumentace Bezpečnostní politiky	10 MD
1.1.8	**Provedení pracovního Workshopu k aktivitě BS01/01, BS02/02-03** **Předání výstupů aktivity BS01/01 a BS02/02-03 k akceptačnímu řízení**	Dokumentace aktivity BS01/01 a BS02/02-03	**Akceptační řízení** Max. do 2 měsíců od podpisu Smlouvy
1.2.0	**Naplňování aktivity BS01/02: Tvorba bezpečnostní dokumentace ISMS:** Navržený **Implementační plán vytvoření systému ISMS MS2014+** bude v návaznosti na výsledky předcházející klíčové činnosti obsahovat vytvoření detailní dokumentace systému ISMS MS2014+. Tato dokumentace bude zpracována v souladu se zásadami a procesy zakotvenými v základních dokumentech ISMS MS2014+: - Směrnice k řízení bezpečnosti informací MS2014+, - Směrnice k systému řízení dokumentace MS2014+, - Směrnice k bezpečnosti lidských zdrojů MS2014+, - Směrnice pro budování bezpečnostního povědomí MS2014+, - Směrnice fyzické bezpečnosti a bezpečnosti prostředí MS2014+, - Směrnice k bezpečnosti informačních a komunikačních technologií MS2014+, - Směrnice k řízení incidentů MS2014+, - Směrnice pro řízení kontinuity činností MS2014+, - Směrnice k zajištění shody s bezpečnostními požadavky v rámci MS2014+, - Plán zvládání rizik MS2014+, - Metodika k provádění interních auditů ISMS MS2014+, - Bezpečnostní směrnice pro činnost bezpečnostního správce MS2014+, - Bezpečnostní směrnice administrátora Prostředí a Infrastruktury serverovny, - Bezpečnostní směrnice uživatele MS2014+; - Zapracování požadavků z aktivity **BS02/02-03**. Součástí výše uvedených směrnic, metodik a plánů budou i veškeré relevantní a potřebné formuláře pro evidenci, hlášení, záznamy a další činnosti, vyplývající ze stanoveného rozsahu ISMS a potřebné pro fungování tohoto systému na denní bázi.	**Pracovní dokumentace aktivity BS01/02** **(Směrnice, šablony, pomůcky apod.)** **Paralelní aktivita s aktivitou BS02/02-03**	Max. do 2 měsíců od akceptace aktivity BS01/01 = max. 40 MD (max. 28 MD)
1.2.1	V návaznosti na Směrnici pro řízení kontinuity vypracuje Uchazeč kompletní **Havarijní plány systému MS2014+** a to v minimálně v následujícím rozsahu:	**Pracovní dokumentace aktivity BS01/02 –**	Max. 8 MD

	- plány pro zvládání krizových situací;
	- dílčí havarijní scénáře;
	- dispečerské povinnosti;
	- krizový tým:
	  o definice členů týmů a definice jejich kompetencí;
	  o postupy a dokumentace činností při zvládání krizových situací;
	- náhradní a dočasné řešení kontinuity služeb:
	  o definice zbytných a nezbytných služeb v návaznosti na klasifikaci aktiv;
	  o stanovení pravidel zajištění náhradního a dočasného provozu.
		Havarijní plán	

1.2.2	V rámci řešení havarijních plánů provede Uchazeč **posouzení Zálohovacího plánu a Plánu obnovy**, které budou zpracovány Uchazečem služeb Prostředí v rámci zadávacího řízení „Pořízení HW platformy a Infrastruktury serverovny pro MS2014+“. Výstupem posouzení bude **doporučení pro Provozovatele Aplikace MS2014+ a Uchazeče služeb Prostředí**, na jejichž základě uvedené subjekty dopracují dokument tak, aby byl v souladu s nastaveným systém ISMS MS2014+ a jeho postupy pro řízení kontinuity a havarijními plány.	Vypracování doporučení pro Objednatele a poskytovatele služeb	Max. 2 MD
1.2.3	**Předání výstupů aktivity BS01/02 k akceptačnímu řízení**	Dokumentace aktivity BS01/02	**Akceptační řízení** Max. do 2 měsíců od akceptace aktivity BS01/01
1.3.0	**Naplňování activity BS01/03: Zavedení systému řízení bezpečnostních incidentů** Poskytovatel bude na denní bázi provádět **řízení bezpečnostních incidentů systému MS2014+**. Detailní postupy a procesy řízení bezpečnostních incidentů budou vycházet ze schválené Směrnice k řízení incidentů MS2014+. Poskytovatel bude vůči Objednateli v oblasti řízení bezpečnostních incidentů primární odpovědnou osobou za řešení bezpečnostně relevantních incidentů, událostí a slabin MS2014+. Uchazeč v rámci této Služby bude využívat formuláře pro hlášení a řešení bezpečnostních incidentů a událostí MS2014+ (zpracované v rámci dokumentace ISMS) a bude vykonávat veškeré relevantní činnosti vyplývající ze stanovených odpovědností a postupů reakce na incidenty, shromažďování důkazů a ponaučení se z těchto incidentů. Pro řešení bezpečnostních incidentů bude Uchazeči zajištěn přístup na ServiceDesk MS2014+ v potřebném rozsahu.	Implementace Směrnice k řízení incidentů MS2014+ do provozu, implementace SLA a procesů parametrů pro vyhodnocování incidentů	Max. do 2 měsíců od akceptace aktivity BS01/01 Max. 2 MD
1.3.1	**Společný pracovní Workshop k aktivitám BS01/02 a BS01/03** **Předání výstupů aktivity BS01/02 a 03 k akceptačnímu řízení**	Výstupní dokumentace, nastavení aktivit denního monitoringu práce s incidenty, nastavení SLA pro práci s incidenty	**Akceptační řízení** Max. do 2 měsíců od akceptace aktivity BS01/01

1.3.2	**BS01/04: Nastavení pravidelného systému vyhodnocování služby:** O poskytnutí všech služeb bude připraven ze strany Uchazeče tzv. "**Protokol o poskytnuté službě**" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující: - Výkaz činností v rámci ISMS - Výkaz stavu bezpečnostní dokumentace s přehledem platné a akceptované dokumentace ISMS - Výkaz za oblast bezpečnostních incidentů s detailním popisem stavu a problému při šetření jednotlivých incidentů.	Pravidelný reporting	1 x za měsíc za uplynulé období, denní monitoring služby 08.00 -16.00
1.3.3	Nastavení systému pravidelné kontroly a úpravy dokumentace: Uchazeč zároveň zajistí pravidelnou **aktualizaci celé dokumentační základny ISMS MS2014+** a to s periodou 1x za 6 měsíců. V rámci aktualizace budou zapracovávány zejména dílčí změny v prováděcích postupech a bezpečnostních mechanismech v návaznosti na běžné změny provozního Prostředí a Aplikace MS2014+. Perioda aktualizace dokumentace je shodná s prováděním Interního auditu ISMS MS2014+ tak, aby bylo možné výsledky interních auditů promítnout v rámci aktualizace dokumentační základny.	1x za 6 měsíců	Perioda aktualizace dokumentace je shodná s prováděním Interního auditu ISMS MS2014+

3.1.2 Procesy a postupy při realizaci služby

3.1.2.1 Zpracování dokumentu Slovník základních pojmů a definic

Vzhledem k faktu, že v oblasti bezpečnosti není zavedená jednotná terminologie, navrhujeme v první řadě zpracování "Slovníku základních pojmů a definic", vycházejícíz následujících zdrojů:

1. Z ustálené české terminologie používané v oblasti informační bezpečnosti publikované v normách řady ČSN/ISO 27000, zejména v samotné ČSN/ISO 27001:2014.
2. Z „Výkladového slovníku kybernetické bezpečnosti"oficiálně uveřejněného na stránkách NBÚ.
3. Z důležitých pojmů, které budou používány ve všech výstupech, a proto bude nezbytné je definovat a udržovat i v období užívání výstupů vytvořených v rámci projektu.

3.1.2.2 Stanovení kontextu systému, hranic a rozsahu ISMS

Při stanovení kontextu systému se vychází z pochopení jeho činnosti. Provede se obecný rozbor činností, které system zajišťuje a provádí, stanoví se hlavní procesy, které jsou v rámci systému vykonávány a jejich důležitost se ohodnotí.

Následně se stanoví předpokládaná očekávání třetích stran. Třetími stranami jsou na jedné straně stát, který od systému očekává plnění stanovených funkcí a stanovuje své požadavky formou zákonných a podzákonných norem a na druhé straně uživatelé systému a další subjekty, kteří předpokládají, že s informacemi, které jsou v systému zpracovávány, se bude zacházet v mezích právních předpisů a nebude docházet k jejich úniku k neoprávněným subjektům.

Očekávání třetích stran se stanovuje tak, že se k identifikovaným procesům stanoví předpisy a zákonné normy se vztahem k bezpečnosti informací a stanoví se rizika, kterým se organizace nedržením těchto předpisů může vystavit. Tyto informace se doplní formou pohovoru se zástupci každého významného organizačního celku zajišťujícího provoz a správu systému.

Na základě **vyhodnocení kontextu a očekávání třetích stran se stanoví hranice a rozsah systému řízení bezpečnosti informací**, který mimo prvních dvou kroků obsahuje také identifikaci bezpečnostních dopadů významných vazeb mezi aktivitami organizace a jejím okolím. Celý kontext systému se prodiskutuje a nechá schválit vedením Objednatele.

Výstupem je schválený dokument " Rozsah ISMS MS 2014+".

3.1.2.3 Způsob realizace analýzy rizik

Námi navržený metodický koncept analýzy rizik nejenom plně odpovídá požadavkům normy ČSN ISO/IEC 27001 – Systémy managementu bezpečnosti informací a ČSN ISO/IEC 27005 – Řízení rizik bezpečnosti informací, ale dle našich letitých zkušeností a na základě řady realizací i požadavkům zákazníků s ohledem na jeho transparentnost, srozumitelnost a nekomplikovanou aplikovatelnost.

Metodický rozsah pro analýzu rizik vyplývá ze zadání a týká se fyzického perimetru, který je daný lokalitami Objednatele pro DC1, DC2 a logickým perimetrem, který zahrnuje procesy a informační systémy provozované v příslušných lokalitách (fyzickém perimetru).

Cílem je získání reálného obrazu o stavu bezpečnosti informací a kvalitních podkladů pro rozhodování jak zabezpečit bezpečnost informací návrhem protiopatření.

Cílem návrhu opatření pro zvládání rizik jsou jasně definována opatření na pokrytí rizik a připravena akceptace zbytkových rizik.

Cílem analýzy rizik je zjistit neakceptovatelná rizika, která hrozí aktivům organizace a tak získat podklad pro návrh opatření na snížení těchto rizik na akceptovatelnou úroveň a to za ospravedlnitelnou cenu (cena na realizaci opatření musí být v „rozumném“ poměru k hodnotě a významu chráněného aktiva).

3.1.2.4 Analýza rizik - popis metodiky

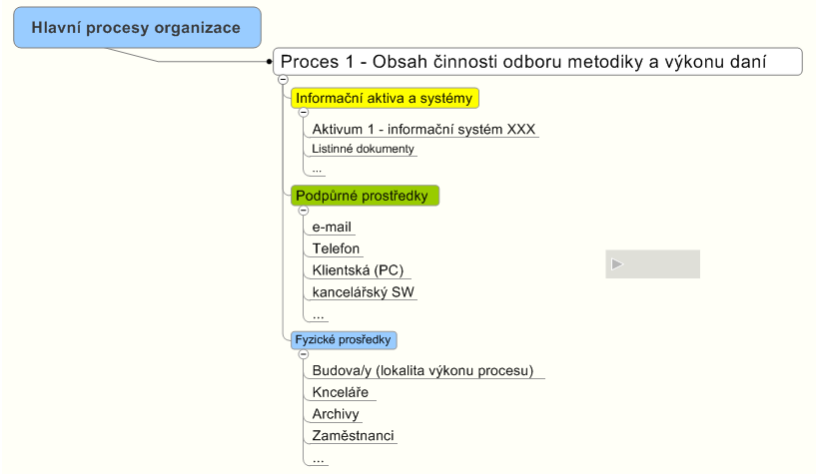
Metoda analýzy rizik používaná uchazečem striktně vychází z podstaty ISMS, která spočívá v podpoře činnosti organizace prostřednictvím zajištění přiměřené bezpečnosti jejích informací.

Analýza rizik probíhá v následujících krocích:

1. Identifikace, ohodnocení a seskupení aktiv.
2. Ohodnocení hrozeb, dopadů a zranitelností.
3. Výpočet rizik a stanovení akceptovatelné úrovně rizika.
4. Výpočet účinnosti opatření.
5. Sdružení výsledků jednotlivých analýz a sestavení výsledné sady opatření a její ověření modelováním.
6. Schválení výsledků analýzy rizik vedením organizace.

3.1.2.5 Identifikace, ohodnocení a seskupení aktiv

Identifikace a ohodnocení aktiv vychází z informací získaných při stanovování kontextu organizace a je založena zejména na procesním přístupu k hodnocené organizaci a systému. Po stanovení hlavních procesů, které organizace vykonává a systém zajišťuje, se k těmto procesům stanoví aktiva, které jsou k jejich vykonávání potřebná (viz obr. 1).



Obrázek 1: Stanovení aktiv k procesům

V rámci sběru informací se aktiva a prostředky ohodnotí z hlediska jejich důležitosti pro vykonávání daného procesu a z hlediska požadavku na důvěrnost, integritu a dostupnost zpracovávaných informací.

Následně se takto shromážděná aktiva promítnou na ICT prostředky organizace a systému (servery, síťové prvky atd.). Tím se získá přehled o tom, který prostředek ICT podporuje který proces, a které

Obrázek 2: Příklad typického rozložení parciálních rizik

aktivum. Od informací o důležitosti procesu, o důležitosti aktiva, o požadavcích na důvěrnost, integritu a dostupnost zpracovávaných informací se odvodí bezpečnostní vlastnosti jednotlivých prostředků ICT i jednotlivých aktiv.

Jelikož několik procesů může využívat stejná aktiva (např. server) tato aktiva se seskupí do tzv. „typových aktiv". Ke každému typovému aktivu se stanoví „vlastník aktiva" (osoba, která má o aktivu nejlepší přehled a je schopna hodnotit působení jednotlivých hrozeb).

Výstupem bude schválený dokument "Registr aktiv MS 2014+" a "Registr typových aktiv MS 2014+"

3.1.2.6 Klasifikace a řízení aktiv

Identifikovaná aktiva je nutné klasifikovat na základě jejich potřebnosti a důležitosti pro zabezpečení činnosti systému a Objednatele. Důležité informace Objednatele budou evidovány v rámci ISMS a bude stanovena odpovědnost za jejich správu.

Výstupem bude schválený dokument "Směrnice pro klasifikaci a řízení aktiv MS 2014+".

3.1.2.7 Ohodnocení hrozeb, dopadů hrozeb a zranitelností

Metoda pracuje se seznamem hrozeb podle standardu ISO/IEC 27005. Ohodnocení intenzity hrozeb, dopadů hrozeb a zranitelnosti aktiva vůči jednotlivým hrozbám se provádí formou řízených pohovorů s vlastníkem příslušného aktiva. Pro provádění pohovorů se používají vygenerované formuláře.

3.1.2.8 Výpočet rizik a stanovení akceptovatelné úrovně rizika

Výpočet hodnoty rizika se provádí pro každé aktivum a každou hrozbu. Riziko vzniklé působením jedné konkrétní hrozby na jedno konkrétní aktivum se nazývá ***„parciální riziko"***. Parciální rizika se vypočítají podle vzorce:

Parciální riziko = Hrozba * Dopad hrozby * Zranitelnost aktiva * Hodnota aktiva

Příklad typického rozložení parciálních rizik je uveden na obrázku č. 2. Červená šipka na obrázku označuje úroveň akceptovatelného rizika, pod kterou se při výběru opatření nebudou brát menší hrozby v potaz. **Úroveň akceptovatelného rizika se stanovuje po dohodě Objednatelem, který ji schvaluje.** Metoda umožňuje brát v potaz všechna parciální rizika.

Výstupem bude schválený dokument "Směrnice pro hodnocení rizik MS 2014+".

3.1.2.9 Hodnocení hrozeb a zranitelností

Výpočet rizik může být použit i k identifikaci zranitelných míst v organizaci. U největších parciálních rizik identifikují aktiva, kterých se riziko týká a hrozby, které riziko způsobují. Toto hodnocení poskytne informaci o tom, která aktiva (které části systému) jsou nejvíce ohrožena a které hrozby toto ohrožení nejvíce způsobují.

Stanovení slabých míst v systému a závažných hrozeb je jedním z dílčích výstupů z analýzy rizik, který se schvaluje Objednatelem a slouží k verifikaci výsledků analýzy rizik.

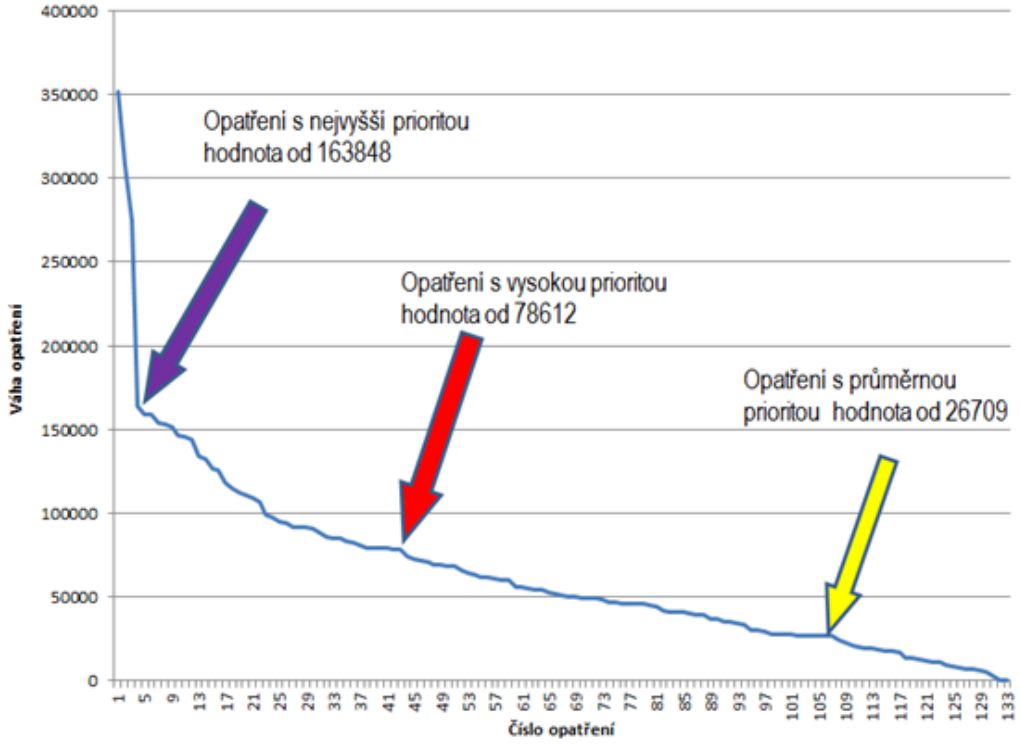
3.1.2.10 Stanovení účinnosti opatření

Metoda analýzy rizik byla vyvinuta pro podporu zavádění ISMS, proto sada opatření pro snížení rizika je totožná s opatřeními uvedenými v příloze „A" standardu ISO 27001:2013 (dále také „opatření ISMS").

Pro každé aktivum se zpracuje „***list aktiva***“, na kterém se hodnotí účinnost každého opatření ISMS ke snížení každého parciálního rizika (v metodice se nazývá jako „***váha opatření***“). Metoda vyhodnocuje pro každé parciální riziko účinnost všech 114 opatření ISMS tak, že pro každé parciální riziko a opatření vypočte ***dílčí váhu opatření***. Váha opatření pro každé aktivum je součtem všech dílčích vah, které jsou pro dané opatření u všech parciálních rizik vypočtena.

Po provedení výpočtů na všech listech aktiv je pro každé opatření ISMS stanovena jeho celková váha, která vyjadřuje účinnost opatření v rámci všech aktiv organizace.

Setřídíme-li sestupně opatření podle jejich váhy a vyneseme-li je do grafu, získáme rozložení opatření podle jejich účinnosti, která určuje prioritu implementace. Opatření, která mají nejvyšší váhu, mají také největší přínos pro bezpečnost organizace a systému a tím i nejvyšší prioritu pro implementaci. Příklad typického rozložení vah opatření je uveden na obrázku č. 3, který představuje reálnou analýzu rizik, provedenou u jednoho ze zákazníků Uchazeče.



Z grafu je zřejmá jedna výrazná úroveň vah opatření

Obrázek 3: Rozložení opatření dle jejich váhy

Opatření nad fialovou šipkou mají mimořádný přínos pro bezpečnost organizace a systému, zatímco váhy ostatních opatření víceméně lineárně klesají. To umožní rozdělit opatření do skupin (podle šipek, od opatření s nejvyšší prioritou (měla by se realizovat co nejdříve), až po opatření (pod žlutou šipkou), která znamenají již jen minimální přínos pro bezpečnost, a mohou se realizovat někdy v budoucnosti, pokud pro to vzniknou vhodné podmínky.

3.1.2.11 Sdružení výsledků jednotlivých analýz a sestavení výsledné sady opatření a její ověření modelováním

V rámci realizace tohoto kroku se sejdou všechny sady opatření a pro každé opatření se vypočítají vážené průměry vah opatření a sestaví se výsledná sada opatření doporučovaných k realizaci, která

bude jednotná pro organizaci a systém. Při sestavování výsledné sady opatření Uchazeč vezme v úvahu možnosti a podmínky Objednatele a navrhne optimální sadu opatření.

Následně se provede modelování účinnosti takto vybrané sady opatření. Modelování umožňuje vypočíst, na jakou hodnotu se sníží parciální rizika po realizaci vybraných opatření (tato rizika se nazývají „***zbytková rizika***“, protože to jsou rizika, která zbydou po realizaci vybraných opatření).

Pokud bude některé zbytkové riziko příliš vysoké, doplní se univerzální sada opatření o další opatření tak, aby bylo toto zbytkové riziko sníženo na přijatelnou úroveň. **Přehled zbytkových rizik je konzultován a následně schválen Objednatelem.**

Výstupem bude schválený dokument “Souhlas s navrhovanými zbytkovými riziky”.

3.1.2.12 Schválení výsledků analýzy rizik vedením organizace

Výsledky analýzy rizik jsou presentovány managementu Objednatele, kterému jsou vysvětlena rizika, zdůvodněna opatření, které analýza rizik doporučuje implementovat, a jsou mu objasněna zbytková rizika. Následně je management Objednatele žádán o schválení výsledků analýzy rizik.

Výstupem bude schválený dokument “Zpráva o hodnocení rizik MS 2014+”.

Schválená finální sada bezpečnostních opatření je podkladem pro zpracování návrhu základního dokumentu ISMS – ***Prohlášení o aplikovatelnosti***, který je jedním z podkladů pro tvorbu registru organizačních požadavků.

Výstupem bude schválený dokument “Návrh Prohlášení o aplikovatelnosti MS 2014+”

3.1.2.13 Registr zákonných požadavků

Registr zákonných požadavků vznikne analýzou platných právních a interních předpisů majících vazbu na bezpečnost informací. V rámci této analýzy budou identifikovány všechny požadavky se vztahem k bezpečnosti informací, vyplývající ze zákonů, podzákonných norem a interních předpisů Objednatele. Tyto požadavky budou logicky strukturovány podle povinností, které ukládají s odkazem na právní předpis, nebo interní normativní akt (dále jen INA).

Základem pro vytvoření komplexního registru všech požadavků na bezpečnost informací je vytvoření registru zákonných požadavků, který vychází z platných zákonů ČR. Tento registr obsahuje většinu podstatných zákonných požadavků na bezpečnost informací pro Objednatele, včetně všech právních norem uvedených Objednatelem v Příloze č. 1 Smlouvy. V případě, že v průběhu realizace projetu bude Objednatelem konstatováno, že se na něj a na systém vztahuje zákon č. 181/2014 o kybernetické bezpečnosti, bude tento zákon zahrnut taktéž do registru zákonných požadavků.

Dalším krokem je vytvoření registru interních požadavků vyplývajících z platných interních předpisů Objednatele.

Požadavky z obou registrů musí být porovnány s výsledky analýzy rizik, ve které musí být doplněna chybějící opatření, jejichž realizace vyplývá ze zákonných požadavků, nebo z interních předpisů. Protože se jedná o vyhledávání mezer v požadavcích analýzy rizik (anglicky je mezera „gap“) nazývá se tento proces „GAP analýza“, která je podrobněji rozebrána v bodě 1.2.1.16 nabídky.

Příklad registru zákonných požadavků je uveden v následující tabulce

Číslo	Název	Charakteristika
101/2000 Sb.	Zákon o ochraně osobních údajů	Upravuje práva a povinnosti při zpracování osobních údajů a stanovuje podmínky, za nichž se uskutečňuje předání osobních údajů.
106/1999 Sb.	Zákon o svobodném přístupu k informacím	Upravuje podmínky práva svobodného přístupu k informacím a stanovuje základní podmínky, za nichž jsou informace poskytovány.
127/2005 Sb.	Zákon o elektronických komunikacích	Tento zákon upravuje na základě práva Evropských společenství podmínky podnikání a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací.

Tabulka 2 Přehled zákonných požadavků

Každý zákon uvedený v registru zákonných požadavků je dále podrobněji rozpracován do podoby uvedené v následující tabulce

Tabulka 3: Zákonná úprava požadavků

Typ normy	Číslo	Název	Účinný	Charakteristika (co řeší)
Zákon	101/2000 Sb.	o ochraně osobních údajů	1.6.2000	Tento zákon v souladu s právem Evropských společenství, mezinárodními smlouvami, kterými je Česká republika vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.

Tabulka 4: Podrobný přehled zákonných požadavků pro konkrétní zákonnou normu

Role	Požadavek	Vyplývá z	Možná sankce
Správce, Zpracovatel	Stanovit účel, k němuž mají být osobní údaje zpracovány.	§ 5/1a	až 10.000.000,- Kč
Správce, Zpracovatel	Stanovit prostředky a způsob zpracování osobních údajů.	§ 5/1b	až 10.000.000,- Kč
Správce, Zpracovatel	Zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje. Nepřesné osobní údaje lze zpracovat pouze v mezích uvedených v § 3 odst. 6. Nepřesné osobní údaje se musí označit. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem příjemcům.	§ 5/1c	až 10.000.000,- Kč
Správce, Zpracovatel	Shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu.	§ 5/1d	až 10.000.000,- Kč
Správce, Zpracovatel	Uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné.	§ 5/1e	až 10.000.000,- Kč
Správce, Zpracovatel	Zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6, nebo	§ 5/1f	až 10.000.000,- Kč

Role	Požadavek	Vyplývá z	Možná sankce
	pokud k tomu dal subjekt údajů předem souhlas.		
Správce, Zpracovatel	Shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti.	§ 5/1g	až 10.000.000,- Kč

3.1.2.14 Zakomponování registru zákonných požadavků do sady vybraných opatření z analýzy rizik a definice registru organizačních požadavků

Požadavky na systém řízení bezpečnosti jsou dány dvěma faktory:

- Požadavky stojící mimo systém řízení bezpečnosti informací, které jsou dány platnými právními a prováděcími předpisy (registr zákonných požadavků) a platnými interními předpisy Objednatele (registr interních požadavků).
- Požadavky, které vyplynuly z analýzy rizik, které definují systém řízení bezpečnosti.

Sjednocení obou množin požadavků definuje úplnou množinu požadavků na realizaci bezpečnostních opatření, tím je definován cílový stav, kterého se má dosáhnout.

3.1.2.15 Požadovaná opatření ISMS

Seznam požadovaných opatření ISMS je dán výstupem z analýzy rizik v podobě návrhu „Prohlášení o aplikovatelnosti“.

Ukázka prohlášení o aplikovatelnosti je uvedena v tabulce č. 3

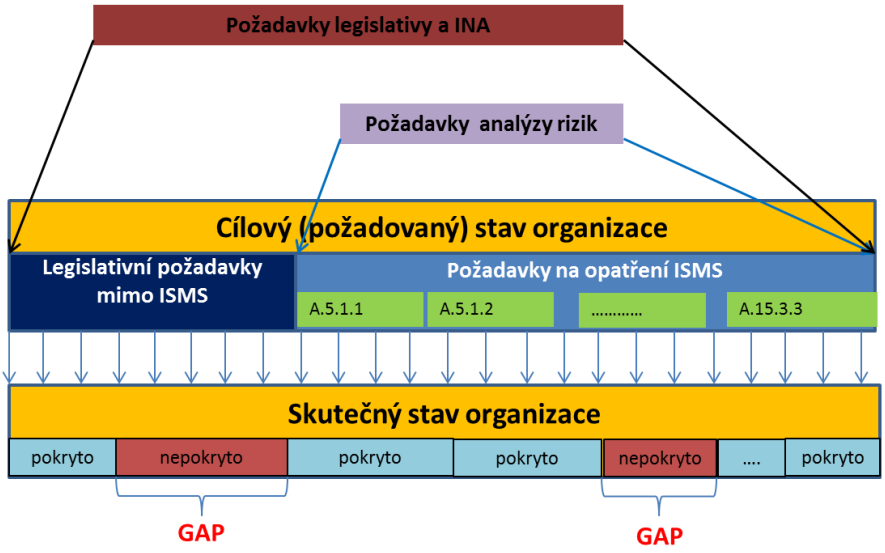
Tabulka 5: Příklad prohlášení o aplikovatelnosti (PoA)

PoA - Přehled vybraných a vyřazených cílů a opatření			
Číslo opatření	**Název**	**Popis opatření**	**Stav opatření**
A. 5	Bezpečnostní politika		**Jméno oblasti**
A. 5.1	Bezpečnostní politika informací	Cíl: Definovat směr a vyjádřit podporu bezpečnosti informaci ze strany vedení v souladu s požadavky organice, příslušnými zákony a regulatorními požadavky.	**Bzpečnostní cíl**
A. 5.1.1	Dokument bezpečnostní politiky informací	Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, vydán a být dán na vědomí všem zaměstnancům a relevantním třetím stranám.	**Opatření má být implementováno**
A. 5.1.2	Přezkoumání a aktualizace bezpečnostní politiky informací	Pro zajištění její neustálé použitelnosti, přiměřenosti a účinnosti by bezpečnostní politika informací měla být přezkou mávána v plánovaných intervalech a vždy když	**Opatření má být implementováno**

3.1.2.16 GAP analýza

Cílový stav bezpečnosti informací je dán sadou bezpečnostních opatření, které jsou dány analýzou rizik a zákonnými požadavky. Jelikož lze předpokládat, že určitá bezpečnostní opatření již jsou u Objednatele implementována, je nutné zjistit rozdíl mezi požadovaným stavem a stávajícím stavem bezpečnosti informací. K tomu slouží „Gap“ analýza, jejímž cílem je porovnat již zavedená bezpečnostní opatření s požadovaným stavem z analýzy rizik. Gap analýza bude provedena tak, že budou identifikovány všechny zavedené a provozované bezpečnostní opatření u organizace a ty budou porovnány s požadovaným stavem. Následně budou identifikovány všechny mezery („gap“ = anglicky mezera) mezi stávajícím stavem a požadovaným stavem.

Na obrázku č. 4 je znázorněno, jak jsou z GAP analýzy identifikovány oblasti, o které je potřeba doplnit bezpečnostní dokumentaci organizace.



Obrázek 4: GAP analýza

V rámci GAP analýzy se provede podrobná analýza stávající dokumentace s cílem zpřesnit, které stati a ustanovení jednotlivých dokumentů mají vztah ke kterým požadavkům definice cílového stavu. Hodnocení realizace požadavků bude provedeno ve třech úrovních:

- je dobře popsáno,
- je popsáno částečně – musí se dopracovat,
- není popsáno, ale provádí se (zvykově),
- chybí.

Vznikne tak registr organizačních požadavků umožňující snadnou orientaci v tom, co je potřeba na stávajícím systému řízení bezpečnosti informací doplnit. Chybějící části se převedou do standardního schématu dokumentů používaných v řízení bezpečnosti informací.

3.1.2.17 Prezentace závěrů a schválení finálního PoA (Prohlášení o aplikovatelnosti).

Na základě analýzy rizik a GAP analýzy byl stanoven finální soubor opatření z přílohy „A“ standardu ČSN ISO/IEC 27001, která budou v hranicích ISMS realizována. Vedení Objednatele se schválením tohoto dokumentu zavazuje k jeho naplnění a implementaci všech vybraných opatření.

Vzor finálního návrhu Prohlášení o aplikovatelnosti je uvedeno v tabulce č. 4.

Tabulka 6: Prohlášení o aplikovatelnosti

Kód opatření	Název opatření	Výběr opatření na základě analýzy rizik a GAP analýzy
A. 5.1.1	Dokument bezpečnostní politiky informací	opatření bylo vybráno
A. 5.1.2	Přezkoumání a aktualizace bezpečnostní politiky informací	opatření bylo vybráno
A. 6.1.1	Závazek vedení	opatření bylo vybráno
A. 6.1.2	Koordinace bezpečnosti informací	opatření bylo vybráno
A. 6.1.3	Přidělení odpovědností v oblasti bezpečnosti informací	opatření bylo vybráno
A. 6.1.4	Schvalovací proces prostředků pro zpracování informací	Nevybráno přehodnotit při přezkoumání ISMS

Kód opatření	Název opatření	Výběr opatření na základě analýzy rizik a GAP analýzy
A. 6.1.5	Dohody o ochraně důvěrných informací	opatření bylo vybráno
A. 6.1.6	Kontakt s orgány veřejné správy	Nebylo vybráno
A. 6.1.7	Kontakt se zájmovými skupinami	Nebylo vybráno
A. 6.1.8	Nezávislá přezkoumání bezpečnosti informací	Nebylo vybráno

Výstupem bude schválený finální dokument "Prohlášení o aplikovatelnosti MS 2014+".

3.1.2.18 Sestavení a schválení plánu zvládání rizik

Účelem plánu zvládání rizik je zkonkretizovat postup zavedení vybraných opatření PoA, včetně stanovení termínů a odpovědných osob, která jsou aplikována v systému řízení informační bezpečnosti a uvedení opatření, která jsou tímto plánem redukována.

Vzor plánu zvládání rizik je uveden v tabulce č. 5

Tabulka 7: Plán zvládání rizik

Opatření	Realizace opatření (pozn.)	Uvedeno v dokumentaci	Odpovědnost a zdroje	Datum zavedení
A. 5.1.2	Přezkoumání a aktualizace bezpečnostní politiky informací	Bezpečnostní politika informací	Předseda bezpečnostního výboru	Do 12 měsíců od účinnosti Bezpečnostní politiky informací

Výstupem bude schválený dokument "Plán zvládání rizik MS 2014+".

3.1.2.19 Bezpečnostní politika MS2014+

V rámci tohoto bodu bude vypracován obecný dokument, formulující základní strategie, cíle, postoje, role, zodpovědnosti a zásady týkající činností se spojených s Informační bezpečností v systému MS2014+.

Dokument má deklarační charakter a bude dále podrobně rozpracován do dokumentů uvedených v bodě "3.1.4 Bezpečnostní dokumentace ISMS."

3.1.2.20 Návrh řídící struktury (výboru) pro ISMS MS2014+

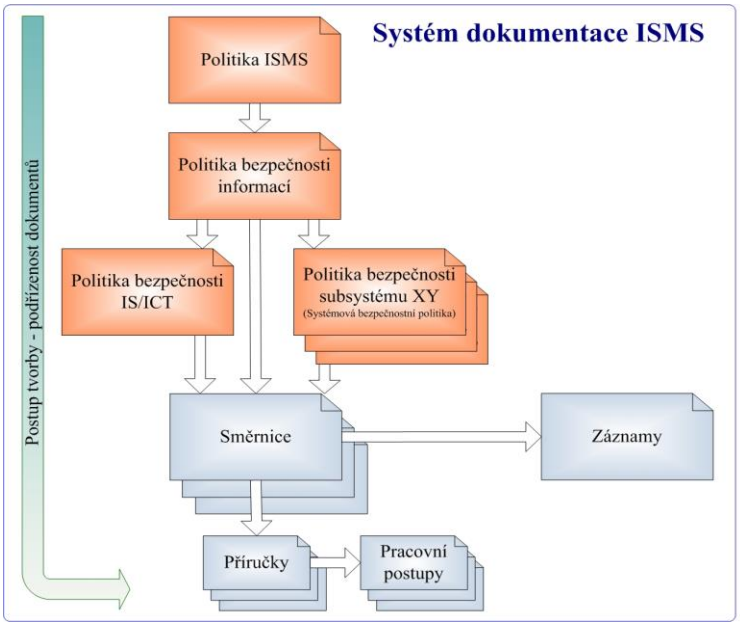
Bude navržena řídící struktura pro ISMS MS 2014, podrobně popsaná v bodě. 3.1.6

Uchazeč provede výše uvedené činnosti a předá stanovené dokumenty ke schválení Objednateli do 2 kalendářních měsíců od data účinnosti této Smlouvy.

3.1.3 Tvorba bezpečnostní dokumentace ISMS

V rámci návrhu dokumentace bude využita nejenom norma ČSN ISO/IEC 27001 – Systémy managementu bezpečnosti informací, ale i ČSN EN ISO 9001 – Systémy managementu kvality, která uvádí základní požadavky nejlepší praxe pro celou řadu norem ISO. Dále budou respektovány interní požadavky a zvyklosti pro vydávání předpisů.

Celý systém dokumentace bude navržený jako centrální (s centrálním řízením a správou). Jednotlivé lokality budou svá specifika řešit formou záznamů k této centrální dokumentaci, tím se celý systém stane konzistentním a snadno spravovatelnýma udržovatelným v souladu s požadavky Přílohy č. 1 Smlouvy.



Obrázek 5: Systém dokumentace ISMS

Postup tvorby dokumentů - od politiky ISMS k řídícím a podpůrným dokumentům a záznamům je znázorněn na následujícím schématu.
V modelu dokumentace bezpečnosti informací ISMS jsou definovány 3 kategorie dokumentů:

- řídící dokumenty
- záznamy
- podpůrné dokumenty

Řídící dokumenty ISMS jsou členěny z hlediska obecnosti (detailnosti) popisu řešené oblasti ISMS do 4 typů:

- politika
- směrnice
- příručka
- pracovní postup

Bezpečnostní dokumentace bude mít jednotnou formu vyplývající ze zpracovaných šablon, které budou součástí upřesnění s Objednatelem, v rámci plnění projektových úloh a požadadavků organizace.

3.1.4 Specifikace modulů dokumentace ISMS

Politika ISMS - prohlášení vedení organizace je koordinovaný soubor cílů, rámce zásad a hlavního směru chování organizace při řízení bezpečnosti informací.

Politika bezpečnosti informací je koordinovaný soubor cílů a opatření uplatňujících stanovené principy, který vede k zajištění požadovaného stupně ochrany informačních a souvisejících aktiv organizace.

Politika bezpečnosti IS/ICT je koordinovaný soubor cílů a opatření uplatňujících stanovené principy, který vede k zajištění požadovaného stupně ochrany IS/ICT.

Politika bezpečnosti subsystému je koordinovaný soubor cílů a opatření uplatňujících stanovené principy, který vede k zajištění požadovaného stupně ochrany významných informačních subsystémů a souvisejících aktiv organizace. Může se například jednat o Politiku bezpečnosti IS/ICT, nebo Bezpečnostní politiku platebního sytému apod. Tyto politiky většinou vznikají mimo vlastní dokumentaci bezpečnosti informací (většinou ji zpracovávají dodavatelé subsystémů), ale po jejich vzniku se do systému zařazují.

Tato politika také musí být schválena vedením a zpravidla se s ní seznamuje jen omezený okruh pracovníků, protože řeší jen zcela specifickou část systému opatření ke zvládání rizik.
Směrnice ISMS (pravidla pro řízení) je soubor nařízení, opatření a postupů vydávaných pro vykonávání procesů jednotlivých oblastí ISMS.

Dle důležitosti, kterou organizace přikládá jednotlivým oblastem, se zpracovávají vlastní směrnice, které na rozdíl od politiky bezpečnosti informací rozpracovávají příslušnou oblast do větší podrobnosti.

Jedná se o tyto oblasti:

- Organizace bezpečnosti informací;
- Řízení aktiv;
- Hodnocení a zvládání rizik;
- Personální bezpečnost;

- Fyzická bezpečnost a bezpečnost prostředí;
- Řízení komunikací a provozu;
- Řízení přístupu k informačnímu systému;
- Sběr dat, vývoj a údržba informačních systémů;
- Řízení incidentů informační bezpečnosti;
- Řízení kontinuity činností;
- Soulad s požadavky.

Příručka je výpisem ze směrnic ISMS pro jednotlivé role. Je to praktický návod k provádění sledu činností k dosažení požadovaného výsledku.

Pracovní postup je praktický návod k provádění posloupnosti úkonů jednotlivých činností krok za krokem. Pracovní postup se vytváří pro důležité, opakovatelné činnosti, u nichž je potřebná standardizace postupu.

Záznamy. Záznam dokládá soulad výkonu s pravidly. Je specifickou kategorií dokumentu, který vzniká jako výsledek realizace směrnice ISMS. Jednotlivé záznamy jsou většinou definované ve směrnicích.

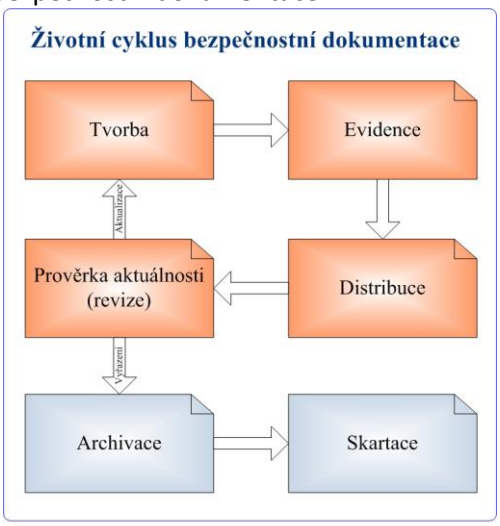
Podpůrné dokumenty. Podpůrné dokumenty jsou všechny ostatní dokumenty, které je vhodné mít k dispozici. Nemusí primárně vznikat v rámci bezpečnostní dokumentace, ale pro řízení bezpečnosti informací je účelné mít takovou dokumentaci. Jedná se například o popis informačního systému, popis zálohování apod. kdy tato dokumentace vzniká v rámci provozu IS/ICT a bezpečnostní dokumentace se na ni odkazuje.

Výstupem bude řízená dokumentace, která svým rozsahem a obsahem bude plně pokrývat požadavky Objednatele uvedené v Příloze č. 1 Smlouvy, v bodě 3.1.2.2.

3.1.5 Systém řízení bezpečnostní dokumentace

Systém řízení bezpečnostní dokumentace detailně popisuje

- Soustavu bezpečnostní dokumentace
- Životní cyklus dokumentů
- Řízení záznamů
- Organizační zajištění bezpečnostní dokumentace



Obrázek 6: Životní cyklus bezpečnostní dokumentace

V systému řízení dokumentace informační bezpečnosti probíhají 4 hlavní procesy:

- Tvorba (aktualizace);
- Evidence;
- Distribuce;
- Prověrka aktuálnosti;

a dva vedlejší procesy zrušení dokumentu

- Archivace (vyřazení);
- Likvidace (skartace).

3.1.6 Organizační zajištění bezpečnostní dokumentace

Role v systému řízení dokumentace. Rolí se chápe příslušná odpovědná osoba, bez ohledu na funkci (pozici) v organizační struktuře organizace a v systému informační bezpečnosti.

Tabulka 8: Role v systému řízení dokumentace

Pojmenování role	Popis role
Schvalovatel	Je pracovník oprávněný schválit dokument a na základě tohoto schválení je dokument vydán a je platný.
Vlastník dokumentu	Vlastník dokumentu je pracovník, do jehož působnosti (gesce) příslušný dokument náleží. Je odpovědný za zpracování a údržbu dokumentu a za jeho věcnou správnost.
Zpracovatel	Je pracovník odpovědný za zpracování návrhu a za provedení připomínkového řízení, pokud je požadováno.
Bezpečnostní manažer	Bezpečnostní manažer informačního systému organizace je role odborného vedoucího pracovníka pro informační bezpečnost, jehož hlavním úkolem je organizovat, řídit a zajišťovat odborné úkoly informační bezpečnosti.
Bezpečnostní správce	Bezpečnostní správce informačního systému je role odborného pracovníka pro informační bezpečnost, jehož hlavním úkolem je výkon odborných činností spojených s informační bezpečností
Správce dokumentu	Je pracovník odpovědný za evidenci a distribuci dokumentu v písemné i elektronické formě.

3.1.7 Tvorba

Tvorbou se rozumí nejen vytvoření nového dokumentu ale i novelizace (tvorba nové verze) dokumentu již existujícího. Tvorbu lze rozdělit na další podprocesy:

- plánování je zařazení do plánu, určení Zpracovatele, stanovení termínů, stanovení okruhu připomínkového řízení, kontrolu plnění plánu, toto provádí Vlastník dokumentu ve spolupráci se Správcem dokumentu,
- zpracování je příprava textu návrhu, toto provádí Zpracovatel pod dohledem Vlastníka dokumentu,
- připomínkové řízení je provedení připomínkového řízení a jeho vypořádání; toto provádí Zpracovatel a uzavírá,
- a vydání je finální kontrola dokumentu a jeho schválení, formální správnost odsouhlasí Zpracovatel, věcnou správnost Vlastník dokumentu, schválí Schvalovatel.

Uchazeč provede výše uvedené činnosti a předá stanovené dokumenty ke schválení Objednateli do 2 kalendářních měsíců od akceptace výstupů.

3.1.8 Havarijní plány systému MS2014+

V rámci přípravy a návrhu havarijního plánování bude nejdříve provedena analýza, která bude obsahovat:

1. Identifikaci činností/procesů/aktiv klíčové pro plnění cílů a poslání systému MS2014+.
   - ✓ Aktiva budou vycházet z Registru aktiv MS2014+
2. Ocenění dopadů v případě, že nejsou činnosti/procesy vykonávány, respektive když nejsou aktiva dostupná. Ocenění dopadů bude provedeno v závislosti na době, po kterou nejsou činnosti/procesy vykonávány, respektive kdy nejsou aktiva dostupná.
3. Stanovení časových rámců, ve kterých musí být na stanovenou minimální úroveň obnoveny činnosti/procesy respektive obnovena dostupnost aktiv (informačních i IKT).
4. Stanovení vzájemných závislostí a potřebných zdrojů pro vykonávání kritických činností/procesů a zajišťování dostupnosti kritických aktiv.

Na základě výstupů z této analýzy bude podrobně vypracována sada Havarijních plánů v rozsahu stanoveném Objednatelem v Příloze č. 1 Smlouvy bodě 3.1.2.2. Havarijní plány systému MS2014+.

3.1.8.1 Zálohovací plán a Plán obnovy

V rámci této činnosti bude Uchazečem v součinnosti s Poskytovatelem služeb Prostředí a s Provozovatelem Aplikace MS2014+ provedeno připomínkové řízení k Zálohovacímu plánu a Plánu obnovy, zpracované výše uvedenými subjekty.

Cílem bude dosažení stavu, který je v plném souladu s požadavky systému řízení bezpečnosti informací MS2014+ a současně zajišťuje provoz v souladu se stanovenými parametry SLA.

Výstupem bude optimalizovaný a aktualizovaný Zálohovací plán a Plán obnovy.

Havarijní plány a aktualizovaný Zálohovací plán a Plán obnovy budou předloženy Objednateli k akceptaci do 2 kalendářních měsíců od akceptace bezpečnostní dokumentace.

3.1.9 Aktualizace dokumentační základny ISMS MS2014+

Systém řízení bezpečnosti informací je nutné chápat jako velmi dynamický a komplexní proces, který ovlivňuje důvěrnost, integritu a dostupnost informačních aktiv v rámci celého systému MS2014+. Proto je nutné provádět pravidelnou supervizi zavedeného a zdokumentovaného systému s cílem reagovat na změny:

- V systému MS2014+ jako takovém (změny Aplikaci, Prostředí, organizační, dislokační, personální atd.);
- V platné a související legislativě

Na základě těchto změn je nutné vyhodnotit dopad změny a v případě potřeby provést změnová řízení.

Uchazeč bude provádět pravidelný monitoring legislativní základny uvedené v "Registru organizačních požadavků" a současně reagovat na zjištění prováděných Interních auditů.

Výstupem bude návrh potřebných změnových řízení v dokumentační základně ISMS MS 2014.

Uchazeč zajistí pravidelnou aktualizaci celé dokumentační základny ISMS MS2014+ a to s periodou 1x za 6 měsíců. V případě souvisejících změn v legislativní základně bude navrhovat změnová řízení neprodleně.

3.1.10 Přezkoumání rozsahu ISMS MS2014+

Jedenkrát ročně provede Uchazeč přezkoumání Rozsahu ISMS MS2014+ s důrazem na posouzení:

- Klíčové charakteristiky MS2014+,
- Procesy zahrnuté do ISMS MS2014+,
- Přehled informačních aktiv zahrnutých do ISMS MS2014+,
- Přehled lokalit zahrnutých do ISMS MS2014+,
- Role a odpovědnosti v rámci ISMS MS2014+,
- Zdůvodnění vyjmutí aktiv z rozsahu ISMS MS2014+

Výstupem přezkoumání bude aktualizovaný Rozsah ISMS MS 2014+ a vyhodnocení splnění cílů ISMS MS2014, včetně dalšího rozpracování dlouhodobých cílů do dalšího období.

3.1.11 Aktualizace Analýzy rizik

Při změně hranic nebo rozsahu ISMS bude vždy provedená potřebná aktualizace Analýzy rizik s cílem aktualizovat PoA a tím I celou dokumentační základnu ISMS MS 2014.

Jedenkrát ročně při změně rozsahu nebo hranic ISMS MS2014+.

3.1.12 Řízení bezpečnostních incidentů

Uchazeč bude provádět a plně zodpovídat za řízení bezpečnostních incidentů systému MS2014+. Na základě vyhodnocených bezpečnostních incident ů bude pro optimalizaci celého systému ISMS MS 2014 sestavena směrnice pro měření účinnosti.

3.1.13 Sestavení směrnice pro měření účinnosti

Tento dokument stanoví pracovní postup Uchazeče pro měření účinnosti vybraných opatření a jeho účelem je stanovit, jak jsou naplňovány požadavky na bezpečnost informací. Výsledkem je skóre vypočtené pro každé opatření, které udává, kolik problémů bylo pro dané opatření za dané období řešeno, a tím ukazuje na velikost odchylky od bezpečného stavu. Skóre by mělo sloužit jako vodítko pro výběr oblasti, které by mělo být v dalším období věnováno více pozornosti.

Vzor tabulky pro výpočet účinnosti opatření je uveden v tabulce č. 7.

Tabulka 9: tabulka pro výpočet a měření účinnosti opatření

Metrika pro měření účinnosti opatření

			Číslo dokumentu				Název dokumentu																							
							METRIKA PRO MĚŘENÍ ÚČINNOSTI OPATŘENÍ																							
			Číslo přílohy				Název přílohy																							
			1				Přehled neshod, incidentů a slabin ISMS																							
Opatření ISMS	Název	Váha opatření	Číslo neshody	Typ neshody	Opak.	Účinost opatření	Váha	po opatření	Číslo neshody	Typ neshody	Opak.	Účinost opatření	Váha	po opatření	Číslo neshody	Typ neshody	Opak.	Účinost opatření	Váha	po opatření	Číslo neshody	Typ neshody	Opak.	Účinost opatření	Váha	po opatření	Skore před opatře ním	Skore po opatře ní	Opatření ISMS
5.1.1	Dokument bezpečnostní politiky informací	76					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	5.1.1
5.1.2	Přezkoumání bezpečnostní politiky informací	36					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	5.1.2
6.1.1	Závazek vedení směrem k bezpečnosti informací	42					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.1.1
6.1.2	Koordinace bezpečnosti informací	17					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.1.2
6.1.3	Přidělení odpovědnosti v oblasti informační bezpečnosti	18					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.1.3
6.1.4	Schvalovací proces prostředků zpracování informací	0					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.1.4
6.1.5	Dohody o ochraně důvěrných informací	7					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.1.5
6.1.6	Kontakt s orgány veřejné správy	0					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.1.6
6.1.7	Kontakt se zájmovými skupinami	0					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.1.7
6.1.8	Nezávislá přezkoumání bezpečnosti informací	0					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.1.8
6.2.1	Identifikace rizik plynoucích z přístupu externích subjektů	27					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.2.1
6.2.2	Bezpečnostní požadavky pro přístup klientů	14					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.2.2
6.2.3	Bezpečnostní požadavky v dohodách se třetí stranou	12					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	6.2.3
7.1.1	Evidence aktiv	21					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	7.1.1
7.1.2	Vlastnictví aktiv	26					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	7.1.2
7.1.3	Přípustné použití aktiv	17					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	7.1.3
7.2.1	Doporučení pro klasifikaci	0					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	7.2.1
7.2.2	Označování a zacházení s informacemi	0					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	7.2.2
8.1.1	Role a odpovědnosti	13					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	8.1.1
8.1.2	Prověřování	0					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	8.1.2
8.1.3	Podmínky výkonu pracovní činnosti	9					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	8.1.3
8.2.1	Odpovědnosti vedoucích zaměstnanců	27					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	8.2.1
8.2.2	Informovanost, vzdělávání a školení v oblasti bezpečnosti informací	13					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	8.2.2
8.2.3	Disciplinární řízení	0					0,00	0,00					0,00	0,00					0,00	0,00					0,00	0,00	0,00	0,00	8.2.3

Pro řešení bezpečnostních incidentů bude Objednatelem Uchazeči zajištěn přístup na ServiceDesk MS2014+ v potřebném rozsahu.

3.1.14 Vyhodnocení služby

O poskytnutí všech služeb bude připraven ze strany Uchazeče tzv. "**Protokol o poskytnuté službě**" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující:

- Výkaz činností v rámci ISMS
- Výkaz stavu bezpečnostní dokumentace s přehledem platné a akceptované dokumentace ISMS
- Výkaz za oblast bezpečnostních incidentů s detailním popisem stavu a problému při šetření jednotlivých incidentů.

3.1.15 Požadavky na součinnost při realizaci

3.1.15.1 Součinnost Objednatele

Pro poskytování dané služby jsou jednotlivé požadavky na součinnost uvedeny v příslušných kapitolách výše, popisující způsob realizace služby.

3.1.15.2 Součinnost Provozovatele Aplikace MS2014+

Pro poskytování dané služby jsou jednotlivé požadavky na součinnost uvedeny v příslušných kapitolách výše, popisující způsob realizace služby.

3.1.15.3 Součinnost Uchazeče služeb Prostředí

Pro poskytování dané služby jsou jednotlivé požadavky na součinnost uvedeny v příslušných kapitolách výše, popisující způsob realizace služby.

3.2 Služba „BS02_Ochrana osobních údajů“

3.2.1 Implementační plán systému řízení informační bezpečnosti

Tabulka 10: Harmonogram implementace služby BS_02

Implementační plán - systému řízení informační bezpečnosti (SŘIB)			
Kód	**Aktivita**	**Očekávaný výstup**	**Termín plnění nebo důležitý milník projektu**
1.4.0	**Naplňování aktivity BS02/01: Metodická a legislativní podpora:** **Poskytovatel bude zajišťovat zejména následující činnosti:** • informovat Objednatele o připravovaných či aktuálních změnách v oblasti OOÚ a navazující legislativy s důrazem na posouzení a identifikaci dopadů těchto změn do podmínek MS2014+, • příprava návrhů, procesů a metodických postupů na základě legislativních změn v oblasti OOÚ s návrhem postupu jejich implementace do systému MS2014+, návrh metodických postupů a odpovědí na metodické dotazy Objednatele, Provozovatele Aplikace MS2014, Poskytovatele služeb Prostředí a uživatelů systému MS2014+.	Nastavení systému pravidelného reportingu	3 MD 1 x za měsíc za uplynulé období, denní monitoring služby 08.00 -16.00
1.4.1	**Naplňování activity BS02/02: Definice metodik, procesů a postupů ochrany osobních údajů a jejich prosazení do bezpečnostní dokumentace ISMS:** Činnosti Uchazeče musí zajistit zejména: - Identifikaci a popis účelu zpracování osobních údajů v systému MS2014+, - Identifikaci a vymezení prostředků zpracování OÚ v rámci MS2014+ a stanovení přesných způsobů a podmínek zpracování OÚ v těchto prostředcích, - Stanovení kategorií OÚ, kategorií subjektů, jejichž OÚ jsou zpracovávány a kategorie příjemců, kterým bude systém MS2014+ tyto údaje poskytovat, - Stanovení přesné identifikace zdrojů OÚ, ze kterých bude systém MS2014+ čerpat. - Stanovit místa zpracování a délku trvání shromažďování OÚ v rámci MS2014+, - Identifikovat a vymezit propojení MS2014+ na jiné	Paralelní aktivita s aktivitou BS01/01	Max. do 2 měsíců od podpisu Smlouvy

	správce nebo zpracovatele OÚ - Definovat způsob poskytnutí souhlasu a zajištění přístupu subjektu, jehož OÚ jsou zpracovávány a shromažďovány, k těmto OÚ, - Identifkovat a definovat předpokládané přenosy OÚ mimo ČR - Vymezit způsob vedení přehledu o zpracování osobních údajů uživatelů systému MS2014+, - Stanovit odpovědnosti za zpracování a ochranu OÚ v rámci systému MS2014+, - Provést analýzu rizik souvisejících se zpracováním OÚ v systému MS2014+, vyhodnocení dopadů a návrh opatření na eliminaci identifikovaných hrozeb, - Stanovit způsob zpracování, uchovávání a likvidace OÚ v podmínkách MS2014+, - Určit a zdokumentovat vhodná technická a organizační opatření k OOÚ s důrazem na zabezpečení automatizovaného zpracování OÚ v systému M2014+.		
1.4.2	**Naplňování aktivity BS02/03**: Kontrola zpracování osobních údajů: Uchazeč bude na denní bázi provádět kontrolní činnost v oblast dodržování zásad OOÚ v systému MS2014+. Kontroly budou zaměřeny zejména na: - dodržování postupů zpracování, uchovávání a likvidace OÚ v podmínkách MS2014+; - dostatečnost a adekvátnost technických a organizačních opatření OOÚ v systému MS2014+; - úplnost kategorií, zdrojů a odběratelů OÚ v systému MS2014+; - dodržování rozsahu zpracovávaných OÚ.	Paralelní aktivita s aktivitou BS01/01	Max. do 2 měsíců od podpisu Smlouvy
1.4.3	**BS02/04: Nastavení pravidelného systému vyhodnocování služby:** O poskytnutí všech služeb bude připraven ze strany Uchazeče tzv. "Protokol o poskytnuté službě" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující: - Výkaz činností za oblast OOÚ; - Protokoly o provedených kontrolách OOÚ; - Přehled čerpání hodin v oblasti Metodické a legislativní podpory Objednatele	Pravidelný reporting	1 x za měsíc za uplynulé období, denní monitoring služby 08.00 -16.00
1.4.4	**BS02/04: Nastavení pravidelného**	Pravidelný reporting	1 x za měsíc za uplynulé období, denní monitoring služby 08.00 -16.00

	systému vyhodnocování služby: O poskytnutí všech služeb bude připraven ze strany Poskytovatele tzv. "Protokol o poskytnuté službě" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující: - Výkaz činností za oblast OOÚ; - Protokoly o provedených kontrolách OOÚ; - Přehled čerpání hodin v oblasti Metodické a legislativní podpory Objednatele		

3.2.2 Metodická a legislativní podpora

Postup řešení si klade za cíl navrhnout a implementovat řízený systém ochrany osobních údajů v systému MS 2014+ za využití stávajících a navrhovaných opatření k ochraně informací ze služby BS01_Informační bezpečnost a doplnit je opatřeními, která chybí k úplnému naplnění specifických požadavků, vyplývajících ze zákona č. 101/2000 Sb., o ochraně osobních údajů v platném znění a související legislativy EU.

Současně bude Uchazeč reflektovat na oficiálně zveřejňovaná stanoviska Úřadu pro ochranu osobních údajů a příslušných orgánů EU a v souvislosti s případnými změnami v těchto stanoviscích navrhovat změny v zavedeném systému řízení osobních údajů v MS2014+.

V navrhovaném systému ochrany osobních údajů budou zohledněny následující zásadní aspekty:

- odpovědnosti, práva a povinnosti orgánu, který zastupuje správce osobních údajů navenek systému MS2014+,
- odpovědnosti, práva a povinnosti orgánu, který zajišťuje a zodpovídá za plnění povinností správce osobních údajů uvnitř systému MS2014+,
- odpovědnosti, práva a povinnosti bezpečnostního management a určených bezpečnostních rolí v systému MS2014+,
- odpovědnosti, práva a povinnosti zaměstnanců, oprávněných ke zpracování osobních údajů v systému MS2014+.

Prioritně budou řešeny ty problematiky, ze kterých hrozí sankce pro organizaci, možná finanční újma a případně ztráta či poškození dobrého jména způsobená únikem zpracovávaných osobních údajů.

Uchazeč již v současnosti pravidelně monitoruje veškeré Informační zdroje uvedené Objednatelem v Příloze č. 1 Smlouvy, kapitole BS_02 Ochrana osobních údajů, bodě 3.2.2.1 Metodická a legislativní podpora Objednatele, protož poskytuje trvalou podporu řádově desítkám klientů v oblasti ochrany osobních údajů.

Uchazeč v rámci této služby využije svých znalostí a v této specifické oblasti zejména zkušeností z obdobných rozsáhlých projektů u ministerstva zemědělství ČR – Sekce pozemkových úřadů, Generálního finančního ředitelství ČR a dalších. Současně bude Uchazečem využita znalost a zkušenost z jednání se zástupci Úřadu pro ochranu osobních údajů v rámci zastupování za klienta.

Pro řešení ad-hoc dotazů z oblasti ochrany osobních údajů bude zřízen Uchazečem Help-desk.

Pro zavedení řízeného systému osobních údajů, korespondujícího se zaváděným ISMS MS2014+ Uchazeč navrhuje v rámci tohoto kroku nejdříve provést Analýzu stavu a rozsahu zpracování osobních údajů.

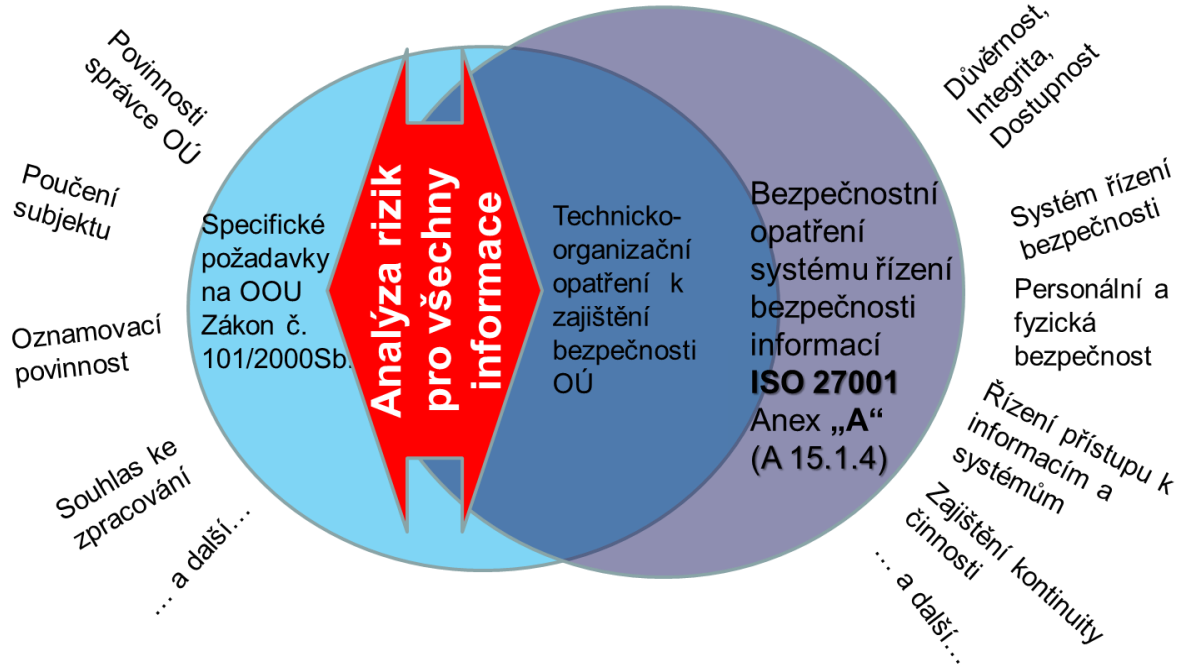
3.2.3 Analýza rozsahu zpracování osobních údajů

Pro analýzu stavu zpracování osobních údajů budou jako základní vstupy využity procesy a agendy, zjištěné v rámci realizace služby BS01_Informační bezpečnost.

Analýza bude provedena následujícím způsobem:

- studiem relevantní dokumentace vztahující se k řídícím procesům u organizace a v systému,
- interview s vybranými pracovníky v rámci BS_01,
- formálním posouzením všech dostupných písemností, zejména dodavatelských a jiných smluv, pracovních smluv, organizačního, pracovního a spisového řádu, provozní a existující bezpečnostní dokumentace systému a dalších interních směrnic a předpisů,
- provedením srovnávací analýzy zjištěných skutečností s požadavky zákonných norem,
- zodpovězením dotazů vzniklých ad-hoc v rámci analýzy.

Níže uvedené schéma zobrazuje průnik mezi zákonem č. 101/2000 Sb. a ISMS a je z něj zřejmé, že ISMS nepokrývá veškeré požadavky zákona o ochraně osobních údajů. Proto je nutná analýza, která zdokumentuje veškeré požadavky zákona o ochraně osobních údajů a zmapuje je na zaváděná opatření ISMS.



Obrázek 7: Analýza rozsahu

Výstupem z analýzy bude Závěrečná zpráva obsahující a hodnotící:

1) Definici zjištěných účelů zpracování osobních údajů rozlišených na:
   a) Zpracování osobních údajů explicitně zpracovávaných na základě zvláštního (jiného) zákona z pohledu (např. věcné zákony, mzdové, personální agendy, smluvní vztahy atd.)
   b) Účelů zpracování osobních údajů zpracovávaných na základě vnitřní potřeby Objednatele z pohledu (např. kamerové systémy se záznamem, data zaměstnanců zveřejňovaná na firemním intranetu atd.)
2) Identifikované účely zpracování budou dále posouzeny a vyhodnoceny dle:
   - Rozsahu zpracovávaných osobních údajů a oprávněnosti jejich zpracování k danému účelu,
   - deklarace prostředků a způsobů zpracování,
   - shromažďování osobních údajů pouze ke stanovenému účelu,
   - doby uchování osobních údajů,
   - zpracování pouze v souladu s deklarovaným účelem.
3) U každého účelu zpracování budou identifikovány zdroje osobních údajů
4) U každého účelu zpracování bude identifikováno, kdo je Správce a kdo Zpracovatelem ve smyslu předmětného zákona
5) Na základě bodu 4) budou sumarizovány účely zpracování, kterých je Objednatel Správcem, a kterých je Zpracovatelem
6) Požadování souhlasu a správnost jeho znění při zpracování osobních a případně citlivých údajů

7) Informování subjektu údajů o zpracování jejich údajů.
8) Přístupu subjektu údajů k informacím.
9) Smluvního vztahu mezi:
    a. Správcem a Zpracovatelem;
    b. Správcem, Zpracovatelem a jejich zaměstnanci.
10) Oznamovací povinnosti.
11) Likvidace osobních údajů.
12) Ochrany práv subjektů údajů.
13) Předání osobních údajů do jiných států.

V rámci tohoto zhodnocení bude jednoznačně uvedeno, která pravidla a postupy je:

- **Nutné** zdokumentovat a zavést,
- **Vhodné** zdokumentovat a zavést,
- **Zakázané** realizovat v souvislosti se zpracováním osobních údajů.

3.2.4 Definice metodik, procesů a postupů ochrany osobních údajů a jejich prosazení do bezpečnostní dokumentace ISMS

V rámci této činnosti bude nejdříve provedeno posouzení rizik v rozsahu požadavků § 13 zákona č. 101/2000 Sb. o ochraně osobních údajů a na jeho základě bude definována nezbytná úroveň bezpečnosti a technickoorganizačních opatření pro zajištění zpracování osobních údajů v identifikovaných agendách. Tato nezbytná úroveň bezpečnosti bude namapována na současně navrhovaná a zaváděná opatření ISM MS2014+ s cílem uplatnit maximum navržených opatření z ISMS a jeho PoA.

Současně budou prověřeny všechny smluvní vztahy mezi Správcem (Objednatelem) a případnými Zpracovateli osobních údajů, kterých je Objednatel Správcem. Smluvní vztahy budou prověřeny zejména z hlediska deklarace Zpracovatelů k dodržení bezpečnosti jimi zpracovávaných osobních údajů (ve prospěch Objednatele – Správce). Zpracovatel musí mít nastevanu úroveň bezpečnosti na minimálně stejné úrovni jako Správce.

Následně bude vypracována řízená dokumentace k ochraně osobních údajů v rozsahu:

- **Směrnice pro ochranu osobních údajů**, která bude u organizace a systému MS2014+ závazným řídícím dokumentem pro všechny zaměstnance Správce a která stanovuje základní pravidla pro práci s osobními údaji v organizaci a systému,
- **Manuál správce osobních údajů** obsahující:
    - **Posouzení rizik** v rozsahu požadovaném § 13 odst. 3 zákona č. 101/2000 Sb. a návrhy opatření k jejich snížení,
    - **Metodika bezpečnostního správce systému** pro zajištění ochrany osobních údajů,
    - **Pravidla práce** s výpočetní technikou pro uživatele systému.
- Manuál dále obsahuje následující přílohy:

- přehledy zjištěných účelů zpracování osobních údajů,
- vzory (šablony) souhlasů subjektů osobních údajů pro zpracování jejich údajů,
- přehledy se zpracovávanými osobními údaji ke splnění oznamovací povinnosti dle § 18 odst. 2 zákona č. 101/2000 Sb.,
- vyplněné registrační formuláře pro zjištěné účely zpracování, které podléhají oznamovací povinnosti dle § 16 zákona č. 101/2000

Uchazeč provede výše uvedené činnosti a předá stanovené dokumenty ke schválení Objednateli do 2 kalendářních měsíců od akceptace výstupů uvedených v kapitole 1.2 nabídky.

3.2.5 Kontrola zpracování osobních údajů

Praktické zkušenosti ukazují, že žádné opatření se neobejde bez technických a procesních kontrolních mechanismů, posuzování kvality a vyhodnocování účinnosti opatření s následným návrhem přiměřených opatření pro zlepšování. V rámci tohoto bodu bude přezkoumáno, zda je zaveden a naplňován „Procesní model řízení – PDCA (PLAN, DO, CHECK, AKT), s doporučením period kontrolní činnosti a aktualizace jednotlivých zavedených pravidel a postupů.

Uchazeč bude na denní bázi provádět kontrolní činnost v oblast dodržování zásad OOÚ v systému MS2014+. Kontroly budou zaměřeny zejména na:

- dodržování postupů zpracování, uchovávání a likvidace OÚ v podmínkách MS2014+;
- dostatečnost a adekvátnost technických a organizačních opatření OOÚ v systému MS2014+;
- úplnost kategorií, zdrojů a odběratelů OÚ v systému MS2014+;
- dodržování rozsahu zpracovávaných OÚ.
- Z výsledků kontrolní činnosti bude Uchazeč na měsíční bázi zpracovávat souhrnné reporty (specifikované v části Vyhodnocení služby) a překládat je Objednateli.

3.2.6 Vyhodnocení služby

O poskytnutí všech služeb bude připraven ze strany Uchazeče tzv. "**Protokol o poskytnuté službě**" za dobu uplynulého vyhodnocovacího období a obsahující zejména následující:

- Výkaz činností za oblast OOÚ;
- Protokoly o provedených kontrolách OOÚ;
- Přehled čerpání hodin v oblasti Metodické a legislativní podpory Objednatele.

3.2.7 Organizační zajištění projektu

Řízení Projektu bude realizováno podle standardů, které reprezentují obvyklé postupy čerpající z nejlepší mezinárodní praxe a ověřené na desítkách obdobných projektů v České republice v soukromém i veřejném sektoru. Řízení Projektu bude rovněž podpořeno osvědčenou metodikou PRINCE2.

V rámci nulté fáze Projektu bude vytvořena a obsazena struktura projektového řízení, která vznikne propojením standardního modelu řízení aplikovaného Uchazečem a projektovou strukturou Objednatele.

Organizační uspořádání navržené Uchazečem je vytvořeno tak, aby umožňovalo efektivní řízení projektových prací a účinnou komunikaci všech složek Projektu. Je navrhován tříúrovňový systém řízení:

- **Strategická a taktická úroveň** – tato úroveň řízení je reprezentována Řídicím výborem (dále též „ŘV“), který je tvořen členy se zástupci Objednatele a partnerem projektu za Uchazeče, popřípadě zástupci dalším zainteresovaných subjektů. Účelem je rozhodovat o vybraných klíčových strategických otázkách a provádět vrcholové řízení Projektu.
- **Operativní úroveň** – Operativní úroveň řízení je reprezentována vedením Projektu (dále též „VP“). Členy vedení Projektu jsou zástupci nominovaní Objednatele, dále pak vedoucí Projektu za Uchazeče, popřípadě administrátoři Projektu a jednotlivé projektové týmy. Účelem operativní úrovně řízení je řídit a realizovat provádění projektových prací na každodenní bázi.

3.2.7.1 Řídící výbor

Řídicí výbor je taktickou úrovní řízení Projektu. Jednání Řídicího výboru jsou organizována pravidelně v předem stanovené frekvenci. Obvykle jsou jednání ŘV organizována na měsíční bázi, dle potřeby lze doporučit frekvenci setkávání ŘV upravit a jednání organizovat např. každých 14 dní. Úlohou ŘV je především:

- průběžně sledovat a kontrolovat plnění cílů a kvality Projektu;
- provádět hodnocení průběhu Projektu v návaznosti na stanovený harmonogram Projektu;
- dohlížet na aplikování metodiky projektových prací;
- schvalovat zásadní změny Projektu;
- řešit zásadní konflikty v nejvyšších strukturách Projektu;
- komunikovat s externími subjekty (zejména s čelními představiteli Objednatele a zástupci samosprávy).

Řídicí výbor je řízen sponzorem projektu. Jedním z úkolů členů řídicího výboru je napomáhat prosazování projektových výsledků.

Vzhledem k charakteru projektu, jehož úspěch je založen na velmi otevřené a intenzivní komunikaci s vysokým počtem zainteresovaných subjektů navrhuje Uchazeč relativně malé složení Řídicího

výboru na úrovní vybraných členů Objednatele, popřípadě třetích stran, zainteresovaných na plnění dílčích projektových plnění celého monitorovacího system.

Ke každému bodu jednání se má právo vyjádřit každý člen řídicího výboru. Cílem jednání je vždy dosažení konsenzu. V případě nejasností či sporů uvnitř řídícího výboru, respektive v celém Projektu, nebo v případě změny priorit Projektu, má hlavní a rozhodující slovo sponzor Projektu Objednatele.

3.2.7.2 Vedení projektu

Vedení projektu je orgán operativního řízení projektových prací. Je složen z vedoucího Projektu Uchazeče administrátorů Projektu Objednatele a administrátora projektu Uchazeče a dle potřeby z dalších relevantních členů Projektu (vedoucí případných pracovních týmů apod.). Úlohou vedení Projektu je:

- zabezpečit přípravu projektových výstupů k akceptaci;
- průběžně monitorovat stav a vývoj projektových prací;
- přijímat operativní rozhodnutí vedoucí k naplnění cílů Projektu;
- připravovat podklady a otázky k rozhodnutí pro Řídicí výbor;
- dbát na dodržování kvality výstupů a jejich včasnost;
- řešit problémy a rizika Projektu a rozhodovat o méně zásadních změnách;
- předkládat Řídicímu výboru k rozhodnutí významná rizika (tj. rizika s dopadem na harmonogram, cenu nebo kvalitu Projektu) spolu s alternativami jejich vypořádání.

Tomuto orgánu předávají jednotlivé projektové týmy informace o stavu a vývoji prací. Tento orgán se schází pravidelně, a to v předem určených termínech.

Vedoucí Projektu za Uchazeče, odpovídá za odborné vedení Projektu, zejména za:

- realizaci Projektu v rámci schválených cílů, postupů a rozsahu prací;
- dodržování schváleného rozpočtu;
- dodržování termínů podle schváleného harmonogramu;
- dodržování definované kvality;
- sběr, vyhodnocování a sumarizaci informací o průběhu Projektu;
- řízení rizik Projektu;
- schvalování požadavků na změnu (po dohodě se správní radou projektu), které nemají zásadní vliv na cíle a rozsah, harmonogram, rozpočet a kvalitu Projektu;
- detailní plánování, schvalování a koordinaci všech aktivit Projektu na vlastní úrovni řízení;
- přidělování úkolů vedoucím jednotlivých projektových týmů;
- koordinaci činností Projektu vzhledem k organizaci a lidským zdrojům na straně Objednatele.

Vedoucí Projektu Uchazeče garantuje splnění smluvně dohodnutých cílů Projektu a odpovídá za zabezpečení vhodných zdrojů ze strany Uchazeče.

Administrátor Projektu za Objednatele

Hlavní rolí administrátora Projektu za objednatele je zabezpečení technicko - organizační podpory projektu, je řízen vedoucím projektu. Mezi jeho hlavní činnosti patří:

- příprava a distribuce dokumentů pro jednání Řídicího výboru a vedení Projektu;
- organizace jednání Řídicího výboru a vedení Projektu;
- zajištění schválení zápisů z jednání Řídicího výboru a vedení Projektu (příp. dalších dle dohody) na straně Objednatele a distribuce účastníkům schůzky ze strany Objednatele;
- rozmnožování a distribuce dokumentů z Projektu na straně Objednatele;
- zveřejňování schválených dokumentů pro ostatní členy projektového týmu na straně Objednatele;
- zabezpečení organizace workshopů/kulatých stolů k prezentaci a diskuzi výsledků a zjištění z jednotlivých procesních analýz za účasti zástupců analyzovaných institucí;
- další technicko - organizační záležitosti.

Administrátor Projektu za Uchazeče

Administrátor Projektu zabezpečuje technicko-organizační podporu pro Projekt za stranu Uchazeče je řízen vedoucím Projektu Uchazeče. Mezi jeho hlavní činnosti patří:

- distribuce dokumentů v rámci týmu Uchazeče;
- správa a administrace projektových nástrojů (přidání uživatelů, správa uživatelských oprávnění, aktualizace struktury a obsahu úložiště atp.);
- předávání oficiálních výstupů Projektu k zahájení procesu akceptace;
- rozmnožování a distribuce dokumentů z Projektu na straně Uchazeče;
- zveřejňování schválených dokumentů pro ostatní členy projektového týmu na straně Uchazeče;
- vyhotovování zápisů z jednání Řídicího výboru a vedení Projektu (příp. dalších dle dohody);
- další technický organizační záležitosti.

3.2.7.3 Projektové týmy

Projektové týmy jsou výkonnou složkou Projektu, která zpracovává výstupy Projektu a plní úkoly dle projektového plánu a pokynů vedoucího Projektu za Uchazeče.

Pro specifické oblasti, které budou předmětem služeb dodávaných Uchazečem, budou vytvořeny popřípadě dílčí projektové týmy (pokud to bude rozsah projektu vyžadovat). Po celou dobu trvání projektu pak bude fungovat tým, jehož odpovědností bude zejména následující:

- dohled nad průběhem změnového řízení, tj. zajištění, že všechny realizované dílčí projekty jsou navzájem v souladu, dochází k efektivnímu sdílení informací napříč jednotlivými týmy,
- naplánované aktivity jsou realizovány ve stanovených termínech, případně zajišťuje úpravu časového harmonogramu v případě vyskytnuvších se problémů;
- komunikaci, a to jak směrem k Objednateli a uživatelům, tak i směrem k veřejnosti, a to jak odborné, tak i laické veřejnosti.

Tyto dílčí týmy budou odpovídat za realizaci konkrétních projektových řešení v daných oblastech. Projektové týmy budou řízeny vedoucím Projektu za Uchazeče a budou svolávány v pravidelných týdenních intervalech (či jiných intervalech dle potřeby Projektu). Každý z projektových týmů předkládá vedení Projektu a Řídicímu výboru ke schválení a akceptaci výstupy Projektu. Projektový tým předkládá vedení Projektu k rozhodnutí problémy / rizika / změny Projektu.

Člen projektového týmu za Poskytovate

Působí v příslušném projektovém týmu jako odborník v oblasti informačních technologií, ICT procesů a bezpečnosti ICT, v oblasti analýz rizik, v oblasti systémově manažerského, metodického a organizačního poradenství a v dalších oblastech dle náplně práce projektového týmu a jeho úkolů.

Jednotliví členové týmu budou odpovědní za:

- metodickou správnost postupu Projektu pro danou oblast;
- směrování práce týmu k dosažení stanovených cílů;
- vlastní realizaci projektových prací;
- vypracování a přípravu projektových výstupů a dalších podkladů.

3.2.7.4 Vedení projektové dokumentace

Pro potřeby stejné a formálně unifikované sestavy dokumentace bude pro každý z typů dokumentu vytvořena samostatná šablona (např. šablona pro vedení registru rizik, status report, zápis z jednání). Všechny dokumenty jsou v tzv. řízeném režimu – u každého dokumentu bude vyplňována hlavička s uvedením garanta dokumentu, jeho zpracovatele, čísla verze a data jejího schválení, stejně jako tabulky se změnami provedenými v dokumentu.

Zápisy z jednání a zprávy o stavu Projektu

Průběh prováděných projektových prací je dokumentován ve formě zpráv o stavu Projektu, které bude připravovat vedoucího Projektu za Uchazeče, jako podklad pro jednání řídicího výboru Projektu, a ve formě strukturovaných zápisů z jednání řídicího výboru. Ze všech důležitých schůzek uskutečněných v rámci projektu bude proveden zápis.

Zpráva o stavu Projektu (status report) je dokument vytvořený vedoucím Projektu za Uchazeče pro řídicí výbor Projektu. Součástí zprávy o stavu Projektu je:

popis realizovaných činností;
plán projektových prací na další období;
popis rizik a návrh opatření;
požadavky na akci ze strany řídicího výboru.

Zpráva o stavu Projektu je vyhotovována jako podklad pro řídicí výbor. Formou příloh je ke zprávě o stavu Projektu připojen i aktuální plán Projektu (došlo-li k jeho změně), seznam rizik, požadavků na změny a souhrnný seznam změn a jejich stavu.

Zápis z jednání se účastníkům jednání předkládá do 24 hodin po jednání. Nevyjádří-li se protistrana k zápisu do 3 pracovních dnů od obdržení, je zápis brán jako akceptovaný bez připomínek. V případě rozporů ohledně znění zápisu z jednání rozhoduje o finálním znění řídící výbor.

Správa dokumentace

Pro účely transparentního a přehledného zpracování jednotlivých verzí dokumentace a jejich revizí je stanovena **procedura správy verzí dokumentace.**

Pro účely efektivního sdílení informací a dokumentů bude vytvořeno úložiště, do kterého budou mít přístup všichni členové Projektu, a to jak na straně Uchazeče, tak i na straně Objednatele. Mezi základní rysy tohoto nástroje patří zejména následující:

- bezpečná výměna dokumentů (publikace nových dokumentů a sledování vývoje verzí u vyvěšených dokumentů);
- odpadají starosti s posíláním nových nebo pozměněných dokumentů e-mailem;
- plynulá komunikace (výměna dokumentů) určená vnitřní strukturou úložiště;
- přístup přes Webové rozhraní dává možnost publikovat či stahovat dokumenty odkudkoli.

Správou úložiště bude pověřen administrátor Projektu za Uchazeče.

Řídicí výbor provede na žádost vedoucího Projektu za Uchazeče akceptaci formy a struktury výstupu. Cílem tohoto kroku je metodicky zafixovat a kodifikovat se zástupci slučovaných subjektů formu a strukturu výstupu ještě před započetím prací a minimalizovat tím riziko rozdílných očekávání o daném výstupu ze strany slučovaných subjektů. O akceptaci formy a struktury dokumentovaného výstupu bude pořízen zápis. Stejným způsobem bude postupováno i v případě ostatních dokumentů, které budou zpracovávány v průběhu Projektu (zejména v případě zpracování návrhů nových procesů řízení a jejich kontroly dle stanovené metodiky, časového a finančního plánu implementace procesů). Schvalování všech výstupů Projektu bude provádět Řídicí výbor na základě požadavku vedoucího Projektu za Uchazeče, který výstupy předkládá ke schválení v souladu s řádnými termíny uvedenými ve věcném a časovém harmonogramu Projektu.

Revize (připomínkování) **výstupů** – pokud to věcný obsah výstupu umožňuje, Uchazeč navrhuje jednotlivé výstupy Projektu před předáním k zahájení procesu formální akceptace průběžně komunikovat a detailně připomínkovat. Již v této fázi akceptačního procesu se mohou i ostatní členové Řídicího výboru zapojit do připomínkového řízení a vznášet své připomínky. K zaznamenání

výsledků revize ze strany Objednatele bude sloužit standardizovaný formulář. Výsledek a stanovisko z této revize bude postoupeno Řídicímu výboru. Termíny pro realizaci připomínkování by neměly překročit 5 pracovních dní (odvozeno od zkušeností Uchazeče).

Finální akceptace Řídicím výborem – po realizaci dílčích akceptací/revizí jednotlivých výstupů dochází k formální akceptaci. Doba pro formální akceptaci výstupu nepřekročí 15 pracovních dní ode dne dodání výstupu administrátorovi projektu za Objednatele, členové Řídicího výboru za Objednatele rozhodnou o formě akceptace:

- akceptace výstupu v plném rozsahu;
- podmínečná akceptace výstupu s definicí připomínek k zapracování;
- výstup není akceptován s definicí důvodu/ů a problémových oblastí výstupu.

Rozhodnutí o formě akceptace bude zachyceno v zápisu z jednání a bude předáno projektovému týmu s připomínkami k zapracování do deseti pracovních dnů od předložení výstupu, přičemž připomínky musejí být konkretizovány s odkazem na skutečnosti uvedené v předloženém výstupním dokumentu, a to včetně termínů pro předložení upravených výstupů. V případě, že připomínky k předloženému výstupu nebudou mít zásadní charakter, mohou členové Řídicího výboru za Objednatele rozhodnout o tzv. **podmíněné akceptaci výstupu** – tím se pokládá daný výstup za akceptovaný s tím, že k plné akceptaci stačí předložení zapracovaných připomínek Řídicímu výboru cestou Projektového administrátora v elektronické podobě bez zbytečného odkladu, nejpozději však do 10 dní.

Pro akceptační řízení platí **obecná zásada**, že nevyjádří-li se členové Řídicího výboru na straně klienta do stanoveného data, jsou výstupy považovány za akceptované bez výhrad. Po úspěšné akceptaci každého z dílčích výstupů Projektu se bude konat **workshop/kulatý stůl** k prezentaci výsledků z dané fáze Projektu a diskuzi příslušných výsledků a zjištění. Na workshop budou přizváni účastníci dle požadavků Objednatele, popřípadě jeho dalších subdodavatelů celkového řešení. Cílem těchto workshopů je do dění Projektu zapojit co nejširší spektrum zainteresovaných subjektů. Zároveň se budou workshopů účastnit minimálně 2 zástupci projektového týmu Uchazeče.

Akceptovaný výstup je vytištěn a předán sponzorovi Projektu na základě podepsaného akceptačního protokolu. Součástí předání výstupu je i jeho předání v elektronické podobě (formou CD přiloženého k tištěnému dokumentu).
Eskalační procedura. Pro zajištění operativní reakce na aktuální problémy/rizika v rámci realizace Projektu a pro zajištění jejich nápravy tak, aby nebylo ohroženo splnění cílů Projektu, jsou stanovena pravidla pro eskalaci problému v rámci Projektu, jež respektují navrženou organizační a řídicí strukturu Projektu.

Aktuální problémy/rizika, které se vyskytnou v průběhu realizace Projektu, budou primárně řešena na té úrovni, na jaké věcně vznikla, tzn. na úrovni projektového týmu, a to v souladu s jím definovanými odpovědnostmi a pravomocemi. Současně platí pravidlo, že problémy, které není možné při dobré vůli vyřešit z jakýchkoliv důvodů na nižší řídicí úrovni, jsou bez zbytečného odkladu postoupeny na vyšší řídicí úroveň Projektu, tzn. z úrovně pracovního týmu na úroveň vedení Projektu, eventuálně v dalším stupni na úroveň Řídicího výboru Projektu.

Na problém, který se vyskytne v průběhu řešení Projektu, může upozornit jakýkoliv člen projektového týmu, vedení Projektu nebo Řídicího výboru, a to neformálním způsobem (ústní informace) a zároveň i formálním způsobem (písemně), a to vždy svému přímému nadřízenému v projektové struktuře, který je povinen přidělit odpovědnost za vyřešení problému / rizika. Osoba zodpovědná za vyřešení problému / rizika připraví návrh řešení, včetně termínů a odpovědností, který si nechá schválit

Objednatelem úkolu. Schválené řešení je následně realizováno, osoba zodpovědná za vyřešení vyhodnotí výsledek, který komunikuje směrem k Objednateli úkolu a jeho prostřednictvím v případě potřeby řídicí úrovni Projektu výboru nebo řídicímu výboru.

Řízení změn je chápáno jako proces, kterým je zajištěna úspěšná realizace požadavku na změnu. Změny jsou integrální součástí Projektu a z tohoto důvodu je řízení změn považováno Uchazečem za jeden z kritických faktorů pro jeho úspěšné dokončení. Jednotlivé změny pak mohou mít dopad jak na projektové plány, kvalitu dodávky, náklady, tak i na smluvní vztahy, na pracovní postupy atd. Většina projektových činností proto podléhá řízení změn. Drobné změny Projektu bez dopadu na časový plán, rozpočet a hlavní cíle Projektu mohou posuzovat a rozhodovat vedoucí Projektu. O výsledku informují řídicí výbor.

Řízení projektových rizik. Proces řízení rizik a problémů je složen z několika základních kroků:

1. **Identifikace a evidence rizik a problémů** – zahrnuje transformaci obecně vnímaných, často jen nejasně definovaných a mnohdy spíše tušených negativních faktorů na jasně definovaná, měřitelná a řiditelná rizika. Pro evidenci rizik a problémů slouží standardizovaný formulář. O rizicích/problémech a způsobu jejich vypořádání informuje vedoucí Projektu Uchazeče řídicí výbor. Řídicí výbor je informován o rizicích/problémech na pravidelných schůzkách formou standardizované sestavy.

2. **Analýza rizik a problémů** – cílem je stanovit předpokládaný dopad rizika/problému na Projekt a určit prioritu jeho řešení. Prioritu řešení rizika/problému určuje vedení Projektu. Rizika, resp. problémy s prioritou „Vysoká“ jsou taková, která zásadně negativně ovlivňují (resp. u rizik mohou potenciálně ovlivnit) harmonogram, rozpočet, kvalitu nebo cíle Projektu. Rizika / problémy s prioritou „Střední“ a „Nízká“ ovlivňují Projekt jen částečně.

3. **Plánování reakce** – cílem je rozhodnout o tom, jak bude s daným rizikem/problémem naloženo. Rizika a problémy jsou primárně řešena na úrovni vedení Projektu. Pověřený zástupce výkonné rady nebo vedoucí Projektu Uchazeče rozhodne o způsobu eliminace rizika, resp. problému a určí osobu odpovědnou za realizaci preventivních, resp. nápravných opatření. V případě vzniku závažného rizika/problému vedení Projektu neprodleně informuje Řídicí výbor a vyžádá si rozhodnutí o způsobu jeho vypořádání. Vedení Projektu předloží Řídicímu výboru alternativní návrhy vypořádání rizika/problému a Řídicí výbor rozhodne o jedné z alternativ (tím není nijak omezeno právo Řídicího výboru na prosazení návrhu vypořádání rizika/problému, který nebyl v alternativách předložených vedením Projektu).

4. **Sledování indikátorů změn** – cílem je poskytnout srozumitelnou představu o tom, v jakém stavu se rizika/problémy nacházejí. Vedoucí Projektu kontinuálně identifikuje, eviduje, analyzuje, plánuje a eliminuje projektová rizika a problémy. V návaznosti na události, které se v Projektu uskutečnily, a na vývoj v řešení jednotlivých rizik problémů vedoucí Projektu Uchazeče průběžně aktualizuje přehled rizik a problémů.

5. **Reakce a uzavření rizika problému** – posledním krokem řízení rizik, resp. problémů je samotná reakce na riziko nebo problém, vyhodnocení preventivních, resp. nápravných opatření a jeho uzavření. Platí pravidlo, že riziko/problém může uzavřít pouze osoba, která je odpovědná za realizaci preventivních, resp. nápravných opatření. Před tím, než je riziko uzavřeno, je nutný souhlas výkonné rady projektu, resp. v případě rizika/problému s vysokou

prioritou Řídicího výboru, o tom, že riziko/problém bylo buď plně eliminováno, nebo bylo zmírněno na takovou úroveň, že již nemůže významně ohrozit průběh Projektu.

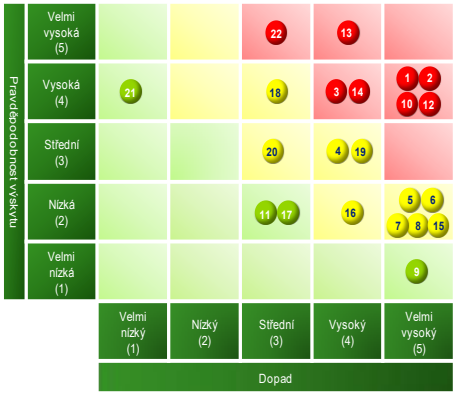
V okamžiku identifikace příslušného rizika dojde k jeho zaznamenání do **registru rizik**. Tento nástroj pro evidenci, monitorování a vyhodnocování rizik se Uchazeči v praxi velmi osvědčil. Strukturu registru rizik zachycuje následující obrázek.

Závažnost (vliv na úspěšnost	*Popis reakce*
Vysoká	Vyžaduje okamžitou pozornost
Střední	Vyžaduje pravidelnou revizi
Nízká	Postačí občasný monitoring

ID	Funkční oblast	Vlastník rizika (jméno)	Datum identifikace rizika	Název rizika	Popis rizika (existuje riziko, že…)	Dopad rizika	Závažnost	Pravděpodobnost výskytu (1-5)	Dopad na úspěšnost projektu (1-5)	Eliminace rizika	Komentář	Status

Obrázek 8: Struktura registru rizik

Na základě registru rizik bude posléze zpracována **matice rizik**, která graficky zachycuje rizika z hlediska jejich závažnosti dopadu a pravděpodobnosti výskytu. Matice pravděpodobnosti-dopadu slouží k stanovení závažnosti rizik a umožňuje hodnocení rizik tak, aby bylo možné určit, kterým rizikům se má vedení projektu prioritně věnovat (viz výše). Pravděpodobnost výskytu je hodnocena na škále od 1 do 5 podle toho, s jakou pravděpodobností reálně může dojít k naplnění rizika (1 nejmenší, 5 největší). Dopad je stanoven obdobně a určuje velikost dopadu rizika na projektové cíle v případě jeho naplnění. V grafu je, podle postoje projektu k riziku, možné zobrazit linii tolerance rizika, která udává oblast, za kterou již nejsou rizika akceptovatelná (obyčejně v průběhu žlutého pole). Ukázka možného zhodnocení rizik je zobrazena na následujícím obrázku. Linie tolerance je odlišená barevně – zeleně značená jsou akceptovatelná rizika (nízká závažnost – 1 – 6 bodů), žlutá rizika jsou akceptovatelná pouze za mimořádných okolností (střední závažnost 7 – 14 bodů) a červená rizika jsou neakceptovatelná (vysoká závažnost 15 – 25 bodů). Zobrazení rizika vyplývá z registru rizik (viz níže).



Obrázek 9: Ukázka matice rizik

3.2.7.5 Komunikační strategie

Cílem této části plnění je zabezpečit pravidelné a standardizované získávání, analyzování a šíření informací o projektu jako takovém, ale zejména zajistit pravidelnou informovanost o aktuálním stavu projektu pro jeho vnitřní řídící struktury. Základem pro sdílení informací v rámci projektu je to, aby jednotliví členové projektového týmu o sobě věděli. Pro projekt nebude zřejmě potřebné vytvářet

robustní LDAP databázi, nicméně základní kontaktní matici lze jednoznačně doporučit. Kontaktní matice bude ze strany projektového manažera pravidelně aktualizována a šířena v rámci projektu. Tím bude zaručena distribuce kontaktů na všechny členy týmu a nebude docházet k prodlevám v komunikaci z důvodu chybějících kontaktů.

Po splnění této základní podmínky lze přistoupit k samotné tvorbě komunikačního plánu, resp. strategie. Na základě dosavadních zkušeností s realizací projektů obdobného charakteru Uchazeč navrhuje vytvořit specializovanou komunikační strategii. Tuto strategii je možné rozdělit do čtyř základních, na se be vzájemně navazujících kroků:

1. **Plánování komunikace**. Jedná se především o určení požadavků zainteresovaných stran na informace a komunikaci. (Kdo potřebuje jaké informace? Kdy je potřebuje? Jakým způsobem budou předány?)
2. **Distribuce informací**. Včasné dodání potřebných informací všem zainteresovaným stranám Projektu. Informace je potřebné kategorizovat dle jejich adresátů.
3. **Sledování průběhu Projektu**. Shromažďování a předávání informací o průběhu Projektu. Součástí tohoto kroku je také vykazování informací o stavu Projektu, měření postupu Projektu a prognózy dalšího vývoje projektových prací či případných rizik Projektu.
4. **Prezentace výsledků**. Jedná se zejména o generování, shromažďování a předávání informací s cílem formalizovat určitou část Projektu nebo ukončení Projektu.

Poté je potřebné definovat tzv. komunikační matici stanovující vhodné komunikační kanály a způsoby sdílení informací pro definované cílové segmenty. Matice je kombinací způsobu sdílení informací do interního a také do externího prostředí Objednatele. Na základě takto definované komunikační matice lze stanovit adresáta - úroveň řízení a typ informace spolu s distribučním kanálem a frekvencí poskytování. Tímto se dojde k optimalizovanému způsobu předávání informací.

Ukázka konkretizovaného modelu je v následující tabulce.

Adresát	Typ informace	Informační kanál	Frekvence	Zátěž adresáta
Členové ŘV	Agregovaná zpráva o postupu projektu	E-mail	1x měsíčně	Vysoká
Zaměstnanec	Obecná informace	Intranet	Kvartálně	Nízká

Po definování a usazení komunikačních pravidel je možné je následně pravidelně vyhodnocovat a realizovat dílčí úpravy směrem k jejich optimalizaci.

3.2.7.6 Požadavky na součinnost Objednatele

Návrh požadované součinnosti Objednatele je navržen tak, aby kládl na zaměstnance Objednatele minimální nároky. Uchazeč očekávává, že Objednatel nanominuje pro projektvé struktury pouze osoby odpovědné za naplňování Smluvního vztahu na straně Objednatele v souladu s požadavky poskytování součinnosti při tvorbě odborné a projektové dokumentace, která je předmětem akceptačních procedur a součástí předmětného plnění.

Požadavky organizačního zajištění:

- Zajištění prostorů pro jednání projektového týmu a uložení projektové dokumentace v prostorách Objednatele;

- Zajištění přístupů bezpečnostního týmu Uchazeče do lokalit Objednatele, které přímo souvisí s místem plnění a poskytováním služeb;
- Zpřístupnění interních normativních aktů Objednatele a odpovídající dokumentace související s předmětem plnění zakázky, po celou dobu plnění Smlouvy;
- Zajištění jedné místnosti pro provádění osobních rozhovorů se zaměstnanci Objednatele a jeho uchazečů služeb;
- Umožnění přístupu k veřejné síti Internet pro členy bezpečnostního týmu Uchazeče;
- Zajištění přístupu k tiskovým službám, pro účely tisku pracovní projektové dokumentace;
- Obsazení role Manažera projektového týmu na straně Objednatele;
- Vyčlenení odpovídajících specialistů pro požadavky naplňování procesů Akceptačního řízení;
- Zajištění odborné součinnosti dodavatelů plnění třetích stran ve prospěch Objednatele, souvisejících s předmětem plnění této zakázky;
- Umožnit členům projektového týmu Dodavatele aktivní účast na jednáních projektového týmu.

Povaha veřejné zakázky vyžaduje součinnost ze strany Objednatele a jeho dodavatelů dílčích plnění. Bez této součinnosti Uchazeč nemá možnost dosáhnout cíle veřejné zakázky, případně je plnění veřejné zakázky ohroženo z hlediska časového a/nebo rozsahu jejího záběru. Při poskytování plnění veřejné zakázky je nezbytná součinnost ze strany Objednatele minimálně v níže stanoveném rozsahu.

a) **Vytvoření prostředí pro činnost** Uchazeče. Pro zdárnou realizaci předmětu veřejné zakázky je potřeba, aby Objednatel zajistil prostředí pro činnost Uchazeč tak, aby mohl vykonávat potřebné práce na realizaci Projektu. Zajištění prostředí zahrnuje:

   - Přístup Uchazeče do míst plnění Projektu;
   - Přístup Uchazeče k zaměstnancům Objednatele. Pro provádění projektového řízení je nutné, aby Objednatel jmenoval v souladu s navrženou organizační strukturou Projektu kompletní obsazení orgánů Projektu a po dobu realizace Projektu zajistil trvale jejich kompletní obsazení.

b) **Změny požadavků na Projekt**. Změny požadavků Objednatele na Projekt specifikované touto nabídkou, ať už jsou způsobeny čímkoliv (např. změny legislativy, změny v organizaci nebo v jejich prioritách, změny vyžádané jinými subjekty nebo paralelními projekty), mohou mít dopad na termíny plnění, rozsah služeb a technické řešení Projektu. V zájmu včasného a řádného plnění projektu je třeba, aby si Objednatel a jeho zaměstnanci uvědomovali, že riziko vyplývající z těchto změn nese Uchazeč. V zájmu minimalizace dopadu změn je nutné, aby Objednatel poskytoval dodavateli informace o chystaných změnách co nejdříve.

c) Včasné zajištění organizačních opatření a řádný průběh dotčených procesů a činností. Je nutné, aby si Objednatel a jeho zaměstnanci uvědomovali svou odpovědnost za včasné zajištění organizačních opatření na své straně tak, aby realizace veřejné zakázky mohla probíhat dle harmonogramu. Pro úspěšnou realizaci projektu je nezbytná součinnost třetích

stran, spolupůsobících na projektu Objednatele, se kterými nemá Uchazeč uzavřenou přímou Smlouvu nebo dohodu o spolupráci.

d) Součinnost při změnovém a akceptačním řízení. Je třeba, aby zaměstnanci Objednatele důsledně respektovali pravidla změnového řízení a akceptací jednotlivých fází projektového plánu.

Komunikace napříč projektovou strukturou bude zajištěna prostřednictvím organizace pravidelných jednání na jednotlivých řídicích úrovních (jednání Řídicího výboru, pracovní schůzky realizačních týmů atp.), na která budou dle potřeb a požadavků Objednatele přizváni také popřípadě další zapojené subjekty. Vzhledem k rozsáhlosti projektu Uchazeč navrhuje pro zabezpečení šíření informací o projektu zpracování komunikační strategie, která je popsána v následující kapitole.

Hlavním nástrojem pro sdílení veškerých výstupů Projektu (jak pracovních/průběžných verzí, tak i akceptovaných dokumentů) bude tzv. úložiště. Komunikace o stavu Projektu a dílčích výstupech směrem k Objednateli pak bude probíhat formou workshop.

3.2.7.7 Součinnost Uchazeče služeb Prostředí

Navržený způsob poskytování služeb řízení bezpečnostního monitoringu

3.3 Služba „BS03_Bezpečnostní monitoring“

3.3.1 Detailní návrh řešení

Systém **IBM Security QRadar** verze 7.2.4 v provedení SIEM ALL-IN ONE poskytuje v rámci několika licencí funkce ***Log Managementu***, ***Security Information and Event Managementu*** (SIEM) a **Risk&Vulnerability Management**. Funkce pro detekci zranitelností na úrovni infrastruktury se vyznačuje pokročilou správou zranitelností (QRadar Vulnerability Management) vůči evidovaným aktivům s možností napojení na *Center for Internet Security* (CIS[1]). Dále je možné řídit skenování infrastruktury na detekci nových zranitelností a jejich lokalizaci v prostředí Objednatele.
QRadar Log management je schopen provádět sběr logů z mnoha tříd zařízení IT infrastruktury, bezpečnostních informací, informací o zranitelnostech a podobně. Tato data je možno archivovat, dle několika retenčních politik a opakovaně k nim v budoucnu přistupovat. Nad uloženými (případně dlouhodobě archivovanými daty) na lokálních uložištích je možno provádět pokročilou bezpečnostní analýzu.

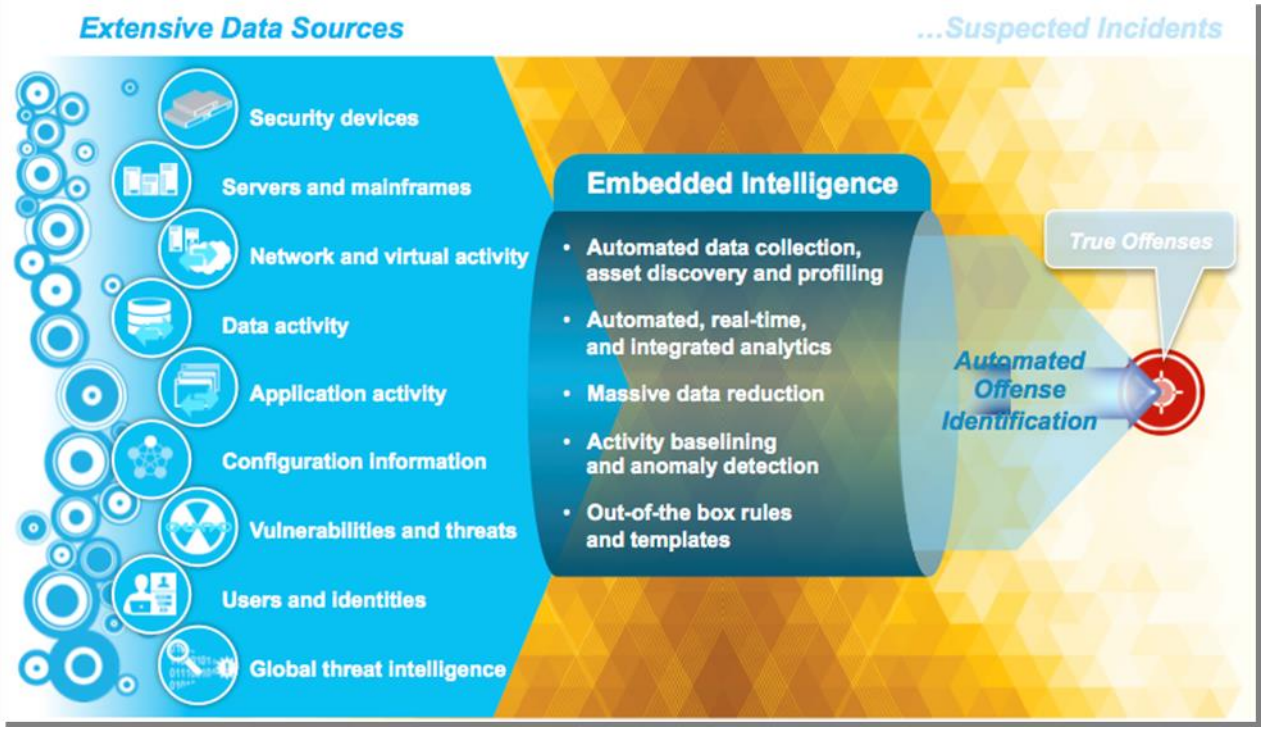
Velmi podstatnou funkcí QRADAR je schopnost modulu *QRadar QFlow Collector* pro sběr záznamů o datových tocích (flow) na úrovni OSI L4 (například formát NetFlow, IPFIX) a dokonce také na OSI L7 (pomocí specializovaných HW nebo SW sond). Sesbírané informace o tocích jsou zpracovány v Network Behavior Anomaly modulu, a získané události je pak možno korelovat se sesbíranými logy ze systémů a aplikací. Tím lze provádět nad flow událostmi další analýzu nebo ustanovit přesnější profil aktiv na základě jejich chování v infrastruktuře. Díky řešení QRadar je možno provádět detekci anomálního chování v reálném čase, včetně kontextuálních anomálií (čím více tříd informací QRadar integruje a přidává do analýzy, tím je potom možno očekávat bohatší a přesnější výstup). Řešení je tak schopno zpracovávat enormní množství informací a z nich vytvářet jednotky vysoce prioritizovaných událostí. Klient je tak schopen zavést IBM QRadar bez nutnosti nasazení dalšího IT personálu.

Specifickým modulem je *QRadar Incident Forensics*, který je primárně určen k pokročilé analýze detekovaných anomálií a incidentů v rámci workflow Incident Response. Umožňuje analytikům získávat nad událostmi přehled jak z pohledu časového kontextu, tak i z pohledu kontextu četnosti, historie, vektoru děje (interní/externí), původce/oběti děje. Pro takto koncipované vyšetřování umožňuje zachytávat datové pakety (Native Packet Capture (PCAP)) a získat tím nejhlubší možný pohled do infrastruktury Objednatele. Výhodou je jednotné prostředí a jednotný pohled na události napříč Incident response týmem. V důsledku se tak jednotlivé kompetentní osoby zabývají výhradně relevantními fakty, nikoliv spekulativními emocemi.

Neopomenutelnou funkcionalitou je *QRADAR API*, které umožňuje napojení produktů třetích stran k informacím SIEM. Bezpečnostní monitoring nemůže být koncipován jako „ostrov“ stojící mimo sledované prostředí, ale naopak je bezpečnost je integrální součástí ICT služby, tak i integrální

[1] http://www.cisecurity.org - organizace standardizující měření kvality a efektivity procesů Vulnerability&Patch management.

součástí infrastruktury. QRADAR API umožňuje bezpečný a řízený přístup k interním informacím SIEM. Využívá se k napojení na middleware prostředí k zajištění akktualizace evidovaných Aktiv nebo k propojení eskalačních mechanismů SIEM s prostředím Objednavatele. Přístup skrze QRADAR API je auditován interním mechanismem SIEM.



Obrázek 10: Princip fungování SIEM systému

Řešení IBM je koncipováno tak, aby bylo již od začátku schopno přijímat maximální množství tříd logů, bezpečnostních informací a dalších. QRadar podporuje množství obecných a specializovaných protokolů a aplikací. U aplikací nebo zdrojů logů, které podporovány nejsou má klient možnost zvolit relativně snadný způsob tvorby vlastního „konektoru“ podle přiloženého návodu.

Kromě logů je QRadar schopen v rámci stejné platformy sbírat, zpracovávat a archivovat záznamy o síťových tocích (flow). Zde je možno zajistit import již vygenerovaných záznamů o flow z aktivních síťových prvků (routery, switche) nebo zařadit speciální flow collector. Jednou z největších výhod nasazení Qflow sondy je, že formát Qflow poskytuje informace i o aktivitě na 7. vrstvě modelu OSI (nejen do vrstvy OSI L4, jako tomu je u formátů typu NetFlow) a dovoluje do analýzy přidat informace o konkrétní využívané aplikaci a zasílaných datech.

Schopnost korelace logů a záznamů o tocích až na OSI L7 je jednou z velkých výhod Qradaru oproti konkurenčním řešením.

Rodina IBM QRadar je modulární platforma pro komplexní pojetí bezpečnosti. Základním modulem je modul QRadar Log Manager. Ten zabezpečuje technický sběr logů, jejich přijetí, porozumnění a bezpečné uložení. V logách lze vyhledávat pomocí uživatelské konzole.

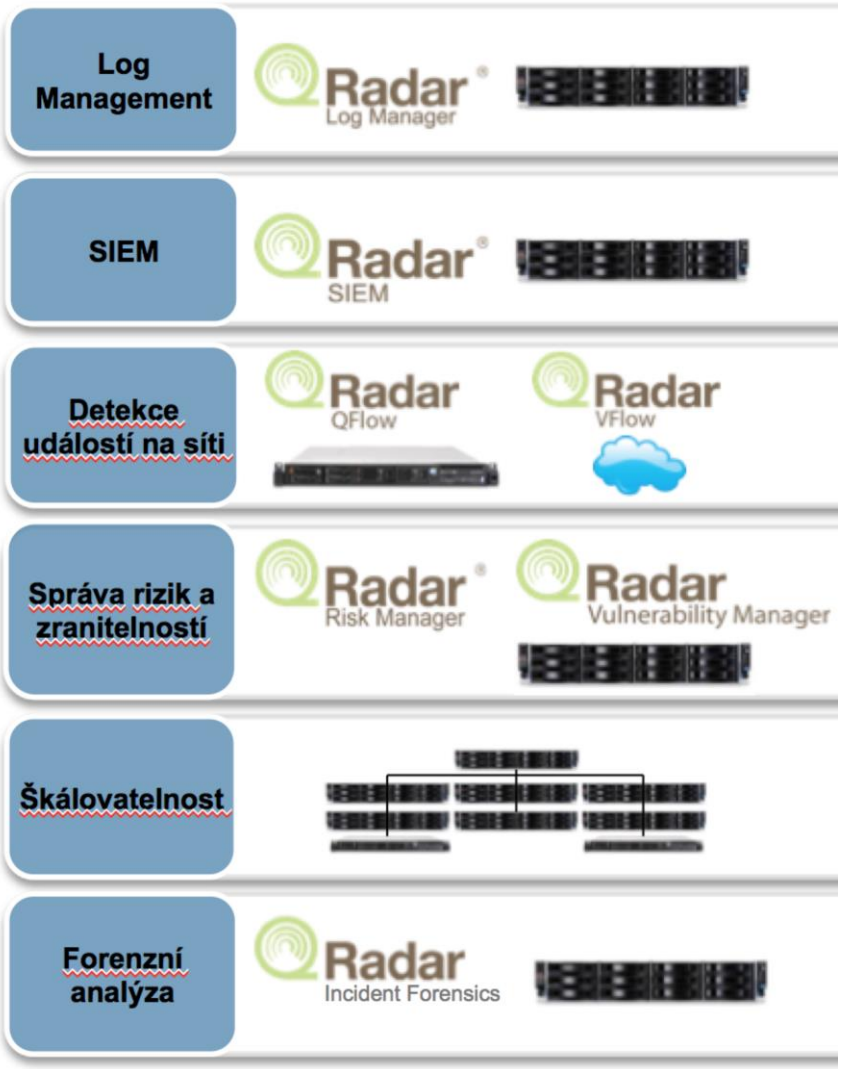
Druhým nástupným modulem je modul QRadar SIEM. Staví na datech z Log Manamentu a přidává systému logiku. Modul obsahuje sadu pravidel, které automatizovaně pracují s přicházejícími logy a detekuje bezpečnostní incidenty. Incidenty poté prioritizuje dle závažnosti a dopadu pro danou konkrétní organizaci. Platforma QRadar ale nekončí tam, co jiné SIEM systémy. Nad modul SIEM

logicky mohou navazovat doplňující moduly z celé bezpečnostní platformy tak, aby daná organizace disponovala pokročilou detekcí hrozeb v cyber prostoru.

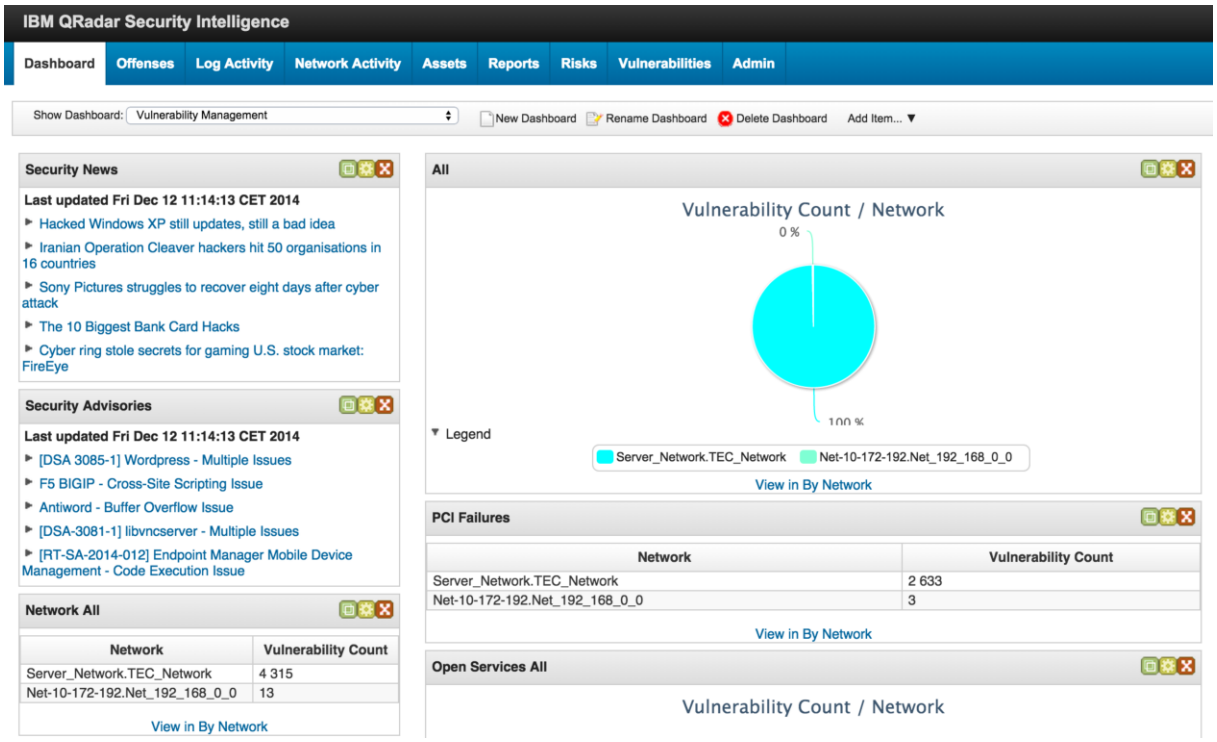
Prvním doplňujícím modulem je detekce zranitelností (QRadar Vulnerability Manager). Ten je nativní součástí platformy a doplňuje informace o konkrétních verzích software a hardware v infrastruktuře, konkrétních zranitelnostech daných verzí apod. Tím řešení poskytuje přesnější detekci hrozeb (co je hrozbou pro jednu organizaci nemusí být pro druhou).

Druhým doplňujícím modulem je analýza rizik (QRadar Risk Manager). Tento modul umožňuje pro bezpečnostní techniky modelovat dopady konkrétní hrozby do organizaceještě než skutečně nastane. Tím je například možné se připravit na veřejně známou hrozbu ještě než bude použita přímo proti konkrétní organizaci.

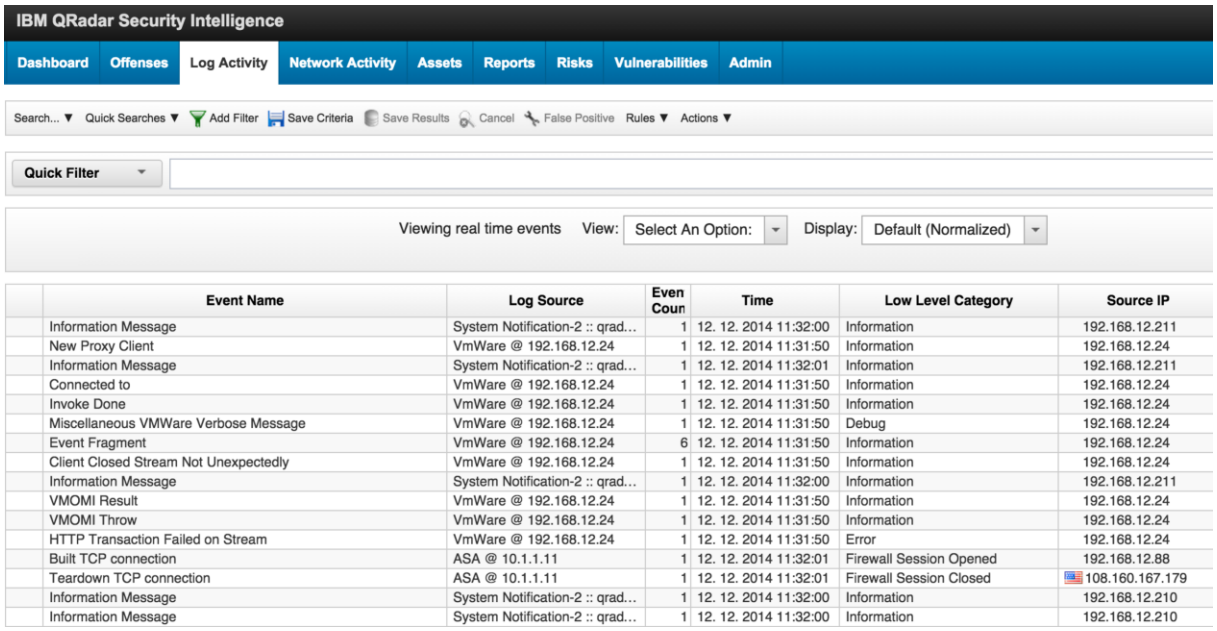
Posledním doplňujícím modulem je forenzní vyšetřování (QRadar Incident Forensics). V případě, že SIEM systém detekuje bezpečnostní incident je nutné takový vyšetřit a přesně zjistit, co se stalo. To není snadné ani v případě, kdy již SIEM zaznaměná řadu informací o incidentu. Modul forenzní analýzy poskytuje bezpečnostnímu technikovi nástroj pro detailní vyhledávání ve veškerých datech a jejich spojování do souvislostí. Tím například lze odhalit případ, kdy incident nastal detekováním malware v interní síti. Forenzně poté lze odhalit odkud došlo k nákaze (z jaké stránky například) a dokonce i zrekonstruovat podobu HTML stránky i přes to, že již z ní byla nákaza odstraněna provozovatelem.



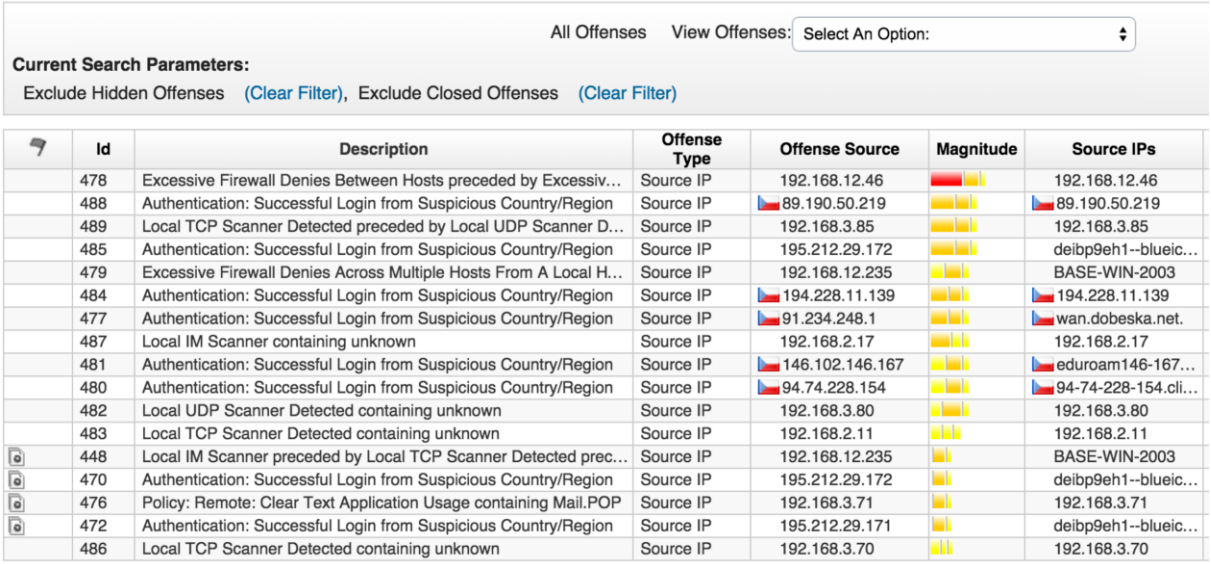
Obrázek 11: Jednotlivé moduly platformy IBM QRadar



Obrázek 12: Hlavní prehledová obrazovka



Obrázek 13: Ukázka přehledu posledních logů zaznamenaných v systému



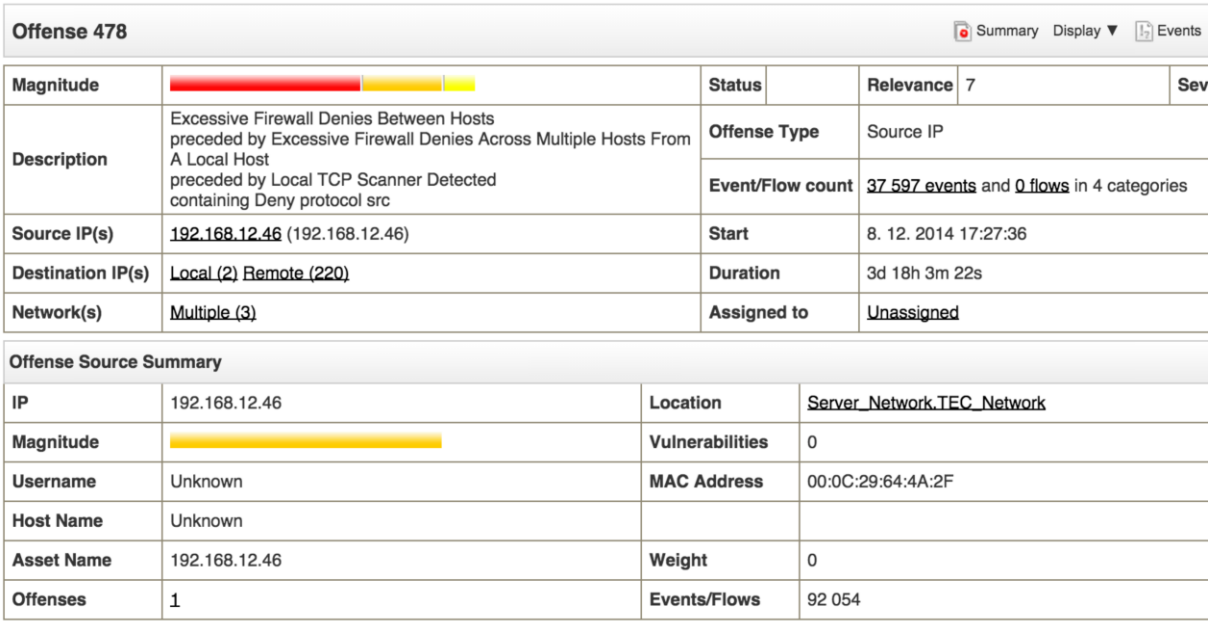
All Offenses View Offenses: Select An Option:

Current Search Parameters:

Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs
478	Excessive Firewall Denies Between Hosts preceded by Excessiv...	Source IP	192.168.12.46		192.168.12.46
488	Authentication: Successful Login from Suspicious Country/Region	Source IP	89.190.50.219		89.190.50.219
489	Local TCP Scanner Detected preceded by Local UDP Scanner D...	Source IP	192.168.3.85		192.168.3.85
485	Authentication: Successful Login from Suspicious Country/Region	Source IP	195.212.29.172		deibp9eh1--blueic...
479	Excessive Firewall Denies Across Multiple Hosts From A Local H...	Source IP	192.168.12.235		BASE-WIN-2003
484	Authentication: Successful Login from Suspicious Country/Region	Source IP	194.228.11.139		194.228.11.139
477	Authentication: Successful Login from Suspicious Country/Region	Source IP	91.234.248.1		wan.dobeska.net.
487	Local IM Scanner containing unknown	Source IP	192.168.2.17		192.168.2.17
481	Authentication: Successful Login from Suspicious Country/Region	Source IP	146.102.146.167		eduroam146-167...
480	Authentication: Successful Login from Suspicious Country/Region	Source IP	94.74.228.154		94-74-228-154.cli...
482	Local UDP Scanner Detected containing unknown	Source IP	192.168.3.80		192.168.3.80
483	Local TCP Scanner Detected containing unknown	Source IP	192.168.2.11		192.168.2.11
448	Local IM Scanner preceded by Local TCP Scanner Detected prec...	Source IP	192.168.12.235		BASE-WIN-2003
470	Authentication: Successful Login from Suspicious Country/Region	Source IP	195.212.29.172		deibp9eh1--blueic...
476	Policy: Remote: Clear Text Application Usage containing Mail.POP	Source IP	192.168.3.71		192.168.3.71
472	Authentication: Successful Login from Suspicious Country/Region	Source IP	195.212.29.171		deibp9eh1--blueic...
486	Local TCP Scanner Detected containing unknown	Source IP	192.168.3.70		192.168.3.70

Obrázek 14: Ukázka přehledu identifikovaných incidentů



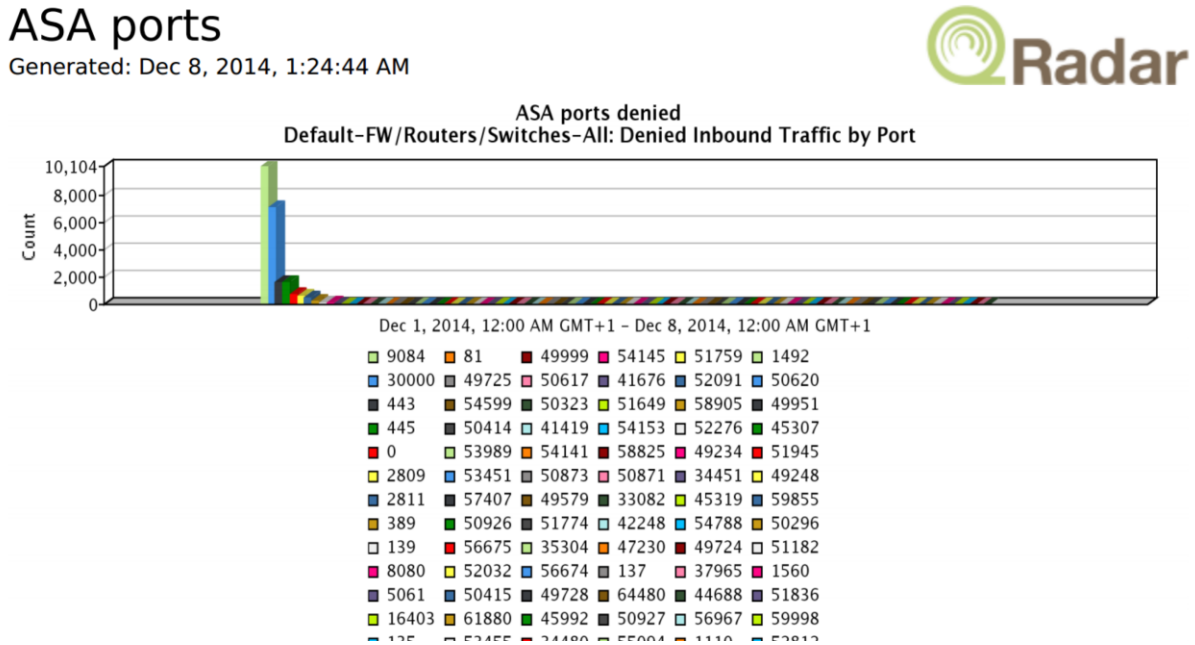
Offense 478 Summary Display ▼ Events

Magnitude		**Status**		**Relevance**	7
Description	Excessive Firewall Denies Between Hosts preceded by Excessive Firewall Denies Across Multiple Hosts From A Local Host preceded by Local TCP Scanner Detected containing Deny protocol src	**Offense Type**	Source IP		
		Event/Flow count	37 597 events and 0 flows in 4 categories		
Source IP(s)	192.168.12.46 (192.168.12.46)	**Start**	8. 12. 2014 17:27:36		
Destination IP(s)	Local (2) Remote (220)	**Duration**	3d 18h 3m 22s		
Network(s)	Multiple (3)	**Assigned to**	Unassigned		

Offense Source Summary

IP	192.168.12.46	**Location**	Server_Network.TEC_Network
Magnitude		**Vulnerabilities**	0
Username	Unknown	**MAC Address**	00:0C:29:64:4A:2F
Host Name	Unknown		
Asset Name	192.168.12.46	**Weight**	0
Offenses	1	**Events/Flows**	92 054

Obrázek 15: Ukázka části detailu jednoho incidentu



Obrázek 16: Ukázka reportu nad firewally Cisco ASA

Příchozí logy do zařízení QRadar jsou automaticky, v době vstupu do zařízení, opatřeny tzv. hash záznamem, který je otiskem daného logu. Hash záznam reprezentuje vlastní log 1:1. Kdykoliv později je poté možné zkontrolovat databázi uložených logů oproti jejich vygenerovaným hash záznamům a tím zjistit, zda nějaké logy nechybí nebo zda nedošlo k jejich změně. Tím je zajištěna integrita a správnost logů v Qradaru uložených.

3.3.1.1 Integrace s centrálním monitorovacím systémem

Napojení na zažízení ArcSight pro monitorování komponent, kde již tento systém běží, je snadné. ArcSight bude nastaven tak, aby přijmuté logy v nezměněné formě přeposílal na nový centrální QRadar systém. Tím bude jeho funkce pouze jako přeposílač. Veškeré další operace (přijmutí logu, porozumnění, kategorizace, uložení, korelace) budou realizovány v ráci řešení QRadar.

3.3.1.2 Harmonogram implementace

Implementace navrhovaného řešení probíhá ze zkušenosti s obdobných projektů v následujících fázích:

1. Vstupní analýza
   a) Detailní analýza prostředí na potřeby Log management, tj. počty jednotlivých komponent pro dohledování, sběr technických parametrů (protokol, typ logu), stanovení typického objemu log dat za den.
   b) Zpracování získaných dat o Log management procesu a stanovení základních tříd Data_retention
   c) Stanovení základních kategorií log dat pro směrování do SIEM modulu – bezpečnostní log data, log data s vlivem na služby, log data s vlivem na aplikace, log data s vlivem na systémy.
   d) Analýza aktiv a stanovení základních kategorií aktiv (Assets) – Analýza IP adresního plánu a sledovaného prostředí. Zjištěna aktiva budou rozložena do tříd client, server,

network, storage s přidělením hodnoty aktiva ve stupních critical, important, normal, low.

e) Ohodnocení aktiv v kontextu jimi obsažených/zpracovávaných informací a dat vázaných na zákony ČR (Spisová služba, Ochrana osobních údajů) a legislativu Objednatele (Důvěrné informace, Monetizační informace).
f) Analýza datových toků a pravidel na perimetrech datových sítí (firewallů) – analýza architektury datových komunikací, kdo může s kým komunikovat, kdo je omezen komunikovat, analýza nastavení systémové politiky detekčních systémů IDS/IPS.
g) Analýza potřeb výstupních informací procesů Configuration management (potřeby na nastavení Dasboard a nastavení Reportů o kondici aktiv – zranitelnosti, počet změn sledovaného prostředí, aktuální verze SW), Incident Response (potřeby na nastavení Dasboard a nastavení Reportů o počtu incidentů, trendy, compliance reporting).

2. Instalace QRadar do prostředí
   a) Vlastní instalace HW/SW SIEM All-in One .
   b) nastavení síťové komunikace (přidělení IP adres, nastavení DNS, NTP), nastavení přístupů pro obsluhu.
   c) Nastavení konfigurace pro sběr log dat.
   d) Nastavení konfigurace pro sběr flow.
   e) Nastavení síťové komunikace s LDAP.
   f) Nastavení základní eskalace o provozních anomáliích.

3. Nastavení Assesment and Risk management
   a) Nastavení tříd aktiv
   b) Nastavení profilů aktiv
   c) Vložení aktiv do profilů, tříd a přidělení odpovídající hodnoty.
   d) Nastavení základních profilů skenování zranitelností pro třídy aktiv client, server.
   e) Možnosti a nastavení Reconciliace aktiv. Detekce konfiguračních změn, detekce přidaného/odebraného aktiva.
   f) Nastavení základní eskalace o provozních anomáliích sběru zranitelností.

4. Nastavení QFlow Collector
   a) Konfigurace pasivního sběru (TAP), sondy, kolektoru.
   b) Napojení dat z flow na SIEM.
   c) Nastavení základní eskalace o provozních anomáliích sběru flow.

5. Nastavení Log management
   a) Nastavení příjmu log dat.
   b) Ověření ovládání dálkové správy sběru log dat.
   c) Detailní nastavení konektorů pro sběr logů z definovaných komponent.
   d) Vývoj a doplnění konektorů pro nestandardní zařízení a formáty log dat.
   e) Nastavení základní Data_retention politiky.
   f) Nastavení základní eskalace o provozních anomáliích sběru log dat.

6. Nastavení korelačních pravidel na SIEM
   a) Nastavení základních továrních korelačních pravidel.
   b) Detailní nastavení korelačních pravidel.
   c) Doplnění individuálních korelačních pravidel pro specifické požadavky.
   d) Nastavení sledování performance a capacity monitoringu s eskalací o provozních anomáliích SIEM.

7. Vytvoření Dasboard profilů a reportů
   a) Aktivace generování továrních reportů.
   b) Tvorba výstupních sestav dle požadavků Objednatele.
   c) Uzpůsobení Dashboard potřebám Objednatele.

8. Ladění False-positives Alarms
   a) Nastavení eskalace z korelačních pravidel dle potřeb procesu Incident Response (eskalační matice, způsob eskalace).
   b) Ladění detekce událostí na skutečném provozu formou sledování výpočtu Event score - Magnitude, hodnoty aktiv v detekované události, významu zranitelností v detekované události, četnosti zachycených událostí – treshold pro alert.
   c) Detekce úspěšnosti konektorů ve zpracování log dat – detekce chyb zpracování log dat.

Tabulka 11: Implementace služby BS_03

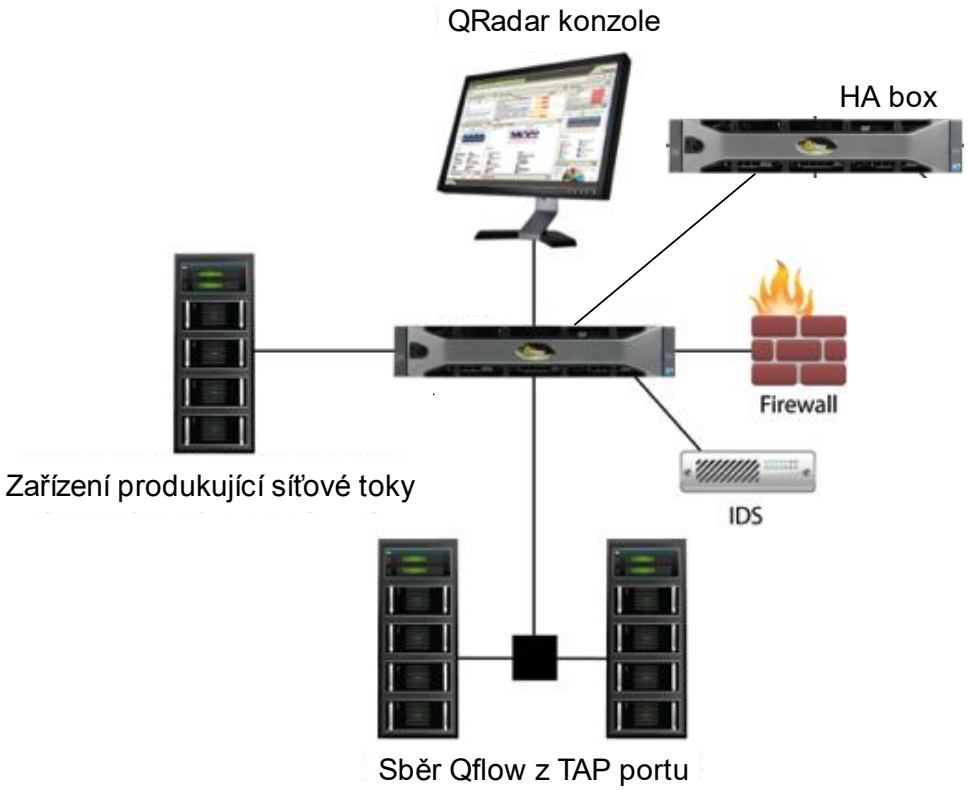
Implementační plán – řízení bezpečnostního monitoringu			
Kód	**Aktivita**	**Očekávaný výstup**	**Termín plnění nebo důležitý milník projektu**
1.	Vstupní analýza	Základní evidence pro analýzu identifikovaná v průběhu plnění	Akceptace evidence
2.	Příprava dokumentace Příprava detailních instrukcí pro administrátory MMR, kteří nastaví posílání logů dle specifikovaných parametrů.	Základní evidence pro analýzu identifikovaná v průběhu plnění	Klíčové dokumenty
3.	Fyzické připojení, rozchození a nastavení SW a HW Vlastní instalace HW do datového centra, nastavení potřebných služeb na úrovni infrastruktur, nastavení přítupů pro obsluhu.	Základní evidence pro analýzu identifikovaná v průběhu plnění	Dokumentace nastavení a akceptace
4.	Nastavení zdrojů, napojení na SIEM/LM Detailní nastavení konektorů pro sběr logů z definovaných komponent. Vývoj a doplnění konektorů na nestandardní zařízení.	Základní evidence pro analýzu identifikovaná v průběhu plnění	Technická architektura
5	Vytvoření uživatelů, práva Tvorba uživatelů systému, individuální nastavení prostředí, přístupová hesla.	Základní evidence pro analýzu identifikovaná v průběhu plnění	Přístupové listy
6.	Nastavení korelačních pravidel Detailní nstavení koleačních pravidel, doplnění individuálních.	Základní evidence pro analýzu identifikovaná v průběhu plnění	Akceptace korelačních pravidel

7.	Vytvoření reportů Tvorba výstupních sestav dle požadavků	Základní evidence pro analýzu identifikovaná v průběhu plnění	Akceptace sady report
8.	Ladění false positives Ladění detekce událostí na skutečném provozu, doladění anomálií.	Základní evidence pro analýzu identifikovaná v průběhu plnění	Ladění provozní parametrů
9.	Školení adminů a uživatelů Uživatelské školení skutečného provedení pro obsluhu a administrátory řešení.	Základní evidence pro analýzu identifikovaná v průběhu plnění	Školení – postimplementační fáze

3.3.1.3 Architektura vyhodnocovacího centra

Systém je možno nasadit v podobě jedné HW appliance, která pokrývá všechny výše zmíněné procesy. Taková appliance je označena jako All-In-One.

Obrázek 17: Appliance QRadar 3105



Obrázek 18: Architektura All-In-One

3.3.1.3.1 HW architektura

Obrázek 18 ukazuje navrhované zapojení prvků IBM QRadar SIEM. V principu obsahuje 2 HW boxy (primární a zálohu). Do primárního jsou připojena všechna monitorovaná zařízení. Záložní box je nepřetržitě synchropnizován s primárním a dojde–li k neočekávanému výpadku primárního boxu, jeho funkci kamžitě přebírá box záložní.

Dodávka předpokládá HW dle tabulky. (Dodávka obsahuje 2x server dle specifikací)

Tabulka 12: Specifikace zařízení

Specifikace	All-in-one 3105
Model	xSeries 3650 M4 BD
Rozměry	29.5"D x 17.6" W x 3.4" H
Váha	52 lbs
CPU	2 x E5-2620 V2, 2.1–2.6 GHz, 6 Core, 15MB Cache 12MB Cache 1066MHz 80w
Paměť	64 GB 8 x 8GB 1600 MHz RDIMM
Úložiště	9 x 3.5” 1TB 7.2K rpm NL SAS Total Raw: 9TB Total Usable: 6.2TB (Raid 5) RAID Controller: ServeRaid M5110 + 512 MB Flash Cache

Síťové adaptéry	2 x 10/100/1000 Base-T network monitoring interfaces 1 x 10/100/1000 Base-T Qradar management interface 1 x 10/100/1000 Base-T integrated system management Interface (IMM) 1 x 2 port 10Gbps Intel X520 SPF+ Embedded Adapter
Napájení	Dual Redundant 750 W AC Power Supply

3.3.1.3.2 SW architektura

Zařízení IBM QRadar SIEM je licencovaný produkt. Dodávka předpokládá dodání licencí dle tabulky. Lience již obsahují v pořizovací ceně podporu výrobce (infolinka pro technické problémy, otázky 24x7)

Tabulka 13: Specifikace SW

1x	D0V5HLL	IBM security qradar siem all-in-one 31xx install license
1x	D0WPFLL	IBM security qradar siem all-in-one 31xx failover feature install license
1x	D0WTULL	IBM Security qradar SIEM Event Capacity Increase from 1K to 2.5K EPS Install License
1x	D0V5JLL	IBM Security qradar SIEM Event Capacity Pack Increase of 2.5K EPS Install License
2x	D14R6LL	IBM security qradar core appliance xx05 G2 appliance install appliance

3.3.1.3.3 Škálovatelnost řešení

Řešení je navrženo tak, aby bylo plně škálovatelné dle potřeby Objednatele. HW a SW architektura základní dodávky je navržena pro splnění následujících parametrů:

- 5000 EPS trvale
- až 750 jednotlivých monitorovaných zařízení

V případě potřeby je možné parametry rozšířit dokoupení patřičné SW licence a HW serveru. Řešení je navíc připraveno na krátkodobé velké zatížení bez nutnosti dodatečných nákladů. Pokud provoz překročí parametr 5000 EPS, zařízení provoz nad tuto kapacitu ukládá a dále zpracovává ve chvíli, kdy provoz opět poklesne. Existuje zde pouze technické omezení, vyplývající z velikosti paměti cache, kam jsou události před zpracováním ukládány. Pro běžný provoz je tím zabezpečen beztrátový sběr logů při kolísavém provozu.

3.3.2 Popis procesů bezpečnostního monitoringu

Uchazeč bude zajišťovat a provádět průběžný bezpečnostní monitoring systému MS2014+ v souladu s požadavky/rozsahem činností zadávací dokumentace Objednatele.

Zajištění služby **BS003 – Bezpečnostní monitoring** je z pohledu Uchazeč koncipováno orchestrací několika vzájemně synergických procesů:

- Log management
- Network Behavioral Analyse (NBA)
- SIEM
- Configuration management – Assesment
- Risk management – Vulnerability&Patch managemenent
- Incident Response

Pro výše uvedené procesy jsou procesním vstupem *log data z prostředí infrastruktury* Objednatele a *informace o sledovaném prostředí* Objednatele. Jednotlivými účastníky procesů je pak posuzována relevantnost získaných vstupních dat se skutečností. V případě zjištěných nesouladů neprodleně ohlašovat zjištěné odchylky do procesu Incident Response.

Z několika leté praxe provozu SIEM systémů, spatřuje Uchazeč pro efektivní fungování služby **BS003 – Bezpečnostní monitoring** kvalitativní parametr **False-pozitive alarms,** kde je klíčová důvěryhodnost získaných informací, se kterými pracuje SIEM a obslužný personál. Ostatní parametry služby BS003 jsou kvantitavní.

Uchazeč v uvedeném kontextu na důraz zajištění kvality provozu SIEM rozděluje získání vstupních procesních dat do dvou skupin:

1. Data o kybernetickém prostředí – *log data a atributová data z prostředí* jsou získávány přímo ze sledovaného prostředí skrze dedikovaná Reconciliation workflow. Log data jsou zpracovány procesy Log management (archivace) a SIEM (analýza). Atributová data jsou zpracovány v Asset managementu a Configuration managementu. Specifickou úlohou je zpracování komunikačních flow, které jsou analyzovány na detekci výskytu anomálií (NBA) a tvorbu atributových dat pro Asset management a Configuration management.
2. Data o reálném prostředí – *informace o sledovaném prostředí* jsou atributová data popisující služby, komponenty a funkce sledovaného prostředí a jsou získávány Objednatelem pověřenými osobami nebo skrze integrační prostředí typu middleware v rámci smluvně stanoveného intervalu. Tyto data jsou udržována v rámci procesu Configuration management v Configurační databázi (CMDB), odkud jsou replikována do SIEM.

Bez průběžné aktualizace *dat o kybernetickém a reálném prostředí* nelze zajišťovat kvalitní výkon provozu SIEM a kvalitní službu **BS003 – Bezpečnostní monitoring.** Nízká kvalita vstupních dat od Objednatele, případně nedostupnost dat o reálném prostředí Objednatele, souvisí s výsledně obdrženou kvalitou služby BS003, tj. **pro Objednatele nesmí být klíčová jen a pouze dostupnost služby BS003**, ale musí být důležitá i kvalita dodaných dat do SIEM.

3.3.3 Provádění průběžného monitoringu

Systémová appliance QRADAR All-in-one obsahuje servisní management síťové rozhraní, které umožňuje sběr dat o kondici hardware prostřednictvím protokolů SNMP a Syslog. Taktéž umožňuje vzdálenou správu ke konfiguraci hardware komponent a BIOS nastavení appliance. Uchazeč považuje za nezbytné napojení appliance QRADAR All-in-one na provozní monitoring Objednatele a přístup eskalací do prostředí Uchazeč nebo přístup *Operátor monitoringu* do provozního monitoringu Objednatele. Uchazeč dekomponuje provádění průběžného monitoringu do následujících podkapitol.

3.1.1.1 Log management

Pro proces Log managementu Uchazeč preferuje členění do následujících oblastí, viz Obrázek 19:

- **Business oblast** – obsahuje vlastní proces Log managementu a workflow pro zajištění shody, zvyšování výkonu okolních procesů Objednatele a měření stanovených metrik.
- **Analytická oblast** – pravidelné i ad-hoc činnosti spojené s detekcí anomálií a určením příčin událostí a incidentů.
- **Technologická oblast** – obsahuje návrh a popis *architektury*, kooperaci s procesem *Configuration management* a workflow pro *správu systémů* Log managementu.
- **Provozní oblast** – obsahuje workflow *Sběru log záznamů*, workflow pro *Monitoring* komponent infrastruktury Log managementu a *Procvičování* eskalačních workflow pro případ incidentu.

Průběžný monitoring nástroje Log management je zajišťován rolí *Operátor monitoringu*. Sleduje kolik logů vchází do QRADAR appliance a s jakou úspěšností jsou log data zpracována kolektory.

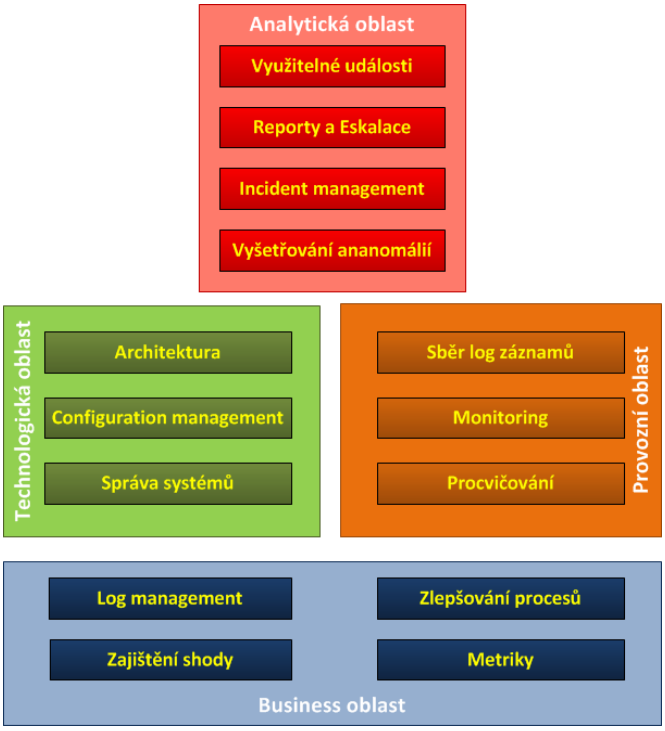
Operátorem monitoringu jsou prokazatelně hlášeny na *Specialista Monitoringu* následující události:

- Výskyty nových formátů log dat z evidovaných zdrojů log dat.
- Detekce chyb zpracování log dat jednotlivými kolektorem.
- Detekce nového zdroje log dat.
- Detekce změn trendu ve sběru log dat – nárůst o více než 2x, pokles o více než 60%.
- Detekce přesahu kapacitních parametrů – storage (volné místo méně něž 10%), CPU(nad 60%), RAM (méně než 25%).

Bezpečnostní monitoring bude mít nastavenu automatickou eskalaci na kompetentní role *Operátorem monitoringu* a *Specialista Monitoringu* při výše uvedených situacích.

Monitoring Log managementu z pohledu procesu je zajišťován rolí *Specialista monitoringu*, který se zabývá:

- Kontrolou procesu a workflow Log managementu (tj. plánování, realizaci, kontrolu souladu, měření kondice) ve shodě s požadavky Objednatele.
- Kontrolou politiky Log managementu – Nastavení a kontrola archivační politiky dle parametrů Data retention ve vazbě na zdroje log, hodnotu aktiv a povahu obsažených informací v log datech.
- Nastavením prioritizace log dat – Za stanovení doby uchování log záznamu dle jejich povahy a procesní/legislativní klasifikace Objednatele. Určení povahy informací provádí v kontextu obsažených informací v log datech a jejich kategorizace na provozní a bezpečnostní povahu.



Obrázek 19: Obrázek 19: Oblasti Log Managementu

- Kontrolou integračních rozhraní – kontrola zda veškerá log data bezpečnostní povahy přechází do SIEM. Kontrola QRADAR API rozhraní – export, import dat. Kontrola jednotného času v log datech a zdrojích log dat.
- Komunikací se *Specialistou Bezpečnostního Monitoringu* – konzultace nad korelačními pravidly a potřebnými informacemi v log datech.
- Komunikací s *Operátorem monitoringu* – konzultace o ohlášených změnách v konfiguraci aktiv a ve zdrojích log dat. Typicky změna kondice aktiv (stop, start, restart), update nastavení, upgrade verze.
- Provozem QRADAR v anomálních stavech – zajištění přípravných a následných činnosti v případě odstávky datové/síťové infrastruktury a opětovného spuštění.
- Provozem QRADAR v servisních stavech – zajištění profylaktických činností, update nastavení, upgrade komponent QRADAR, patch management operačního systému appliance QRADAR.

Předmětem zájmu Log managementu, v rámci zajištění služby Uchazečem, jsou následující typy log záznamů:

- **Přístup**. *Kdo* nebo *Co* využívá službu Objednatele.
- **Změna konfigurace** nebo **sledování**. *Jak* a *Kdy* došlo ke změně služby Objednatele.
- **Závada**. *Čas*, kdy služba Objednatele selhala.
- **Využití zdrojů**. Kolik kapacity se používá sledovanou službou Objednatele.
- **Bezpečnostní události**. *Kdy* a *Jaké* činnosti vyvstaly během incidentu u Objednatele.
- **Aktivity uživatelů.** *Jak* a *Co* uživatelé dělají se službami Objednatele.

Předmětem zájmu Log managementu, v rámci zajištění služby Uchazeče, jsou následující zdroje log záznamů:

- **Aplikace** - sběru log záznamů podléhají aplikace s vlivem na core-procesy Objednatele, bezpečnost Objednatele nebo aplikace pracující s klasifikovanými informacemi[2].
- **Databáze** - sběru log záznamů podléhají databáze s vlivem na core-procesy Objednatele, bezpečnost Objednatele nebo aplikace pracující s klasifikovanými informacemi.
- **Systémy** a **storage**
    - sběru log záznamů podléhají následující zařízení:
        - Operační systémy (Windows, Unix)
        - Web servery
        - Tiskové servery
        - Souborové servery
        - Autentizační servery (MS Active Directory, Novell eDirectory,atp.)
        - DHCP servery
        - DNS servery
        - Poštovní servery (SMTP, PostFix,atp.)
        - Centrální storage a NAS zařízení
- **Koncová zařízení**
    - sběru log záznamů podléhají následující zařízení:
        - Stanice – pouze bezpečnostní funkce personálního firewallu, antimalware ochrany.
        - Síťové tiskárny.
        - SmartDevice – Telefony a Tablety.
        - Technologická podpůrná zařízení – UPS, Měřící systémy (Teploměry), atp.
- **Datová síť**
    - sběru log záznamů podléhají následující zařízení:

[2] Obchodní tajemství, osobní údaje, spisová služba, účetní údaje, legislativa EU.

- Routery
- Switche
- Wireless access pointy
- Network-based firewally
- Personální firewally
- Intrusion detection and prevention systems (IPS)
- VoIP Switche
- SAN Switche

- Jednotný čas - je důležité, aby všechny komponenty IT infrastruktury Objednatele měly synchronizovány hodiny. Použití jednotné časové služby3 je vysoce doporučeno a bude sledováno jeho užívání.

Cílem Bezpečnostního monitoringu je zajištění přehledu o bezpečnostní situaci a schopnost určit a lokalizovat anomálii. Pro naplnění uvedeného cíle je klíčová úloha **log dat**. Uchazeč proto prosazuje dobrou praxi již od úrovně provozu Log managementu, který musí být sledován a řízen jak v technologické, tak i v procesní úrovni.

3.3.3.1 Network Behavioral Analyse (NBA)

Systém Network Behavioral Analyse (NBA) slouží k vizualizaci komunikačních vztahů mezi aktivy v komunikační infrastruktuře, a tím může vytvořit dostatečnou úroveň interpretace k rozpoznání útoku a k rozhodnutí o následných protiopatřeních. Systém ukazuje pověřenému uživateli, které aktivum je cílem útoku, popř. Kontext jak k útoku dochází nebo prostřednictvím jakých zdrojů je útok veden.

Průběžný monitoring nástroje NBA je zajišťován rolí *Specialista monitoringu*. Sleduje, kolik flow vchází do QRADAR QFlow a jaké trendy jsou vykazovány jednotlivými profily komunikací, protokolů a aktivy. *Specialista monitoringu* prokazatelně ohlašuje na *Specialistu Bezpečnostního Monitoringu* následující události:

- Výskyty nových komunikačních schématů.
- Detekce změn chování aktiva vůči danému profilu.
- Detekce nového komunikujícího aktiva, které není evidováno.
- Detekce změn trendu komunikací – nárůst o více než 2x, pokles o více než 60%.
- Detekce přesahu kapacitních parametrů – storage (volné místo méně něž 10%), datová síť.
- Detekce selhání sběru flow.

Monitoring NBA bude mít nastavenu automatickou eskalaci na kompetentní role *Specialistu Bezpečnostního Monitoringu, Bezpečnostního specialistu* a *Vedoucího týmu monitoringu a testování* při výše uvedených situacích.

Monitoring NBA z pohledu procesu je zajišťován rolí *Specialista monitoringu*, který se zabývá:

- Kontrolou politiky perimetru datových sítí – Nastavení a kontrola komunikační politiky pro sběr flow.
- Komunikací *Specialistou Bezpečnostního Monitoringu* – konzultace nad korelačními pravidly a potřebnými informacemi ve flow datech.
- Součinnost při hloubkové analýze flow a datových paketů – ovládání modulu *QRadar Incident Forensics* pro potřeby členů Response Teamu.

[3] jako je např. NTP služba

Cílem Bezpečnostního monitoringu je zajištění přehledu o bezpečnostní situaci a schopnost určit a lokalizovat anomálii. Pro naplnění uvedeného cíle je klíčová úloha **sběru flow a jejich správná analýza**. Uchazeč má své know-how, co je efektivní ve sběru flow pro Systém Network Behavioral Analyse. Analýzou získané informace musí být nejen předány do SIEM, ale analyzovány na kontext dotčených aktiv z pohledu jejich významnosti pro Objednatele, tak i na kontext chování aktiva v datové síti (Firewall, Proxy, Web Server, DB Server, atp.). Procesní úroveň řízení NBA spočívá v odpovědné kontrole nastavené politiky, hodnocení detekovaných změn a profesionální komunikaci s ostatním procesními rolemi.

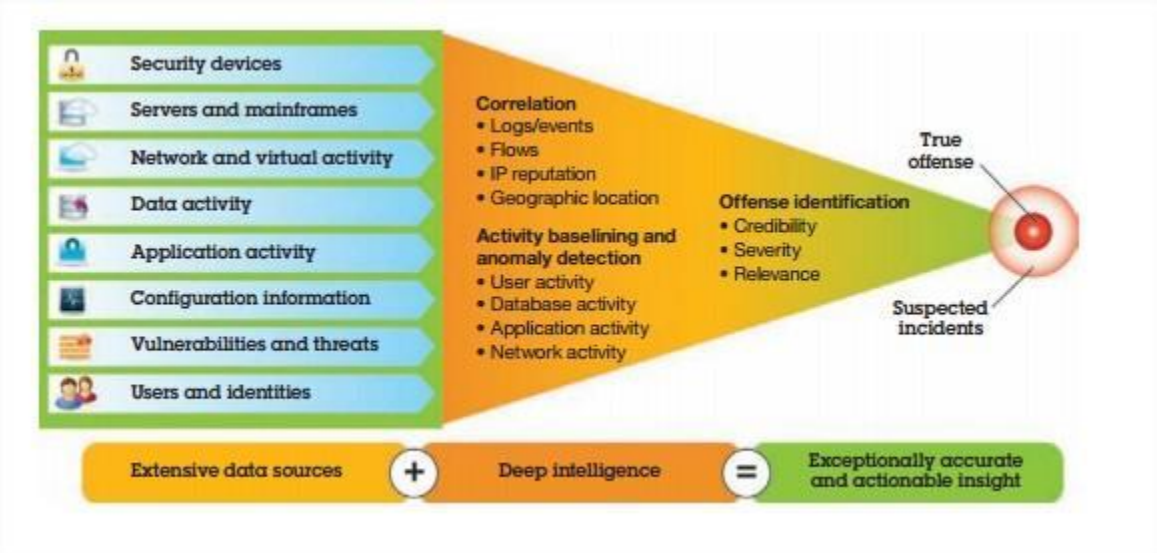
3.1.1.2 SIEM

Infrastruktura Event managementu obvykle obsahuje následující tři úrovně:

Zpracování logových záznamů. První úroveň obsahuje zařízení, která zpracovávají logová data na události. Protože jde o zpracování značného množství dat, tak v této úrovni je více serverů. Jejich úkolem je provést tokenizaci, parsing, normalizaci, taxonomizaci a přenos událostí prostřednictvím datové sítě na analytické servery v druhé úrovni. Současně data událostí jsou uložena v databázových serverech nebo v samostatně určeném databázovém serveru.

Real-time analýza. Druhá úroveň se skládá z jednoho nebo více analytických serverů, které přijímají události ze serverů v první úrovni. Analytické servery obsahují výhradně korelační funkce a jsou výrazně zatíženy na procesor a na operační paměť. Výsledné korelované události jsou uloženy v databázových serverech nebo v samostatně určeném databázovém serveru.

Long-time analýza. Třetí úroveň je ovládací prostředí, které obsahuje administrátorské konzole nebo jednotné grafické rozhraní používané ke sledování událostí a incidentů. Prezentuje výsledky automatizovaných analýz. Prostředí může být také použito pro generování reportovacích sestav, šetření anomálií, ale i pro konfiguraci celého SIEM prostředí. Prostředí umožňuje využít přístupových oprávnění, kterými může být SIEM uživatel omezen jen k vykonání pouze nezbytných funkcí a k přístupu jen příslušných událostí.



Obrázek 20: Filozofie SIEM Q Radar

Průběžný monitoring nástroje SIEM je zajišťován rolí *Operátor monitoringu*. Sleduje události (eventy) zpracovávané v SIEM, kde detekuje a posuzuje bezpečnostní situaci z Dashboardu, především významnost událostí (Magnitude score) a trendy v četnosti výskytů událostí.

Operátor monitoringu prokazatelně ohlašuje na *Specialistu Monitoringu* následující události:

- Disciplinovanou real-time analýzou log dat, především posuzováním výskytu událostí s vysokým Magnitude score.
- Detekce změn trendu ve sběru log dat – nárůst o více než 2x, pokles o více než 60%.
- Detekce přesahu kapacitních parametrů jednotlivých komponent SIEM – storage (volné místo méně něž 10%), CPU(nad 60%), RAM (méně než 25%).

SIEM bude mít nastavenu automatickou eskalaci na kompetentní role *Operátorem monitoringu* a *Specialista Monitoringu* při výše uvedených situacích.

SIEM z pohledu procesu je zajišťován rolí *Specialista monitoringu*, který se zabývá:

- Kontrolou procesu a workflow SIEM (tj. plánování, realizaci, kontrolu souladu, měření kondice) ve shodě s požadavky Objednatele.
- Kontrolou aktuálnosti aktiv a jejich profilů – Nastavení a kontrola hodnoty aktiv. Posuzování množství změn v aktivech při plánovaných změnách Objednatelem v rámci projektových změn infrastruktury. Řešení nesouladů informací o evidovaných aktivech – Reconcialiace.
- Kontrolou nastavené politiky Risk managementu – kontrola nastavení profilů a plánování skenování aktiv na detekci zranitelností.
- Analýzou událostí z NBA – kontrola relevantnosti událostí (False-positive alarm) a analýza dopadů zjištěných informací na bezpečnost aktiv. Posuzování účinosti systémových bezpečnostních politik na firewallech a IDS/IPS.
- Pokročilou long-time analýzou (vizuální analýzy) nad log daty pro úpravu korelačních mechanizmů a také pro účinnou detekci neočekávaných anomálií.
- Sledování efektivnosti korelací (Alert scoring) – kontrola správné detekční citlivosti SIEM na události z pohledu hodnoty aktiva, významu zranitelnosti, severity události, historické četnosti události. Vytváří nebo upravuje korelace dle potřeb Objednatele nebo v reakci na klesající detekční účinnost SIEM.
- Úprava reportů dle potřeby Objednatele.
- Komunikací se *Specialistou Bezpečnostního Monitoringu* – konzultace nad korelačními pravidly a potřebnými informacemi v log datech, flow datech a kontextových informací.
- Komunikací s *Vedoucím týmu monitoringu a testování* – příprava eskalačních scénářů, příprava scénářů pro penetračními testy na kontrolu detekční účinnosti SIEM a prověření efektivity eskalačních workflow.
- Komunikací s Operátorem *monitoringu* řeší anomálie a analyzuje události, ze kterých zakládá incidenty/bezpečnostní incidenty.

Role Specialista Bezpečnostního monitoringu se zabývá:

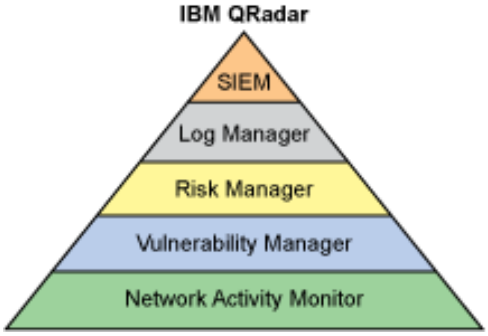
- tvorbou všech typů korelací, ale hlavně pokročilých korelací (korelace incidentů, korelace nesouladů – chyba konfigurace vyvolá jiné události, transakční korelace – změna oprávnění uživatele v kontextu s časovým průběhem jiných dějů v systémech/aplikacích).
- Pokročilou long-time analýzou (vizuální analýzy) nad vybranými log daty pro úpravu korelačních mechanizmů a také pro účinnou detekci neočekávaných anomálií.
- tvorbou všech typů reportů, dle busines potřeb Objednatele.

Role Specialista tester zajišťuje:

- testování nových reportů a korelací před jejich nasazením do produkčního prostředí.
- testování eskalačních workflow
- testování integračních rozhraní

Role *Vedoucí týmu monitoringu a testování* především:

- přiděluje úkoly z vyhodnocených incidentů členům Incident Reponse týmu nebo na ServiceDesk Objednatele .
- řeší kolize priorit úloh k eskalaci v rámci Incident Response a Busines Continuity.
- zajišťuje komunikaci týmu bezpečnostního monitoringu s jinými týmy (CIRT, CSIRT), správci, administrátory, uživateli.



Obrázek 21: Moduly SIEM Q Radar

Cílem Bezpečnostního monitoringu pro SIEM část je:

- sledování zpracování log dat na události, jejich normalizace na standardizované formáty (čas, struktura), taxonomizace událostí (přiřazení události do standardizované kategorie, třídy, oblasti), spojení události s kontextovými informacemi o aktivech, uživatelích a vlivu na business Objednatele,
- zajištění přehledu o bezpečnostní situaci se schopností neprodleně určit anomálii, lokalizovat původce a eskalovat na odpovědné osoby,
- zajištění interpretace událostí a incidentů z pohledu potřeb bezpečnosti datové sítě, potřeb bezpečného chování uživatelů, potřeb kontroly zajištění souladu s regulativy ČR/EU a standardy

Pro naplnění uvedeného cíle je klíčová úloha nastaveného množství a věrohodnosti atributových dat **aktiv** a nastaveného množství a efektivnosti **korelačních scénářů**. Uchazeč má ze své mnohaleté zkušenosti s provozem SIEM systémů vytvořenou knowledge-base obsahující cca 400 korelačních scénářů, obsahující zkušenosti jaké informace a data v log záznamech mají klíčovou roli k získání potřebného alertu. Navíc Uchazeč má korelační scénáře také nad incidenty, nikoliv jen nad událostmi. Veškeré korelační scénáře byly úspěšně prověřeny jak penetračními testy, tak i reálnými incidenty v rozsáhlých infrastrukturách, včetně zkušeností o vlivu kybernetického útoku na provozní chování SIEM infrastruktury.

Procesní úroveň řízení SIEM spočívá v odpovědné kontrole aktuálnosti informací o aktivech, hodnocení detekovaných změn, efektivitě korelačních pravidel a profesionální komunikaci při zvládání incidentů. Uchazeč uplatňuje postoj, že **primárním cílem** ve zvládání incidentu **je maximalizace informací pro poučení z incidentu**. Hledání viníka není správným morálním principem, neboť původcem incidentu v kybernetickém prostředí bývá software, hardware a uživatelé. Přičemž uživatelé jsou viníky na 99% z přirozené příčiny lidské omylnosti, nikoliv z úmyslně negativních pohnutek.

3.1.1.3 Configuration management – Asset Assesment

Asset Assesment je proces získávání znalostí, dokumentace a evidence komponent sledovaného prostředí, tak aby reálný stav a reálná evidence odpovídala evidenci v configurační databázi procesu Configuration management.

Využití Asset assesmentu a informací v CMDB je důležité:

- pro efektivní separaci detekovaných událostí, dle korelací vyhodnocené priority v SIEM.
- pro přiřazení k příslušnému eskalačnímu workflow Incident Response v rámci SIEM alertů.

V rámci bezpečnostního dohledu jsou významně využívány korelační funkce, které implementují matematické a statistické vzorce nad přicházejícími logovými záznamy. Využití dalších doplňujících informací popisující ovlivňující či ovlivňovanou komponentu informačního systému (aktivum) řádově navyšuje schopnosti bezpečnostních správců detekovat anomální chování a lokalizovat příčiny vzniku anomálie. Nicméně pouze korelační funkce umožňuje správcům tuto schopnost zajistit v real-time režimu. Doplňující informace, které pomáhají k vysoké účinnosti korelací, jsou uloženy v CMDB a zajišťuje je proces Configuration management.

Průběžný monitoring pro proces Configuration management je zajišťován správou Aktiv v prostředí QRADAR appliance.

Role *Operátor monitoringu* zajišťuje:

- Sleduje události (eventy) zpracovávané v SIEM, kde je detekována změna konfigurace aktiva. Tyto změny sleduje v Dashboardu, především změny na významných aktivech a trendy v četnosti výskytů zranitelností.
- Kontrolu evidovaných aktiv – kontroluje denní report o provedených nebo detekovaných změnách v aktivech.
- Kontrolu interních nastavení QRADAR – kontroluje auditní záznam QRADAR, především nastavení jednotného času, komunikačních komponent, nastavení operačního systému, nastavení interních komponent QRADAR.

Role *Specialista monitoringu* se zabývá:

- Kontrolou hodnoty evidovaných aktiv – posuzuje změny infrastruktury a procesů Objednatele v kontextu realizovaných změn uzpůsobuje hodnoty evidovaných aktiv.
- Kontrola QRADAR API rozhraní – export, import dat. Kontrola jednotného času v log datech a zdrojích log dat.

Pro naplnění kvality provozu bezpečnostního monitoringu je klíčová úplná evidence komponent sledovaného prostředí. Uchazeč má knowledge jak efektivně nastavit základní evidenci aktiv a průběžně evidenci aktualizovat. Nezbytná je komunikace se Objednatelem pro kontrolu správnosti evidence nebo součinnost na integraci evidence aktiv v QRadar s evidencí (CMDB) Objednatele.

3.1.1.4 Risk management – Vulnerability&Patch managemenent

Risk management je proces identifikace a prioritizace rizik s asset assessmentem. V rámci system QRadar je zajišťován procesem Vulnerability management, tj. skenováním prostředí na výskyt zranitelností aktiv. Proces Vulnerability management posílá do SIEM informaci o zařízeních, na které nejsou bezpečnostní aktualizace aplikovány. Na druhou stranu jsou v rámci Vulnerability management řešeny i zranitelnosti spojené se zařízeními, na které nejsou včas bezpečnostní aktualizace nasazeny, ať již z důvodu nevycházejících bezpečnostních aktualizací (zařízení není již výrobcem podporováno) nebo z důvodů provozních (nemožnost nasazení bezpečnostní aktualizace z důvodu způsobení nefunkčnosti provozovaných služeb). Pro tato zařízení jsou v rámci Vulnerability managementu přijímány alternativní opatření po dobu, kdy není možné všechny bezpečnostní aktualizace aplikovat.

Pokud jsou v rámci Vulnerability managementu odhaleny zranitelnosti operačních systémů nebo služeb operačního systému, je Objednateli doporučeno zranitelnost ošetřit jedním ze tří hlavních způsobů:

- **Odinstalace softwaru** – pokud je nalezena zranitelnost v softwaru, který není klíčový pro běh aplikace, databáze nebo služby operačního systému běžící na daném serveru, je možno tento zranitelný software odinstalovat a zamezit tak zneužití identifikované zranitelnosti.

- **Úprava konfigurace** – pokud je možno ošetřit zranitelnost úpravou systémových nastavení nebo konfigurace služby tak, že nebude ovlivněna funkčnost a dostupnost produkčního prostředí, je možné řešit identifikovanou zranitelnost pomocí úpravy konfigurace.

- **Instalace aktualizace** – pokud existuje bezpečnostní aktualizace, která adresuje identifikovanou zranitelnost, je možno předat informaci o chybějících aktualizacích, informace o zařízeních, na kterých aktualizace není nainstalovaná a kritičnosti aktualizace procesu Implementace bezpečnostních aktualizací, kde jsou tyto informace využívány pro nastartování patchovacího cyklu.

Proces Patch management (řízení bezpečnostních aktualizací) musí být úzce navázán na proces Vulnerability management. Zranitelnosti identifikované SIEM v rámci procesu Vulnerability management, které jsou spojeny s chybějícími bezpečnostními aktualizacemi, jsou řešeny v procesu Incident Response s napojením na procesy Objednatele - Proces Patch management.

Průběžný monitoring pro proces Risk management je zajišťován rolí *Specialista monitoringu,* který:

- Stanovuje profily pro rozsah a čas skenování aktiv
- Vyhodnocuje získané data a informace o zranitelnostech, tj. dopad na aktiva, způsob potlačení negativních dopadů
- Formou reportu informuje *Vedoucí týmu monitoringu* o úrovni procesu Patch managementu, tj. schopnosti odstraňovat zranitenosti.
- Kontroluje detekční a alertovací workflow v případě výskytu velmi závažné zranitelnosti (ZeroDay).

Uchazeč na základě svého know-how detekci rizik zajišťuje kombinací následujících systémových nástrojů, z jejichž log dat, lze korelací získat potřebné kompletní informace pro Risk management:

1. systém detekce ICT zranitelností;
2. anti-X technologie (X=vir, spam, spy, botnet), Content filtering http provozu;
3. nástroje Patch managementu;
4. systém network a host IDS, systém Network Behavior Analyse;

5. technologie firewallů a proxy serverů;
6. systém pro kontrolu integrity souborů.

Nezbytná je komunikace se Objednatelem pro zajištění Patch management procesu. Pokud nebudou zranitelnosti Objednatelem průběžně řešeny, nelze proces Risk management nijak pozitivně ovlivnit.

3.1.1.5 Incident Response

Incident Response je proces, který úzce vázán na tým rychlé reakce IRT[4], CIRT[5], CSIRT[6]. Uvedené týmy využívají kolaborativní aplikace (Phone, Skype, Mail, Kalendář, atd.), a jednotné prostředí ke sdílení informací (SIEM) k zajištění uceleného pohledu na vzniklou situaci a její působitele.

Uchazeč definuje strategii v procesu Incident Response následujícím výčtem oblastí zájmu:

1. Prověření všech dostupných skutečností k průkaznému ověření, že vznikl bezpečnostní incident (při nejkratším možném čase).
2. Udržení nebo obnovení činností Business Continuity.
3. Snižování dopadů bezpečnostních incidentů na chod procesů Objednatele.
4. Vyšetření způsobu a okolností vzniku bezpečnostních incidentů s cílem „poučení se“ pro další možné případy.
5. Zabránit opakovaným útokům nebo incidentům.
6. Zlepšovat bezpečnost a vylepšovat reakci na incidenty.
7. Stíhat protiprávní činnosti.
8. Řízeně informovat o bezpečnostní situaci a o reakcích na incidenty.

Pro dosažení kvality procesu Incident Response se Uchazeč v bezpečnostním monitoringu zaměřuje na:

- dosažení optimalizace výkonnosti systémů a datové sítě a kontrolovat odchylky.
- kontrolu aktivit uživatelů.
- identifikaci incidentů, porušení pravidel, defraudačních aktivit a provozních problémů.
- forenzní vyšetřování anomálií a transakčních incidentů.
- podporu vnitřního vyšetřování anomálií, událostí, incidentů.
- stanovení základních metrik, identifikaci negativních trendů a časovou detekci vleklých problémů.

Průběžný monitoring pro proces Incident Response spočívá v preventivní činnosti, tj. hotovosti a průběžných analýz ohlášených anomálií.

Role *Operátor monitoringu* zajišťuje:

- 8h denně na vyhodnocování/detekci hrozeb identifikovaných SIEMem. Jeho výstupem je základní identifikace událostí a alertů, včetně potenciálních FALSE POSITIVES ALARMS pro pozdější úpravu korelačních pravidel a dále zakládaní událostí (alert/incident/atd.) o identifikovaných bezpečnostních nálezech/alertech, které následně řeší Specialista Monitoringu.

Role *Specialista monitoringu* řeší*:*

- přípravu postupů pro správu bezpečnostních technologií (přístupové, autentizační, datové, zálohovací, atp.).

[4] Incident Response Team
[5] Computer Incident Response Team
[6] Computer Security Incident Response Team

- přípravu postupů (scénářů) pro reakci na incidenty (detekce, prioritizace, způsob reakce).
- přesnou detekci incidentů, jejich ohodnocení a prioritizaci.
- ohlášení incidentu příslušným osobám, dle schváleného postupu a koordinaci reakce na detekované incidenty.
- Součinnost při hloubkové analýze flow a datových paketů – ovládání modulu *QRadar Incident Forensics* pro potřeby členů Response Teamu.

Role *Specialista Bezpečnostního monitoringu* se zabývá:

- Pokročilou long-time analýzou (vizuální analýzy) nad vybranými log daty pro úpravu korelačních mechanizmů a také pro účinnou detekci neočekávaných anomálií.
- Analýzou transakčních incidentů – kombinované útoky nebo incidenty vyskytujících se ve více kategoriích nebo časových posloupnostech.
- Forenzní analýzou - ovládání modulu *QRadar Incident Forensics* pro potřeby součinnosti s externími skupinami.

Role *Vedoucí týmu monitoringu a testování* je především:

- přiděluje úkoly z vyhodnocených incidentů členům Incident Reponse týmu nebo na ServiceDesk Objednatele .
- řeší kolize priorit úloh k eskalaci v rámci Incident Response a Busines Continuity.
- zajišťuje komunikaci týmu bezpečnostního monitoringu s jinými týmy (CIRT, CSIRT), správci, administrátory, uživateli.

Uchazeč v procesu Incident Response zajišťuje pro Objednatele nepopíratelnost a tím odpovědnost každé fyzické osoby za její veškeré činnosti uskutečněné v informačním systému Objednatele. Dále včasnou reakcí na neobvyklé stavy v prostředí Objednatele zajistit minimalizaci ztrát ze vzniklých chyb a incidentů.

3.3.4 Vyhledávání slabých míst

Uchazeč je primárně zaměřena na využití systémů SIEM a doplňujících komponent k nalézání příležitostí ke zlepšování bezpečnosti nebo kvality ICT služeb Objednatele. Historickou zkušeností Uchazeč s některými správci je až neobvyklá nečinnost v odstraňování rizik, typicky vůči legacy systémům nebo z důvodu nízké kvality Change managementu. Uchazeč doručí Objednateli know-how pro systematické a kontinuální vyhledávání slabých míst infrastruktury.

Uchazeč na základě svého know-how v detekci využívá kombinací systémových nástrojů z jejichž log dat lze korelací získat potřebné informace o aktuálním stavu rizik:

1. systém detekce ICT zranitelností – QRADAR Risk management;
2. anti-X technologie (X=vir, spam, spy, botnet), Content filtering http provozu;
3. nástroje Patch managementu;
4. systém network a host IDS, systém Network Behavior Analyse;
5. technologie firewallů a proxy serverů;
6. systém pro kontrolu integrity souborů.

Pro zajištění kvalitního workflow pro vyhledávání slabých míst považuje Uchazeč nejen identifikaci míry zranitelnosti a lokalizaci zranitelného aktiva, ale také přiřazení k původci zranitelnosti. Jde o zranitelnosti vyvolané chybou konfigurace aktiva, např. chybným nastavením systémové bezpečnostní politiky operačních systémů, chybou nastavení firewallu, proxy serveru, aj.

Risk management hodnotí aktiva z pohledu technické funkčnosti zkoumaného aktiva a vlivu zjištěných slabých míst na dostupnost, důvěrnost a integritu informací, což ve výsledku ovlivní kvalitu produktu nebo kvalitu služby. Nicméně až obsluha QRadar může posoudit: *„slouží nám aktivum správně a je to aktivum bez vad?“*. Jednotlivé hrozby pak posuzuje ve vztahu:

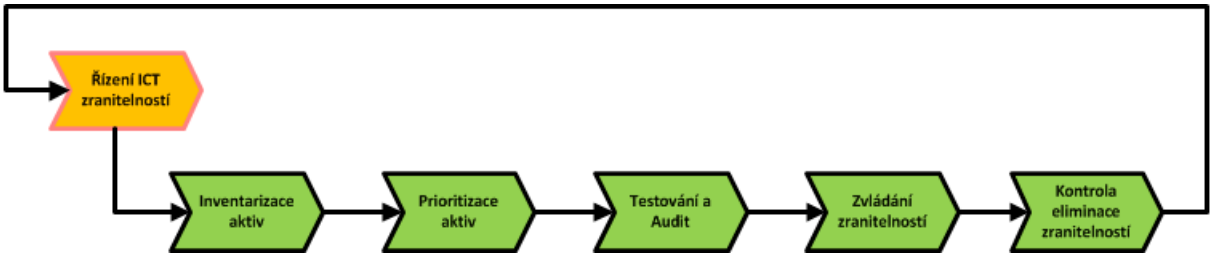
1. jejich snadnosti ovlivnit dotčené aktivum, které je součástí business oblasti, tj. jak snadno lze slabé aktivum využít.

2. závažnosti dopadů na business oblasti či jiná aktiva, tj. dopady jsou tak vztaženy k příslušným hrozbám s interpretací *s jak nízkým úsilím vyrobím závažnou situaci = incident*?

Aktivní vyhledávání slabých míst je zajišťováno skenování prostředí na zranitelnosti v QRADAR Risk managener. Obecně Uchazeč doporučuje následující fáze:

- Definice politiky odhalování ICT zranitelností - obsahuje vymezení požadovaného stavu pro konfigurace kontrolovaných zařízení, jejich interních uživatelských identit a nastavených oprávnění přístupu ke zdrojům kontrolovaných zařízení.
- Nastavení bezpečnostních limitů pro prostředí informačního systému k identifikaci zranitelných míst a detekci prahových odchylek od korektního dodržování zásad.
- Prioritizace aktivit na zmírnění dopadů založené na hodnocení vnějšího ohrožení informací, účinnosti vnitřních bezpečnostních ochran a hodnoty aktiva.
- Provoz bezpečnostních ochran/funkcí směřující k detekci nebo už k přímému odstranění zranitelnosti, pomocí SW a HW nástrojů[7].
- Minimalizace zranitelností a odstraňování kořenových příčin zranitelnosti eskalací do Incident Response.
- Průběžné sledování prostředí informačního systému a detekce odchylek od politiky s identifikací nových zranitelných aktiv, tj. nastavení reportů s výčtem vážných rizik, výčet dotčených vysoce hodnotných aktiv a trend výskytu rizik v prostředí Objednatele.

Uchazeč v procesu Risk managementu zavádí následné workflow, viz obrázek.



Obrázek 22:Workflow pro proces Risk Management

Pro naplnění kvality sledování slabých míst je klíčová úplná evidence komponent sledovaného prostředí.

Ze zkušenosti Uchazeč upozorňujeme na klíčovou fázi subprocesu **Inventarizace aktiv**, který prakticky zajišťuje identifikaci a návazné zatřiďování aktiv do příslušných skupin dle lokality, příslušnosti k ICT službě, významu v infrastruktuře nebo procesu Objednatele s cílem:

a) dosažení evidence všech ICT aktiv umístěných v informačním systému;
b) periodické prověřování a aktualizace seznamu ICT aktiv pro analýzu změn[8];

[7] Např. antivirová ochrana, NBA, atp.

c) odhalení nepovolených ICT aktiv[4];

Vstupem do subprocesu Inventarizace aktiv je:

- IP adresní plán;
- harmonogram skenování;
- intenzita testů.

Subproces **Prioritizace aktiv** pro každé sledované ICT aktivum určuje míru kritičnosti a míru závažnosti nalezené zranitelnosti s cílem vyjádření úrovně bezpečnostního rizika (viz tab.1). Podle úrovně bezpečnostního rizika se stanovuje priorita plánování aktivit při odstraňování zranitelností z dotčených ICT aktiv.
Skupiny aktiv lze dělit na:

- **skupina tiskáren** – test přítomnosti a zjištění všech dostupných identifikačních informací (DNS, NetBios, Vendor, Type);
- **skupina koncových stanic**, tzn. počítače, notebooky, PDA:
  - test operačního systému – prověření verzí všech spustitelných programů vůči seznamu zranitelných programů, prověření správnosti nastavení programů;
  - test služeb (aktivních portů), test procesů – prověření aktivních služeb vůči seznamu schválených služeb, prověření spuštěných procesů na detekci anomálních aktivit
  - test uživatelských účtů, tj. kontrola vazby **IP-Hostname-User_name** pro proces User management.
- **skupina serverů**
  - test operačního systému – prověření verzí všech spustitelných programů vůči seznamu zranitelných programů, prověření správnosti nastavení programů;
  - test služeb (aktivních portů), test procesů – prověření aktivních služeb vůči seznamu schválených služeb, prověření spuštěných procesů na detekci anomálních aktivit (u serverů často realizováno přes systém Host IDS, nicméně není to vždy pravidlem);
  - test uživatelských účtů, tj. kontrola vazby **IP-Hostname-User_name** pro proces User management.
- **skupina komponent datové sítě**, tzn.: switche, routery;
- **skupina specifických komponent**, tzn.: např. systémy bezpečnostní infrastruktury;

Tabulka 14: Definice kritičnosti ICT aktiva

Kritičnost ICT aktiva	Závažnost dopadu
1. Stupeň (velmi nízký)	Aktiva/systémy jejichž možné zranitelnosti a jejich minimalizace mají velmi nízký vliv na zajištění ICT služeb. (událost)
2. Stupeň (nízký)	Aktiva/systémy jejichž možné zranitelnosti a jejich minimalizace mají nízký vliv na zajištění ICT služeb. (událost)
3. Stupeň (střední)	Aktiva/systémy jejichž možné zranitelnosti a jejich minimalizace mají prokazatelný vliv na zajištění ICT služeb.(problém)
4. Stupeň (vysoký)	Aktiva/systémy jejichž možné zranitelnosti a jejich minimalizace mají významný vliv na zajištění ICT služeb.(incident)
5. Stupeň (velmi vysoký)	Aktiva/systémy jejichž možné zranitelnosti a jejich minimalizace mají velmi významný vliv na zajištění ICT služeb.(incident)

[8] Provádí bezpečnostní dohled porovnáváním dat z evidence CMDB.

Subproces **Testování a audit konfigurace** zajišťuje periodické prohledávání informačního systému na zranitelnosti ICT aktiv. Využívá se systému detekce ICT zranitelností pro testování ICT aktiva na zranitelnosti a bezpečnostní audit konfigurace ICT aktiva s cílem detekce nových zranitelností.

Výstupem subprocesu jsou:

- Report s popisem každé zranitelnosti, míry její závažnosti a postupu k jejímu odstranění nebo k její minimalizaci.
- Report nalezených zranitelností pro každé ICT aktivum, vytvořenou skupinu aktiv a míře závažnosti nalezených zranitelností.
- NSR a CSV soubor s přehledem zranitelných ICT aktiv, skupin aktiv a mírou jejich závažnosti.
- On-line přístup k souhrnným údajům o počtu nalezených zranitelností s uvedenou mírou závažnosti pro jednotlivé ICT aktiva, definovaných skupin aktiv a vyjádření trendů vývoje počtu zranitelností v čase.

Následný subproces **Zvládání nalezených zranitelnosti** zajišťuje eliminace zranitelností v požadovaných lhůtách a v závislosti na míře zranitelnosti i hodnotě ICT aktiva.

Vstupem je míra zranitelnosti ICT aktiva, vazba na ICT službu a vazba na příslušného administrátora[9]. Postup zvládání zranitelností řeší Uchazeč, dle následující tabulky.

Tabulka 15: Postup dle kritičnosti IT aktiva

Kritičnost ICT aktiva (systémy)	Postup
ICT aktiva kritičnosti 3	Administrátor ICT aktiva rozhodne o čase a rozsahu zálohování systému před realizací nápravného opatření. (rekonfigurace nebo instalace záplaty, hotfixu, update, service packu,…)
ICT aktiva kritičnosti 4	Administrátor ICT aktiva musí mimořádně zálohovat systém před realizací nápravného opatření. Akceptuje lhůtu realizace nápravného opatření od bezpečnostního správce nebo si do uvedené lhůty vyžádá řešitelský tým, který rozhodne o nové lhůtě a způsobu realizace.
ICT aktiva kritičnosti 5	Administrátor ICT aktiva svolává řešitelský tým (Incident Response Team) (případně i s účastí dodavatele systému/aplikace/řešení) a ve lhůtě stanovené bezpečnostním správcem musí být rozhodnuto o lhůtě a způsobu realizace nápravného opatření.

Při implementaci nápravných opatření se postupuje v souladu s procesem **Change management**[10]. Pro komunikaci stanovených lhůt k řešení zranitelností slouží následující tabulka.

[9] Nebo jemu příslušný organizační útvar.
[10] Ten musí navazovat na Patch management Objednatele.

Tabulka 16: Definice lhůt k řešení zranitelnosti

Hodnocení kritičnosti ICT aktiv	**Hodnocení nalezených zranitelností ICT aktiv**				
	Rizikovost 5 (velmi vysoká)	Rizikovost 4 (vysoká)	Rizikovost 3 (střední)	Rizikovost 2 (nízká)	Rizikovost 1 (velmi nízká)
Kritičnost 5 (velmi vysoká)	2 dny na rozhodnutí o způsobu a lhůtě řešení	5 dnů na rozhodnutí o způsobu a lhůtě řešení	10 dnů na rozhodnutí o způsobu a lhůtě řešení	Bez fixní lhůty, řešení dle domluvy	Bez fixní lhůty, řešení dle domluvy
Kritičnost 4 (vysoká)	5 dnů	7 dnů	14 dnů	Bez fixní lhůty, řešení dle domluvy	Bez fixní lhůty, řešení dle domluvy
Kritičnost 3 (střední)	10 dnů	14 dnů	21 dnů	Bez fixní lhůty, řešení dle domluvy	Bez fixní lhůty, řešení dle domluvy

Výstupem subprocesu jsou seznamy otevřených, uzavřených a ignorovaných zranitelností s příslušnými lhůtami k vyřešení a s přidělenými administrátory. Lze generovat i souhrnné zprávy o počtech vyřešených a nevyřešených zranitelnostech rozdělené podle míry zranitelností, řešitelských útvarů, ICT služeb, procesů, atp. Je nutné, aby Objednatel průběžně dodával aktualizované informace o organizační struktuře a vazbách na procesy Objednatele.

Proto jsou vykonávány následující činnosti, dle role ve workflow:

Role *Specialista monitoringu*:

- Zajišťuje konfiguraci a provoz systému detekce ICT zranitelností QRadar Risk management.
- Monitoruje příslušné provozní a bezpečnostní parametry systému detekce ICT zranitelností.
- Rozděluje řešení bezpečnostních zranitelnosti dle Bezpečnostním manažerem nastavených priorit a lhůt.

Role *Specialista Bezpečnostního monitoringu*:

- Sleduje trendy zranitelností za jemu svěřenou oblast v denní periodě – report o aktivech a dopadech.
- Sleduje trendy vlivu zvládání zranitelností - posuzuje seznamy Objednatelem neošetřených a ignorovaných zranitelností. Následně eskaluje nové lhůty či řešení k realizaci nápravných opatření nebo navrhuje úpravy bezpečnostní politiky, tj. úpravy eskalační lhůty k přijetí nápravných opatření.
- Upozorňuje na bezpečnostní zranitelnosti *Vedoucí týmu monitoringu a testování*
- Komunikuje nalezené zranitelnosti a možná řešení s týmem *Incident Response*.
- Zajišťuje vstupy pro inventarizaci aktiv v QRadar (manuálně nebo automatizovaně přes QRADAR API).

Role *Bezpečnostní konzultant* a *Bezpečnostní specialista* zajišťují podporu a konzultace (tvorba postupů) pro zákazníka/porovozovatele aplikace/provozovatele infrastruktury při nasazení oprav (patchů) v prostředí MS2014+.

Z obdržených výsledků z QRADAR Risk management a z událostí obdržených v SIEM jsou učiněny následující nastavení:

- Report s porovnáním aktuálního stavu hardware a software v kontextu již známých zranitelností, týkajících se evidovaných systémů, jejich konkrétních verzí a implementovaných záplat.

- Report o již provedených aktualizacích firmware, operačních systémů, databázových a aplikačních platforem, a antimalware řešení s důrazem na implementaci dostupných bezpečnostních update, patchů, hotfixů, servicepacků a virových databází.
- Report o provedených změnách v konfiguracích systémů a jejich verifikace s požadavky v ServiceDesk.
- Report ošetřených a neošetřených zranitelností s přiřazenou mírou rizika (míra zranitelnosti plus hodnota ICT aktiva) a lhůtou pro jejich odstranění. Pokud stanovené lhůta k odstranění není opět splněna musí být příslušným administrátorem uvedeny důvody k neplnění lhůty[11].
- Soubor doporučení k odstranění nepoužívaných nebo nadbytečných síťových služeb, aktivovaných služeb operačních systémů a aplikací, za účelem snížení možných zranitelných míst, nadbytečné komunikace, otevřených portů a provedení hardeningu jednotlivých komponent systému MS2014+.

Systém QRADAR bude vytvářet denní reporty dle výše navržené struktury. Tvorba souboru opatření a způsob jeho distribuce k Objednateli bude ujasněna v implementace SIEM QRadar.

3.3.5 Stanovování provozních, technických a konfiguračních parametrů

Uchazeč vnímá bezpečnost jako integrální součást ICT služeb a procesů Objednatele. Z pohledu řízení bezpečnosti bude Uchazeč kooperovat s garanty procesů následovně:

- Incident a Request Management – Integrace na ServiceDesk.
- Change a Release Management – Integrace na Asset assesment.
- Problem Management - reporty.
- Configuration Management – Integrace na Asset assesment, Risk management.
- Service Level Management – reporty, integrace s MIS[12].

V rámci systému QRadar budou garantům procesů a jimi pověřeným osobám přiděleny přístupová oprávnění k Dashboardu a k Reportům k zajištění sdílení informací a jednotného pohleduna bezpečnostní situaci v prostředí Objednatele. Uchazeč přijímá jakékoliv podněty od procesních garantů jako přínos pro provoz a rozvoj SIEM systémů, ať přímé integrace workflow správy SIEM Uchazeče s workflow Objednatele nebo integrací systému QRadar se systémy a evidencemi Objednatele.

Pro specifické procesy nabízí Uchazeč následující kooperaci:

Change a Release Management

- zpracování stanovisek ke změnovým požadavkům z pohledu dopadů navrhovaných změn do bezpečnostních parametrů MS2014+,
- testování funkčnosti změn ovlivňujících chování Qradar prostředí nebo vybraných typových zdrojů log dat.
- verifikace provedení změn v systému MS2014+ detekcí v Qradar jak ve formě událostí, zjištěných změn komunikačních flow, tak i detekcí změn u sledovaných Aktiv.

[11] Analogický postup k vyšetřování bezpečnostního incidentu.
[12] Manažerský Informační Systém.

Configuration Management

- součinnost a zpracování podkladů evidence aktiv, business hodnot a míry zranitelností.
- verifikace provedení změn u aktiv prošlých procesy Change a Release management.
- detekce provedení změn u aktiv, které neprošly schválením, ani procesy Change a Release management. Tyto změny budou klasifikovány jako alerty a směrovány na Incident Reponse.

Incident a Request Management

- schvalování bezpečnostních pravidel, konfigurací bezpečnostních mechanismů a jejich změn u jednotlivých komponent systému MS2014+ v rámci reakce na potřeby log managementu a Network Behavioral Analyse.
- Poskytnutí nezbytné součinnosti a odborné pomoci pro Objednatele.

Problem Management

- řešení bezpečnostních incidentů v souladu s klíčovou činností dle kap. 3.4 Řízení bezpečnostních incidentů.
- Poskytnutí nezbytné součinnosti a odborné pomoci pro Objednatele.

Service Level Management

- součinnost při intepretaci bezpečnostních incidentů majících negativní dopad do ICT služeb Objednatele.
- Tvorba reportů nebo konfigurace integrační rozhraní QRADAR API pro přenos informací o bezpečnostních parametrech SLA.

Uvedené součinnosti budou zajišťovat role:
Role *Vedoucí týmu monitoringu a testování* v rámci **Incident a Request Management, Problem managementu.**
Role *Bezpečnostní konzultant* v rámci **Change a Release Management** a **Service Level Management**
Role *Specialista Bezpečnostního Monitoringu* v rámci **Problem management** a **Configuration managmentu**.

3.3.6 Souhrn rolí

Činnosti jednotlivých rolí popisuje názorně následující tabulka:

Tabulka 17: Činnosti rolí v projektu

Role	**Provádění průběžného monitoringu**	**Vyhledávání slabých míst**	**Stanovování provozních, technických a konfiguračních parametrů bezpečnostních prvků celého prostředí MS2014+**
Bezpečnostní specialista	X	Podpora, hotovost	Podpora, hotovost
Bezpečnostní konzultant	X	Konzultace	Konzultace
Vedoucí týmu monitoringu a testování	Řízení/ Rozhodování	Řízení/ Rozhodování	Rozhodování
Specialista - bezpečnostní monitoring	Tvorba korelací/reportů	Posuzování dopadu nalezených zranitelností	Podpora, hotovost
Specialista - monitoring	Pokročilé analýzy 2hodiny	Konfigurace a úpravy testovacích politik	Konzultace, hotovost
Operátor - monitoring	Vyhodnocování a detekce hrozeb	X	X
Specialista – tester	Testování nových reportů a korelací	Testování nových verzí SW	X

3.3.7 Minimalizace vzniku provozních a bezpečnostních incidentů vzniklých v souvislosti s poskytováním služeb Uchazeče

Uchazeč v maximální míře využívá svoje interní testovací prostředí (LAB), kde testuje navrhované úpravy SIEM konfigurace tak aby byla minimalizována šance nesprávného zásahu a tím poškození konfigurace provozního SIEMu na straně zákazníka.

Taktéž všichni zaměstnanci Uchazeče jsou pravidelně školeni jak na SIEM, tak na zásady bezpečného chování v informačních systémech.

3.3.8 Minimalizace vzniku chyb způsobených lidským faktorem Uchazeče

Uchazeč minimalizuje rizika procesním uspořádáním organizace práce a prioritaizace úloh dle ITIL metodiky. V rámci projektového řízení Uchazeč zpracovává SWOT analýzu projektu, aby definovala oblasti možných rizik a příčinných vztahů k jejich vzniku nebo vztahu k dopadům na klienta.

V rámci kontraktu jsou identifikovaná rizika popsána a se Objednatelem diskutována, a parametrizována. Výsledkem jsou definované metriky pro SLA se smluvní odpovědnosti Uchazeč. Pro metriky nad rámec možností Uchazeč je uplatňováno pojištění na škody.

Snižování chyb vlivem působení lidského faktoru zajišťuje Uchazeč průběžným školením technického personálu, probíhající každý týden. Zde jsou sdíleny know-how při zvládání incidentů, účinná řešení k minimalizaci dopadů na systémy a aktiva. Souběžně 1x týdně probíhá elektronická edukace personálu Uchazeč o nových poznatcích ze zdrojů dodavatelů a partnerů Uchazeč. Ověření probíhá prokazatelnou formou přezkoušení znalostí na následném školení technického personálu.

Výčet veškerých možných chyb způsobených lidským faktorem Uchazeče je uveden v následujícím výčtu, vč. uvedení nápravného opatření navrženého k minimalizaci vzniku těchto chyb:

- Nedodržení smluvních termínů z důvodu nárůstu pracnosti požadovaného řešení – bude flexibilně řešeno doplněním dalších členů do realizačního týmu.
- Vznik chyb při implementaci projektu – Uchazeč disponuje rozsáhlým know how při implementaci SIEMů. Toto know how je reprezentováno interními postupy implementací SIEMů, které detailně popisují ověřené a bezproblémové postupy při implemetaci SIEM.
- Vznik chyb při provozu bezpečnostního dohledu SIEM – Uchazeč disponuje rozsáhlým know how z provozu SIEMů. Toto know how je reprezentováno interními postupy pro provoz SIEMů, které detailně popisují ověřené a bezproblémové postupy při provozu SIEM.
- Vznik chyb při servisních zásazích projektu (plánovaných i neplánovaných) – viz bod 3.3.1 - Uchazeč v maximální míře využívá svoje interní testovací prostředí (LAB), kde testuje navrhované úpravy SIEM konfigurace tak, aby byla minimalizována možnost nesprávného zásahu a tím poškození konfigurace provozního SIEMu na straně zákazníka. Taktéž všichni zaměstnanci Uchazeč jsou pravidelně školeni jak na SIEM, tak na zásady bezpečného chování v informačních systémech.

3.3.9 Požadavky na součinnost při realizaci

3.3.9.1 Objednatele

Předpokladáme minimální požadavky na Objednatele, přesto bude potřeba nezbytné součinosti v následujících fázích:

- Definice uživatelských rolí a oprávnění v rámci fáze analýzy
- Konzultace/potvrzení výstupní dokumentace (cílový koncept) s fáze analýza
- Součinost při samotné fyzické instalaci HW a jeho síťovém oživení
- Vytvoření přístupů/uživatelských účtů pro VPN
- Dodání informací a dat popisujíích sledované prostředí Aplikace MS2014+
- Zajištění napojení Qradar All-In-One na provozní monitoring ke sledování kapacitních parametrů
- Zajištění informací o eskalačním workflow, včetně technologie k realizaci, pro integraci s QRadar SIEM.

3.3.9.2 Provozovatele Aplikace MS2014+

Předpokládané požadavky na provozovatele aplikace MS2014+ jsou v oblasti identifikace a vysvětlení funkcí a logů jednotlivých logujících komponent, bude se tedy jednat o součinost v následujících fázích projektu:

- Konzultace/potvrzení výstupní dokumentace (cílový koncept) z fáze Analýza.
- Konzultace a konfigurace zdrojů při napojování jednotlivých zdrojů logů do SIEMu.

3.3.9.3 Uchazeče služeb Prostředí

Předpokládané požadavky na provozovatele služeb Prostředí jsou z titulu funkcionalit SIEMu velmi podobné jako požadavky na provozovatele Aplikace MS2014+ a jsou tedy opět v oblasti identifikace a vysvětlení funkcí a logů jednotlivých logujících komponent, bude se znova jednat o součinost v následujících fázích projektu:

- Konzultace/potvrzení výstupní dokumentace (cílový koncept) z fáze Analýza.
- Konzultace a konfigurace zdrojů při napojování jednotlivých zdrojů logů do SIEMu.
- Konzultace o komunkačních flow ve sledovaném prostředí Aplikace MS2014+ a návazných informačních systémů.

Navržený způsob poskytování služeb auditu

3.4 Služba „BS04_Kontrola kvality poskytovaných služeb“

Služba BS04 bude poskytována s respektováním principů řízení kvality a uznávaných rámců pro řízení kvality, které zajišťují ucelený přístup, plně adresují problematiku zlepšování a jsou zejména vhodné v prostředí, kde působí více subjektů (multi vendor enviroment).

3.4.1 Plánování systému řízení kvality

Systém řízení kvality projektu obsahuje několik kroků zajišťující úplnou systémovou podporu kvality. Jako vodítko pro stanovení obsahu jednotlivých kroků bude použito normy ISO 10006 pro účely posuzování činností s charakteristikami řízení projektu a pro činnosti s charakterem provozních procesů se využijí oborové standardy (ISO/IEC 20000, ISO/IEC 27000 případně ISO/IEC 22301). Dále bude posuzován soulad s požadavky projektu, projektovému zadání, akceptačním kritériím, validace a verifikace. Detailní postup a použité metody a standardy budou projednány a upřesněny s objednatelem služby.

3.4.2 Kontrola a vyhodnocování parametrů služeb

Na základě požadavků zadávací dokumentace bude poskytována služba kontroly kvality plnění služeb Provozovatele Aplikace MS2014+ a Uchazeče služeb Prostředí. Bude provedena revize rámce (frameworku) reportování a provázání cílů, kritických faktorů úspěchu (CSF) a tomu odpovídající „sady“ požadovaných a smluvených úrovní služeb (SLA). K revizi a dalšímu rozvoji rámce řízení bude přiměřeně využito ověřených principů z metodiky COBIT.

Požadovaná kontrola výkazů a protokolů bude prováděna formou analýzy a následného *Status Report meetingu* (řídící výbor) s uchazečem služeb, vyhodnocování trendů a vyhodnocování vlivu na plnění provozních cílů.

Na základě požadavků bude ustaven vlastní monitoring, který bude zaměřen na nejcitlivější parametry s významným nebo zásadním vlivem na plnění provozních cílů. Předpokládává se, že vlastní monitoring bude doplňovat monitoring uchazečů a podle potřeby bude relativně často modifikován, aby plnil funkci spíše ověřovací, než primární funkci sběru dat.

Formulace zjištění z provedené kontroly bude prováděno na jednak základě vyhodnocování průběžných dat a analýzy vztahů provozních cílů, kritických faktorů úspěchu a dohodnutých úrovní služeb, ale též dle expertního posouzení a využití metody hledání kořenových problémů (root causes) na základě vytvoření stromu žádoucích a nežádoucích efektů (desirable effect a undesirable effects). Uvedené dvě metody, respektive jejich kombinace umožní přesněji adresovat možnosti zlepšení a vyvarovat se neefektivním krokům. Zároveň je třeba zmínit, že efektivita výše uvedených opatření může být limitována smluvními podmínkami mezi uchazečem a odběratelem služeb a možnosti jejich pružné modifikace.

Pro účely komunikace mezi jednotlivými subjekty bude využíván příslušný řídící výbor (např. *Report Status meeting*), kde kromě prezentace výsledků budou řešeny i návrhy na zlepšení a řešení vzniklých sporů, respektive formální zastřešení řešení sporů, které bude probíhat na pracovních jednáních.

Lhůty na poskytování služeb budou v souladu s požadavky zadávací dokumentace (5 pracovních dní). Pracovní jednání a řídící výbory budou naplánované s měsíční periodicitou.

3.4.3 Dohled nad poskytovateli služeb a dodržováním smluvních parametrů služeb

Činnost Posouzení výsledků a závěrů z kontroly kvality:

Dohled nad poskytovateli v rámci provozně orientovaných služeb (operation) bude odvozen primárně ze smluvních ujednání ale též z výsledků v rámci činnosti Kontrola a vyhodnocování parametrů služeb, kde budou ustaveny všechny důležité předpoklady pro efektivní dohled, zejména rámec pro řízení kvality. Použitím tohoto rámce pro řízení kvality ve formě cílů, kritických faktorů úspěchu (CSF) a dohodnutých úrovní služeb (SLA) a jejich explicitního povázání bude dosaženo konzistentní logiky řízení a uzavřen řídící cyklus PDCA. Uvedený přístup umožní posoudit jak vhodnost, tak přiměřenost stanovených provozních cílů s ohledem na provozní reálie. Jako etalon bude přiměřeně použit standard COBIT. Tímto bude zajištěno, že je možné posuzovat soulad smluvních požadavků na SLA a provozních cílů.

Pro účely kontroly dodržování projektových harmonogramů a lhůt, či vzájemných sousledností budou použity nástroje pro řízení kvality projektových činností. Plán řízení kvality bude vypracován podle principů obecných standardů PMBOOK či projektových metodik PRINCE2 v návaznosti na již zavedený způsob řízení kvality mezi Provozovatelem MS2014+ a Poskytovatelem služeb Prostředí a Objednatelem.

Tento plán bude doplněn o požadované aspekty z oblasti řízení lidských zdrojů, posuzování dopadů do smluvních vztahů a identifikací možných smluvních či jiných rizik. Součástí budou i požadované úkony z oblasti řízení životního cyklu systémů, tj. posuzování vhodnosti a úplnosti akceptačních kritérií, testovacích scénářů, a tomu příslušející verifikace a validace. Jako základní východisko bude využit standard pro řízení životního cyklu systému ISO/IEC 15288, popř. další standardy dle dohody se Objednatelem.

Činnost Kontrola dodržování závazných smluvních parametrů:

Na základě výše uvedenho principu bude prováděno posouzení jak smluvních, tak přímo nezasmluvněných parametrů. Posuzování bude prováděno v kontextu ostatních parametrů řídícího rámce, tj. kritických faktorů úspěchu a provozních cílů, a personálně orientovaných parametrů a parametrů mající dopad na ochranu dat a další apekty.

Činnost Posouzení dopadů změn do smluvních vztahů:

V rámci této aktivity bude prováděno odborné posouzení dopadů schválených změn na smluvní vztahy, jmenovitě předmět plnění, rozsah a jeho kvalitu a také na strukturu smluvních řídících parametrů (SLA).

Činnost Dostatečnost akceptačních postupů a kriterií:

Výše uvedený řídící framework umožní vytvořit přesnou mapu souvislostí mezi smluvními úrovněmi služeb, akceptačními kriterií, měřenými veličinami a možnostmi měření. Tímto způsobem je možné provést vyhodnocení dostatečnosti, navíc i efektivnosti akceptačních postupů a kriterií.

Posouzení výsledků závěrů z kontroly kvality bude prezentováno formou zprávy, popřípadě k tomu účelu ustavenému řídícímu výboru

3.4.4 Vyhodnocení služby

V souladu se zadávací dokumentací bude na konci každého období vypracován **Protokol o poskytnuté službě za uplynulé období**, obsahující požadované údaje, tj. posouzení úplnosti a vhodnosti sledovaných paramterů, porovnání vybraných výsledků za sledované období. Uvedený report bude sumarizovat závěry z předchozích aktivit, proběhlých řídících výborů a dalších pracovních jednání s poskytovateli služeb a vlastnní analytické činnosti.

Předpokládaný obsah reportu v rámci požadované struktury bude odrážet:
- struktura provozních cílů a sledovaných veličin a posouzení logické konzistence,
- vyhodnocení sledovaných parametrů z hlediska smluvních a provozních požadavků,
- závěry a výsledky z kontroly kvality,
- analýza a vyhodnocení trendů ve vybraných parametrech,
- návrhy a doporučení pro řešení zjištěných nežádoucích výsledků a efektů

Vyhodnocení dodržování smluvních parametrů, jež bude součástí předkládáné zprávy, obsahově vznikne v rámci plnění předchozích bodů a zpracování strukruty provozních cílů, kritickcých faktorů úspěchu (CSF) a měřených úrovní služeb (SLA).

Návrhy a doporučení pro řešení zjištěných negativních výsledků vznikne v rámci identifikace žádoucích a nežádoucích efektů a hledání kořenových problémů (root causes). Uvedená metoda zajistí též prioritizaci řešení kořenových problémů (root causes) a v případě dostatku vstupních podkladů i možnost odhadu očekávaných benefitů.

3.5 Služba „BS05_Audit prostředí“

3.5.1 Popis metodiky penetračních testů

Penetrační testy v prostředí systému MS2014+ (dále jen **systém**) budou periodicky probíhat na klíčových komponentách systému v souladu s požadavky uvedenými v kapitole 3.5.2.1 ZD.

Cílem metodiky penetračních testů v prostředí systému MS2014+ (dále jen **metodika**) je zavést postupy a procesy provádění bezpečnostních testů v prostředí systému MS2014+ a definovat základní sadu testů, které umoží otestovat bezpečnost systému a ověřit efektivitu bezpečnostních opatření v přijatelném čase a bez zbytečné administrativní zátěže.

3.5.1.1 Rámec metodiky pentračních testů

Metodika penetračních testů v prostředí MS2014+ vychází ze standardu OSSTMM a metodologie OWASP. Metodika bude upravena po detailním seznámení poskytovatele s prostředím systému MS2014+ a podrobena akceptaci Objednatele. Vhodnost metodiky bude ověřena v rámci první iterace penetračních testů. Metodika umožňuje provádět a zkoušet nové testy a reagovat tak na vývoj zranitelností HW a SW.

3.5.1.2 Seznam testů a organizace dokumentů

Seznam testů a jejich popis je veden v návrhu testů pro nadcházející vyhodnocovací období. Přesný postup ověření zranitelnosti ve specifickém prostředí bude popsán ve zprávě nálezu zranitelností, která je výsledkem každého penetračního testu. Frekvence opakovaných penetračních testů bude určována na základě výsledků testu a náročnosti navrhovaných opatření.

3.5.1.3 Fáze penetračního testu

Každý penetrační test v prostředí MS2014+ prochází těmito fázemi: příprava testovacího plánu, schválení plánu, provedení penetračního testu a jeho vyhodnocení.

Příprava testovacího plánu

Specialista – tester připraví a navrhne rozsah testu, jeho typ (interní, externí nebo test konfigurace), naplánuje čas a datum provedení testu a určí cílové komponenty nebo systémy. V této fázi komunikuje specialista – tester s kordinátorem na straně Objednavatele (bezpečnostní manažer nebo jiná autorizovaná osoba), která poskytuje součinnost a informace nutné k provedení testovacího plánu, zejména: IP adresy a doménové názvy části systému, kontroluje stav existujících bezpečnostních opatření, stav záloh, poskytuje kontakt na administrátory cílových systémů, zřizuje síťové přístupy a prostupy, nutné účty do operačního systému, aplikací, databází, terminálových serverů nebo jiných systémů, případně zajistí vhodnou místnost v prostorech Objednatele a přístup do budovy po celou dobu plánovaného testu. Specialista – tester seznámí koordinátora se specifickými riziky testovacího plánu, které budou součástí žádosti o schválení testovacího plánu.

Schválení detailního testovacího plánu

Plánovaný penetrační test a jeho rozsah musí být schválen zodpovědnou osobou na straně Objednavatele - bezpečnostním manažerem (nebo jinou pověřenou osobou mající obdobné kompentence). Schvalování je dvoukrokové – nejprve je předkládán plán testů pro nadcházející vyhodnocovací období, následně je před započetím každého testu předkládán jeho detailní popis a harmonogram. Schválení také autorizuje specialistu – testera takovou činnost provádět ve sjednaném rozsahu. V rámci schválení penetračního testu se bezpečnostní manažer seznámí s rozsahem testu, cílovými systémy, které jsou předmětem testu a souvisejícími riziky. Bezpečnostní

manažer může k posouzení žádosti vyžadovat další informace od koordinátora testu a specialisty testera. Bezpečnostní manažer může omezit rozsah testu, navrhnout a implementovat další opatření před provedením penetračního testu. Bezpečnostní manažer na základě svého uvážení schválí nebo zamítne testovací plán (případně vrátí testovací plán koordinátorovi s připomínkami k přepracování).

Provedení penetračního testu
V této fázi specialista – tester provede cílený penetrační test dle metodiky a schváleného testovacího plánu. V případě, že by penetrační tester nalezl zranitelnost, která nesnese odkladu a významě ohrožuje bezpečnost systému MS2014+, nahlašuje nález ihned bezpečnostnímu manažerovi.

Vyhodnocení penetračního testu
Specialista – tester vyhotoví zprávu o nálezech zranitelností v systému MS2014+, která popisuje zjištění na základě provedeného penetračního testu. Zpráva u každé zranitelnosti klasifikuje její závažnost, místo výskytu, postup ověření zranitelnosti a jednoznačný odkaz testu v metodice, resp. ve standartu, který je součástí metodiky. Součástí zprávy je také doporučená strategie nápravy, tj. jak zranitelnosti odstranit a v jakém pořadí. Specialista – tester výslednou zprávu doručí bezpečnostnímu manažerovi, který přijetí zprávy stvrdí svým podpisem, klasifikuje dokument dle stupnice ochrany organizace a zajistí jeho ochranu před neautorizovanými osobami v prostředí objednatele.

3.5.1.4 Provedení penetračního testu

V této fázi je schválený testovací plán a specialista – tester vykoná penetrační test v těchto fázích:

1. **Příprava testovacích nástrojů** – aktualizace nástrojů nebo jejich bází dat.
2. **Sběr informací** – sběr informací a to pasivně dostupnými prostředky ve veřejné síti internet nebo aktivně síťovými skenery. Síťové skenery už zahajují aktivitu na sítí a testují porty systémů, služby a jejich verze. V této fázi tester detekuje existující moduly a pluginy určité aplikace. Typickým nástrojem této kategorie je síťový skener Nmap, bezpečnostní skener Nessus a aplikační skener Nikto nebo veřejné služby Whois, DNS. Nástroje se liší podle typu cílového systému a služeb, které na něm běží.
3. **Analýza zranitelností systémů** - na základě informací o dostupných službách (otevřených portech) a jejich verzích penetrační tester vyhledává zdokumentované zranitelnosti aplikací a jejich modulů ve veřejných databázích zranitelností, na stránkách výrobce SW nebo v repozitářích exploitovacích nástrojů.
4. **Exploitace zranitelností** - získání přístupu do systému použitím programu, který využívá zranitelnost aplikace s cílem spustit vlastní kód. Takovým programem (exploitem) může být jednoduchý skript v jazyce C, perlu nebo pythonu, který zranitelnost vyvolá a pošle do aplikace kód, který zpravidla vytvoří uživatele nebo spustí vzdálený shell na síťovém portu. Typickým příkladem pokročilejších nástrojů pro exploitaci je metasploit framework obsahující sadu otestovaných exploitů nebo Core Impact Pro. Existijí i veřejně dostupné databáze exploitů, ale každý takový program je potřeba otestovat v laboratorních podmínkách, zda nenaruší intergitu systému a neobsahuje další nežádoucí instrukce. V případě webových aplikací jsou typickými nástroji BurpSuite – webová proxy s doplňujícími moduly pro manuální testování, sada vstupů (řetězců) pro testy zranitelností XSS, CSRF, nástroj SQLmap pro testy zranitelností typu SQL Injection a nástroje pro lámání hesel online nebo offline (THC Hydra, Medusa, Hashcat nebo John the Ripper).
5. **Postexploitace** - eskalace práv uživatele na administrátora systému a získání přístupu k dalším systémům. Součásti této fáze je i pochopení role systému, komunikace s ostatními systémy, obsah diskového prostoru, běžící procesy, existující skripty, výčet existujícího softwaru, uživatelské a aplikační účty, lámání jejich hesel, získání přístupu do databáze apod.

3.5.1.5 Metody a postupy pro testování webové části MS2014+

Penetrační testy pro ověření webové části systému MS2014+ se řídí metodikou OWASP, přesněji dokumentem OWASP Testing Guide 2014 se zaměřením na testování zranitelností, které jsou určeny projektem OWASP TOP 10 (zprávou z roku 2013).

Penetrační test webové aplikace navazuje na metodiku v části - Provedení penetračního testu (v bodech: sběr informací, analýza zranitelností a exploitace) a obecně probíhá v následujících fázích:

1) Sběr informací a identifikace počtu webových rozhranní a technologií.
2) Použití aplikace z hlediska uživatele, pochopení funkčnosti a použití aplikace v různých režimech (návštěvník, uživatel, případně administrátor, obnova a reset hesla).
3) Rozpoznání hranic webové aplikace a interakce s dalšími systémy.
4) Systematické mapování webových stránek, vstupních paramterů a polí přenášených HTTP protokolem. Pomocí nástroje webové proxy (BurpSuite) v manuálním režimu nebo v automatickém módu (Crawler) vytváří penetrační tester HTTP požadavky na jednotlivé stránky a mapujeme chování a jednotlivé odpovědi, adresářovou strukturu a celkový model aplikace.
5) Testujeme webovou stránku po stránce a zkouší různé kombinace vstupnáích parametrů. V případě na podezření zranitelnosti dokumentuje pozorované chování a snaží se zranitelnost exploitovat.

Penetrační tester je v průběhu testování provázen dokumentem OWASP Testing Guide v.4 (od kapitoly 4 - Web Application Security), kde je definováno celkově 92 kontrol (rozuměj bezpečnostních testů) celkem v jedenácti kategoriích. Vzhledem k požadavku objednatele zaměřit se na nejčastější zranitelnosti webových aplikací (OWASP TOP 10), jsou ostatní kontroly volitelné, pokud nejsou určeny v testovacím plánu.

3.5.1.6 Skenování a detekce zranitelností bezpečnostním skenerem

V rámci metodiky budeme využívat automatizovaný bezpečnostní síťový skener (např. Nessus) a to v maximální míře 50% všech bezpečnostních testů. Použití bezpečnostního skeneru nám umožňuje zmapovat rychleji prostředí a detekovat obvyklé zranitelnosti. Získané informace o nálezech pomohou přesněji plánovat další penetrační testy. U podpůrných systemů MS2014+, které netvoří jádro aplikace, je použití bezpečnostního skeneru vhodnou doplňující variantou, protože penetrační testy nelze provádět kontinuálně a na všech komponentách systemu. Využití tohoto automatizovaného nástroje je také vhodné pro testy existence nových zranitelností, na které ještě neexistuje oprava výrobce softwaru a inženýři bezpečnostních skenerů vyvinou alespoň metodu detekce takové zranitelnosti.

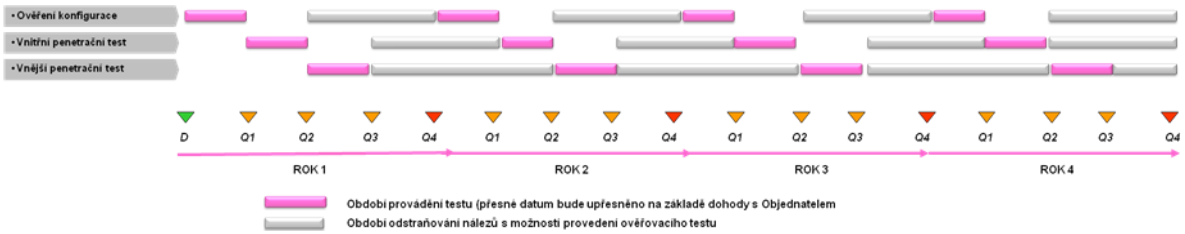
3.5.1.7 Opatření pro minimalizaci provozních a bezpečnostních incidentů

V rámci požadavku zmírnit dopady penetračního testu metodika zavádí následující opatření, která lze navzájem kombinovat:

a) provést penetrační test v testovacím prostředí (případně přenést komponentu, konfiguraci nebo část dat do testovacího prostředí),
b) provést neinvazivní test na produkci (a to v kombinaci s předchozím opatřením, indikujeme pouze podezření na zranitelnost),
c) zredukovat obsah testu na jednu komponentu nebo jeden systém,
d) prověřit systém zálohy a obnovy před penetračním testem (opatření objednatele),
e) dohled administrátora nad chováním systému (opatření objednatele).

3.5.1.8 Harmonogram testů

Testy budou prováděny dle harmonogramu tak, aby každý rok byla provedena kompletní sada požadovaných testů (testy konfigurace, vnitřní a vnější penetrační testy). Hrubý harmonogram je navržen níže.



3.5.1.9 Nástroje

Veškeré uvedené nástroje jsou provozovány v režii poskytovatele a použity v souladu s licenčními podmínkami a jejich užití neklade žádné nároky na objednatele. Seznam použitých nástrojů se může lišit.

Mezi základní vybavení penetračního testera patří linuxová distribuce **Kali** se souborem doplňujících nástrojů, zejména:

- **Nmap** – síťový skener pro detekci portů, síťových služeb a jejich verzí (opensource),
- **BurpSuite** – freeware nástroj pro hledání zranitelností webových aplikací (freeware),
- **Nikto** – web server skener detekující různé aplikace a jejich verze, doplňující moduly včetně nastavení web serveru (opensource),
- **DirBuster** – nástroj pro odhalování existujících adresářů a souborů na web server (opensource),
- **SQLmap** – nástroj pro testování a exploitaci zranitelností typu SQL injection (opensource),
- **THC Hydra, Medusa** – nástroje pro lámání hesel online (opensource),
- **HashCat, John the Ripper** – nástroje pro lámání hesel offline (freeware, opensource),
- **Metasploit framework** – nástroj pro penetrační testování se skenovacími a exploitační moduly včetně platformy pro vývoj dalších modulů (volně k použití),
- **Core Impact Pro** – komplexní penetrační nástroj obsahující detekční skenovací moduly a připravené exploity (komerční nástroj).
- **ncat** – nástroj pro demonstraci zadních vrátek v případě úspěšné exploitace (vzdálený shell) a jednoduché testování síťových portů (volně k použití),
- **BeEF** – nástroj pro exploitaci zranitelností webového prohlížeče (volně k použití),
- **Firefox** – webový prohlížeč doplněný o vývojářské a HTTP moduly (volně k použití),
- **Nessus** – síťový a bezpečnostní skener, umožňuje pouze detekovat zranitelnosti (komerční nástroj),
- **SIUX** – nástroj pro ověřování konfigurací UNIX/Linux systémů (komerční interní nástroj),
- **WinAudit** – nástroj pro ověřování konfigurací MS Windows (komerční nástroj).

3.5.2 Kontroly dodržování pravidel informační bezpečnosti

Audit ISMS je soubor aktivit sloužících k ověření stavu a úrovně bezpečnosti v organizaci (v tomto případě ke kontinuálnímu systematickému ověřování na měsíční bázi tak, aby bylo zajištěno ověření všech kontrolovaných domén 2x ročně). Aktivity bezpečnostního auditu lze rozdělit do několika základních fází (viz následující obrázek), v rámci nichž budou pokryty požadavky Objednatele uvedené v ZD (kapitola 3.5.2.2).

Samotný audit (fáze II a III) je prováděn ve dvou krocích. Prvním je ověření designu bezpečnostních opatření, druhým ověření jejich efektivity. Ověření designu má za úkol zjistit, zda bezpečnostní dokumentace a opatření

- odrážejí potřeby organizace (zda dostatečně pokrývají identifikovaná rizika a jsou v souladu se strategií),
- zda jsou v souladu s nejlepší praxí (zejména standardy a de-facto standardy a legislativou),
- zda jsou v souladu se zvoleným etalonem (zejména sada požadavků norem rodiny ISO 27000).

V rámci ověření efektivity je následně zjišťováno, zda principy a opatření popsané v bezpečnostní dokumentaci organizace jsou v reálu prosazovány. Etalon pro auditní činnosti bude definován v intencích jednotlivých oblastí ISMS. Konkrétní metodika bude doplněna a rozpracována na základě seznámení se se skutečným stavem systému MS2014+ a předložena k akceptaci Objednateli.

Hlavním předpokladem úspěšného zvládnutí prací je vhodné složení autidního týmu a zapojení dostatečně zkušených auditorů. Jejich vyšší seniorita umožní provedení integrovaného auditu. Během něj jsou jednotliví respondenti dotazováni na všechny oblasti, které jsou prověřovány (v tomto případě technologie, personální oblast, procesy). Respondenti tak nejsou nuceni účastnit se opakovaně auditních schůzek, což přináší úsporu a má menší negativní dopady na motivaci zaměstnanců Objednatele. Senioritu zapojených auditorů lze ověřit například jejich certifikacemi (CISA, CISM, CISSP, CGEIT, CRISC) a profesní zkušeností (délka praxe v auditních pozicích). Dalším klíčovým předpokladem úspěšnosti je dostatečná podpora vrcholového vedení a aktivní účast Management committee.

3.5.1 Součinnost při auditech a kontrolách

Uchazeč bude poskytovat součinnost při auditech a kontrolách v rozsahu **20 MD ročně**, způsobem, formou a v termínech stanovených Objednatelem. Uchazeč je připraven poskytnout zdroje odborníků s následujícími znalostmi a certifikacemi:

- **CISSP** Certified Information Systems Security Professional
- **CISA** Certified Information Systems Auditor
- **CISM** Certified Information Security Manager
- **CRISC** Certified in Risk and Information Systems Control
- **GCIH** GIAC Certified Incident Handler
- **GWAPT** GIAC Certified Web Application Penetration Tester
- **CISSP-ISSAP** Certified Information Systems Security Professional – Information Systems Security Architecture Profesional
- **PRINCE2** GIAC Foundation Certified
- **COBIT** Project in controlled environment Foundation certified
- **TOGAF9** Project in controlled environment Foundation certified
- **CGEIT** Certified in Governance of Enterprise IT
- **ISMS Manager** ISMS Manager according to ISO/IEC 27001:2005
- **CCNA** Routing and Switching CISCO Network Associate
- **MCSE** Microsoft Certified Systems Engineer
- **ASE** Compaq Accredited systems engineer (SCO, UnixWare)
- **SCSECA Solaris** Sun Certified Security Administrator
- **Master ACE** SCO Advanced Systems Engineer (UnixWare)
- **STA** Symantec Technology Architect - Virus Protection and Content Filtering
- **ITIL V3** Information Technology Infrastructure Library
- **Radware** Radware Network IAS Certified
- **CEH+** Certified Ethical Hacker
- ArcSight/ISM SIEM solution
- **eCPPT** eLearnSecurity Certified Professional Penetration Tester

A dále odborníky se širokým spektrem znalostí a zkušeností v oblasti technologií (informační a síťové technologie prakticky všech výrobců působících na trhu) či soudní znalce.

Znalosti a kapacity těchto odborníků budou využity rovněž v rámci plnění následující kapitoly.

3.5.2 Součinnost při certifikacích

Uchazeč bude zajišťovat součinnost při atestu Aplikace MS2014+ a Prostředí dle podmínek ISVS a součinnost při případné certifikaci ISMS dle normy ISO 27001. V rámci součinnosti budou zajištěny požadavky uvedené v kapitole 3.5.2.4 zadávací dokumentace, v rozsahu 10 MD ročně.

4 Rejstřík a seznamy

Tabulka 1: Implementace služby BS_01 6
Tabulka 2 Přehled zákonných požadavků 15
Tabulka 3: Zákonná úprava požadavků 16
Tabulka 4: Podrobný přehled zákonných požadavků pro konkrétní zákonnou normu 16
Tabulka 5: Příklad prohlášení o aplikovatelnosti (PoA) 17
Tabulka 6: Prohlášení o aplikovatelnosti 18
Tabulka 7: Plán zvládání rizik 19
Tabulka 8: Role v systému řízení dokumentace 23
Tabulka 9: tabulka pro výpočet a měření účinnosti opatření 26
Tabulka 10: Harmonogram implementace služby BS_02 28
Tabulka 11: Implementace služby BS_03 53
Tabulka 12: Specifikace zařízení 55
Tabulka 13: Specifikace SW 56
Tabulka 14: Definice kritičnosti ICT aktiva 69
Tabulka 15: Postup dle kritičnosti IT aktiva 70
Tabulka 16: Definice lhůt k řešení zranitelnosti 71
Tabulka 17: Činnosti rolí v projektu 74

Obrázek 1: Stanovení aktiv k procesům 11
Obrázek 2: Příklad typického rozložení parciálních rizik 11
Obrázek 3: Rozložení opatření dle jejich váhy 13
Obrázek 4: GAP analýza 18
Obrázek 5: Systém dokumentace ISMS 20
Obrázek 6: Životní cyklus bezpečnostní dokumentace 22
Obrázek 7: Analýza rozsahu 32
Obrázek 8: Struktura registru rizik 42
Obrázek 9: Ukázka matice rizik 42
Obrázek 10: Princip fungování SIEM systému 47
Obrázek 11: Jednotlivé moduly platformy IBM QRadar 48
Obrázek 12: Hlavní prehledová obrazovka 49
Obrázek 13: Ukázka přehledu posledních logů zaznamenaných v systému 49
Obrázek 14: Ukázka přehledu identifikovaných incidentů 50
Obrázek 15: Ukázka části detailu jednoho incidentu 50
Obrázek 16: Ukázka reportu nad firewally Cisco ASA 51
Obrázek 17: Appliance QRadar 3105 54
Obrázek 18: Architektura All-In-One 55
Obrázek 19: Obrázek 19: Oblasti Log Managementu 58
Obrázek 20: Filozofie SIEM Q Radar 61
Obrázek 21: Moduly SIEM Q Radar 63
Obrázek 22:Workflow pro proces Risk Management 68

Číslo v CES: 5390

Příloha č. 5 Smlouvy o poskytování služeb

Bezpečnostní tým

1 Seznam členů bezpečnostního týmu

[1] V případě, že Poskytovatel obsazuje z důvodu potřeb Služeb některou roli více pracovníky, adekvátním způsobem upraví tabulku a přidá potřebný počet řádků