

ДОГОВОР

за възлагане на обществена поръчка

№ MC-58 / 23.05.2018 г.

Днес, 23.05......2018 г. в гр. София, между:

АДМИНИСТРАЦИЯТА НА МИНИСТЕРСКИЯ СЪВЕТ с адрес в гр. София, пощенски код 1594, бул. „Княз Ал. Дондуков” № 1, БУЛСТАТ 000695025, представлявана от г-н Веселин Чинов, директор на дирекция „Административно и правно обслужване и управление на собствеността” – упълномощено лице по чл. 7, ал.1 от Закона за обществените поръчки със Заповед № В-17 от 23.01.2018 г. на министър-председателя и Румяна Славчева Петрова – директор на дирекция „Бюджет и финанси“, наричана по-нататък в договора **ВЪЗЛОЖИТЕЛ**, от една страна, и

„Сървис Центрикс“ ООД, със седалище и адрес на управление: гр. София 1715, ж.к. Младост 4, бул. Александър Малинов 85, ет. 6, офис 20, ЕИК: 200027636, представлявано от Владимир Кънчев Кънчев - управител, наричано по-долу **ИЗПЪЛНИТЕЛ**, от друга страна,

на основание чл. 194, ал. 1 от ЗОП и утвърден Протокол от 10.05.2018 г. на комисия, назначена със Заповед № ФС-52 от 30 април 2018 г. на директора на дирекция „Административно и правно обслужване и управление на собствеността“, да разгледа и оцени офертите, получени след публикуване на обява (№ в РОП 9074880/12.04.2018 г.) за обществената поръчка с предмет: „Одит на информационната сигурност на ИСУН2020” по Проект BG05SFOP001-4.002-0003-C01 „Повишаване на ефективността и ефикасността на Централното координационно звено“, Дейност 1: „Осигуряване на функционирането на информационните системи“, финансиран по Оперативна програма „Добро управление“, се сключи настоящият договор.

Страните се споразумяха за следното:

І. ПРЕДМЕТ НА ДОГОВОРА

Чл. 1. ВЪЗЛОЖИТЕЛЯТ възлага, а **ИЗПЪЛНИТЕЛЯТ** приема да предоставя, срещу възнаграждение и при условията на този Договор, следната услуга: Одит на информационната сигурност на ИСУН2020, който включва следните основни дейности: Одит на информационната сигурност на ИСУН2020, Тестове за пробив в сигурността на ИТ системите на ИСУН2020, Преглед на информационната система ИСУН2020 за съответствие с Общ регламент за защита на данните (GDPR), наричана за краткост „Услугата“.

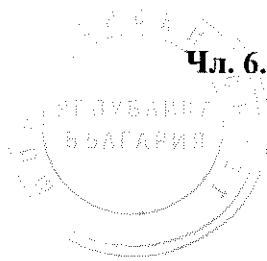
Чл. 2. ИЗПЪЛНИТЕЛЯТ се задължава да предостави Услугата в съответствие с Техническата спецификация, Техническото предложение на **ИЗПЪЛНИТЕЛЯ** и Ценовото предложение на **ИЗПЪЛНИТЕЛЯ**, и чрез лицата, посочени в Списък на персонала, който ще изпълнява поръчката, съставляващи съответно Приложения №№ 1, 2, 3 и 4 към този Договор („Приложенията“) и представляващи неразделна част от него.

Чл. 3. В срок до 3 (три) дни от датата на сключване на Договора, **ИЗПЪЛНИТЕЛЯТ** уведомява **ВЪЗЛОЖИТЕЛЯ** за името, данните за контакт и представителите на подизпълнителите, посочени в офертата на **ИЗПЪЛНИТЕЛЯ**. **ИЗПЪЛНИТЕЛЯТ** уведомява **ВЪЗЛОЖИТЕЛЯ** за всякакви промени в предоставената информация в хода на изпълнението на Договора в срок до 3 (три) дни от настъпване на съответното обстоятелство.

ІІ. СРОК НА ДОГОВОРА. СРОК И МЯСТО НА ИЗПЪЛНЕНИЕ

Чл. 4. Договорът влиза в сила от датата на сключването му.

Чл. 5. Срокът на Договора е 3 (три) месеца, считано от датата на сключването му.



Чл. 6. Място на изпълнение на Договора е отдалечено в следните локации:

- Държавен хибриден частен облак (ДХЧО) към ДАЕУ.
- Областна администрация Пловдив, гр. Пловдив, пл. „Никола Мушанов“ №1.

III. ЦЕНА, РЕД И СРОКОВЕ ЗА ПЛАЩАНЕ

Чл. 7. (1) За предоставяне на услугата одит на информационната сигурност на ИСУН2020, **ВЪЗЛОЖИТЕЛЯТ** се задължава да заплати на **ИЗПЪЛНИТЕЛЯ** обща цена в размер на 69 400,00 (шестдесет и девет хиляди и четиристотин) лева без ДДС и 83 280,00 (осемдесет и три хиляди двеста и осемдесет) лева с включен ДДС, съгласно Ценовото предложение на **ИЗПЪЛНИТЕЛЯ**, съставляващо Приложение № 3 към настоящия договор.

(2) В цената по ал. 1 са включени всички разходи на **ИЗПЪЛНИТЕЛЯ** за изпълнение на услугата одит на информационната сигурност на ИСУН2020, включително и разходите за персонала, който ще изпълнява поръчката, като **ВЪЗЛОЖИТЕЛЯТ** не дължи заплащането на каквито и да е други разноски, направени от **ИЗПЪЛНИТЕЛЯ**.

(6) Цената, посочена в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ**, за предоставяне на Услугата за одит на информационната сигурност на ИСУН2020 е фиксирана за времето на изпълнение на Договора и не подлежи на промяна, освен в случаите, изрично уговорени в този Договор и в съответствие с разпоредбите на ЗОП.

Чл. 8. (1) **ВЪЗЛОЖИТЕЛЯТ** плаща на **ИЗПЪЛНИТЕЛЯ** Цената по този Договор в срок до 15 (петнадесет) работни дни след подписване на двустранен приемо-предавателен протокол за извършените дейности.

Чл. 9. (1) Плащането по този Договор се извършва след подписване на двустранен приемо-предавателен протокол за извършените дейности, съгласно чл. 27 от Договора, от упълномощени представители на **ВЪЗЛОЖИТЕЛЯ** и **ИЗПЪЛНИТЕЛЯ**, посочени в чл. 47, ал. 2, и представяне на фактура от **ИЗПЪЛНИТЕЛЯ**.

Чл. 10. (1) Всички плащания по този Договор се извършват в лева, чрез банков превод, по следната банкова сметка на **ИЗПЪЛНИТЕЛЯ**:

Банка: Банка ДСК

BIC: BSTSABGSF

IBAN: BG57STSA93000021890800

(2) Изпълнителят е длъжен да уведомява писмено **ВЪЗЛОЖИТЕЛЯ** за всички последващи промени по ал. 1 в срок от 3 (три) дни, считано от момента на промяната. В случай, че **ИЗПЪЛНИТЕЛЯТ** не уведоми **ВЪЗЛОЖИТЕЛЯ** в този срок, счита се, че плащането е надлежно извършено.

IV. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ

Чл. 11. При подписването на този Договор, **ИЗПЪЛНИТЕЛЯТ** представя на **ВЪЗЛОЖИТЕЛЯ** гаранция за изпълнение в размер на 5% (пет на сто) от общата стойност на Договора без ДДС, съгласно чл. 7, ал. 1, а именно: 3 470,00 (три хиляди четиристотин и седемдесет) лева, която служи за обезпечаване на изпълнението на задълженията на **ИЗПЪЛНИТЕЛЯ** по Договора.

Чл. 12. (1) В случай на изменение на Договора, извършено в съответствие с този Договор и приложимото право, **ИЗПЪЛНИТЕЛЯТ** се задължава да предприеме необходимите действия за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на Договора, в срок до 10 (десет) дни от подписването на допълнително споразумение за изменението.

(2) Действията за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на Договора могат да включват, по избор на **ИЗПЪЛНИТЕЛЯ**:

1. внасяне на допълнителна парична сума по банковата сметка на **ВЪЗЛОЖИТЕЛЯ**, при спазване на изискванията на чл. 13 от Договора; и/или;

2. предоставяне на документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, при спазване на изискванията на чл. 14 от Договора; и/или

3. предоставяне на документ за изменение на първоначалната застраховка или нова застраховка, при спазване на изискванията на чл. 15 от Договора.

Чл. 13. Когато като Гаранция за изпълнение се представя парична сума, сумата се внася по следната банкова сметка на **ВЪЗЛОЖИТЕЛЯ**:

Банка: БЪЛГАРСКА НАРОДНА БАНКА

BIC: BNBGBGSD

IBAN: BG38 BNBG 9661 3300 1579 01

Чл. 14. (1) Когато като гаранция за изпълнение се представя банкова гаранция, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на банкова гаранция, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, която трябва да отговаря на следните изисквания:

1. да бъде безусловна и неотменяема банкова гаранция;

2. да бъде със срок на валидност за целия срок на действие на Договора, плюс 30 (тридесет) дни след прекратяването на Договора, като при необходимост срокът на валидност на банковата гаранция се удължава или се издава нова.

(2) Банковите разходи по откриването и поддържането на Гаранцията за изпълнение във формата на банкова гаранция, както и по усвояването на средства от страна на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 15. (1) Когато като Гаранция за изпълнение се представя застраховка, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на застрахователна полица, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, която трябва да отговаря на следните изисквания:

1. да обезпечава изпълнението на този Договор чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ**;

2. да бъде със срок на валидност за целия срок на действие на Договора, плюс 30 (тридесет) дни след прекратяването на Договора.

(2) Разходите по сключването на застрахователния договор и поддържането на валидността на застраховката за изисквания срок, както и по всяко изплащане на застрахователно обезщетение в полза на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 16. (1) **ВЪЗЛОЖИТЕЛЯТ** освобождава Гаранцията за изпълнение в срок до 30 (тридесет) дни след прекратяването на Договора/приключване на изпълнението на Договора и окончателно приемане на Услугата в пълен размер, ако липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

(2) Освобождаването на Гаранцията за изпълнение се извършва, както следва:

1. когато е във формата на парична сума – чрез превеждане на сумата по банковата сметка на **ИЗПЪЛНИТЕЛЯ**, посочена в чл. 10, ал. 1 от Договора;

2. когато е във формата на банкова гаранция – чрез връщане на нейния оригинал на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице;

3. когато е във формата на застраховка – чрез връщане на оригинала на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице.

(3) Гаранцията или съответната част от нея не се освобождава от **ВЪЗЛОЖИТЕЛЯ**, ако в процеса на изпълнение на Договора е възникнал спор между Страните относно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** и въпросът е отнесен за решаване пред съд. При решаване на спора в полза на **ВЪЗЛОЖИТЕЛЯ** той може да пристъпи към усвояване на гаранциите.

Чл. 17. ВЪЗЛОЖИТЕЛЯТ има право да задържи съответна част и да се удовлетвори от Гаранцията за изпълнение, когато **ИЗПЪЛНИТЕЛЯТ** не изпълни някое от неговите задължения по Договора, както и в случаите на лошо, частично и забавено изпълнение на което и да е задължение на **ИЗПЪЛНИТЕЛЯ**, като усвои такава част от Гаранцията за изпълнение, която съответства на уговорената в Договора неустойка за съответния случай на неизпълнение.

Чл. 18. ВЪЗЛОЖИТЕЛЯТ има право да задържи Гаранцията за изпълнение в пълен размер, в следните случаи:

1. ако **ИЗПЪЛНИТЕЛЯТ** не започне работа по изпълнение на Договора в срок до 10 (десет) дни след Датата на влизане в сила и **ВЪЗЛОЖИТЕЛЯТ** развали Договора на това основание;

2. при пълно неизпълнение, в т.ч. когато Услугата не отговаря на изискванията на **ВЪЗЛОЖИТЕЛЯ**, и разваляне на Договора от страна на **ВЪЗЛОЖИТЕЛЯ** на това основание;

3. при прекратяване на дейността на **ИЗПЪЛНИТЕЛЯ** или при обявяването му в несъстоятелност.

Чл. 19. Във всеки случай на задържане на Гаранцията за изпълнение, **ВЪЗЛОЖИТЕЛЯТ** уведомява **ИЗПЪЛНИТЕЛЯ** за задържането и неговото основание. Задържането на Гаранцията за изпълнение изцяло или частично не изчерпва правата на **ВЪЗЛОЖИТЕЛЯ** да търси обезщетение в по-голям размер.

Чл. 20. Когато **ВЪЗЛОЖИТЕЛЯТ** се е удовлетворил от Гаранцията за изпълнение и Договорът продължава да е в сила, **ИЗПЪЛНИТЕЛЯТ** се задължава в срок до 10 (десет) дни да допълни Гаранцията за изпълнение, като внесе усвоената от **ВЪЗЛОЖИТЕЛЯ** сума по сметката на **ВЪЗЛОЖИТЕЛЯ** или предостави документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, съответно застраховка, така че във всеки момент от действието на Договора размерът на Гаранцията за изпълнение да бъде в съответствие с чл. 12 от Договора.

Чл. 21. ВЪЗЛОЖИТЕЛЯТ не дължи лихва за времето, през което средствата по Гаранцията за изпълнение са престояли при него законосъобразно.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ

Чл. 22. Изброяването на конкретни права и задължения на Страните в този раздел от Договора е неизчерпателно и не засяга действието на други клаузи от Договора или от приложимото право, предвиждащи права и/или задължения на която и да е от Страните.

Чл. 23. ИЗПЪЛНИТЕЛЯТ има право:

1. да получи възнаграждение в размера, сроковете и при условията по чл. 7-10 от договора;

2. да иска и да получава от **ВЪЗЛОЖИТЕЛЯ** необходимото съдействие за изпълнение на задълженията по този Договор, както и всички необходими документи, информация и данни, пряко свързани или необходими за изпълнение на Договора.

Чл. 24. ИЗПЪЛНИТЕЛЯТ се задължава:

1. да предоставя Услугата и да изпълнява задълженията си по този Договор в уговорените срокове и качествено, в съответствие с Договора и Приложенията;

2. да информира своевременно **ВЪЗЛОЖИТЕЛЯ** за всички пречки, възникващи в хода на изпълнението на работа, да предложи начин за отстраняването им, като може да поиска от **ВЪЗЛОЖИТЕЛЯ** указания и/или съдействие за отстраняването им;

3. да изпълнява всички законосъобразни указания и изисквания на **ВЪЗЛОЖИТЕЛЯ**;

4. да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 42 от Договора;

5. да не възлага работата или части от нея на подизпълнители, извън посочените в офертата на **ИЗПЪЛНИТЕЛЯ** и да контролира изпълнението на техните задължения;

6. да не променя състава на персонала, който ще отговаря за изпълнението на Услугата, без предварително писмено съгласие от страна на **ВЪЗЛОЖИТЕЛЯ**;

7. да предостави на **ВЪЗЛОЖИТЕЛЯ** пълен електронен доклад, съдържащ резултатите от одита и анализа на данните, съгласно изискванията на Техническата спецификация на **ВЪЗЛОЖИТЕЛЯ**;

8. **ИЗПЪЛНИТЕЛЯТ** се задължава да сключи договор/и за подизпълнение с посочените в офертата му подизпълнител/и в срок от 3 (три) дни от сключване на настоящия Договор. В срок до 3 (три) дни от сключването на договор за подизпълнение или на допълнително споразумение за замяна на посочен в офертата подизпълнител, **ИЗПЪЛНИТЕЛЯТ** изпраща копие на договора или на допълнителното споразумение на **ВЪЗЛОЖИТЕЛЯ** заедно с доказателства, че са изпълнени условията по чл. 66, ал. 2 и 11 ЗОП.

Чл. 25. ВЪЗЛОЖИТЕЛЯТ има право:

1. да изисква и да получава Услугата в уговорените срокове, количество и качество;

2. да контролира изпълнението на поетите от **ИЗПЪЛНИТЕЛЯ** задължения, в т.ч. да иска и да получава информация от **ИЗПЪЛНИТЕЛЯ** през целия срок на Договора, или да извършва проверки, при необходимост и на мястото на изпълнение на Договора, но без с това да пречи на изпълнението;

3. да изисква от **ИЗПЪЛНИТЕЛЯ** преработване или доработване на извършената услуга (одит на информационната сигурност на ИСУН2020), в съответствие с уговореното в чл. 29 от Договора;

4. да не приеме извършената услуга, в съответствие с уговореното в чл. 28 от Договора;

Чл. 26. ВЪЗЛОЖИТЕЛЯТ се задължава:

1. да приеме изпълнението на Услугата, когато отговаря на договореното, по реда и при условията на този Договор;

2. да заплати на **ИЗПЪЛНИТЕЛЯ** Цената в размера, по реда и при условията, предвидени в този Договор;

3. да предостави и осигури достъп на **ИЗПЪЛНИТЕЛЯ** до информацията, необходима за извършването на Услугата, предмет на Договора, при спазване на относимите изисквания или ограничения съгласно приложимото право;

4. да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 42 от Договора;

5. да оказва съдействие на **ИЗПЪЛНИТЕЛЯ** във връзка с изпълнението на този Договор, включително и за отстраняване на възникнали пречки пред изпълнението на Договора, когато **ИЗПЪЛНИТЕЛЯТ** поиска това;

6. да освободи представената от **ИЗПЪЛНИТЕЛЯ** Гаранция за изпълнение, съгласно клаузите на чл. 16 от Договора;

VI. ПРЕДАВАНЕ И ПРИЕМАНЕ НА ИЗПЪЛНЕНИЕТО

Чл. 27. Предаването на изпълнението на Услугата за одит на информационната сигурност на ИСУН2020 се документира с протокол за приемане и предаване, който се подписва от представители на **ВЪЗЛОЖИТЕЛЯ** и **ИЗПЪЛНИТЕЛЯ**, посочени в чл. 47, ал. 2 от Договора, в два оригинални екземпляра – по един за всяка от Страните („Приемо-предавателен протокол“).

Чл. 28. (1) ВЪЗЛОЖИТЕЛЯТ има право:

1. да приеме изпълнението, когато отговаря на договореното;

2. когато бъдат установени несъответствия на изпълненото с уговореното или бъдат констатирани недостатъци, **ВЪЗЛОЖИТЕЛЯТ** може да откаже приемане на изпълнението до отстраняване на недостатъците, като даде подходящ срок за отстраняването им за сметка на **ИЗПЪЛНИТЕЛЯ**;

3. да откаже да приеме изпълнението при съществени отклонения от договореното.

(2) Окончателното приемане на изпълнението на Услугата по този Договор се извършва с подписване на окончателен Приемо-предавателен протокол, подписан от Страните в срок до 10 (десет) дни след изтичането на срока на изпълнение по чл. 5 от Договора. В случай, че към този момент бъдат констатирани недостатъци в изпълнението, те се описват в окончателния Приемо-предавателен протокол и се определя подходящ срок за отстраняването им или налагането на санкция, съгласно чл. 29-33 от Договора.

VII. САНКЦИИ ПРИ НЕИЗПЪЛНЕНИЕ

Чл. 29. При просрочване изпълнението на задълженията по този Договор, неизправната Страна дължи на изправната неустойка в размер на 0.5 % (нула цяло и пет на сто) от Цената за одит на информационната сигурност на ИСУН2020 за всеки ден забава, но не повече от 15% (петнадесет на сто) от Стойността на Договора.

Чл. 30. При констатирано лошо или друго неточно или частично изпълнение или при отклонение от изискванията на **ВЪЗЛОЖИТЕЛЯ**, посочени в Техническата спецификация, **ВЪЗЛОЖИТЕЛЯТ** има право да поиска от **ИЗПЪЛНИТЕЛЯ** да изпълни изцяло и качествено, без да дължи допълнително възнаграждение за това. В случай, че и повторното изпълнение на услугата е некачествено, **ВЪЗЛОЖИТЕЛЯТ** има право да задържи гаранцията за изпълнение и да прекрати договора.

Чл. 31. При разваляне на Договора поради виновно неизпълнение на някоя от Страните, виновната Страна дължи неустойка в размер на 15% (петнадесет на сто) от Стойността на Договора.

Чл. 32. **ВЪЗЛОЖИТЕЛЯТ** има право да удържи всяка дължима по този Договор неустойка чрез задържане на сума от Гаранцията за изпълнение, като уведоми писмено **ИЗПЪЛНИТЕЛЯ** за това.

Чл. 33. Плащането на неустойките, уговорени в този Договор, не ограничава правото на изправната Страна да търси реално изпълнение и/или обезщетение за понесени вреди и пропуснати ползи в по-голям размер, съгласно приложимото право.

VIII. ПРЕКРАТЯВАНЕ НА ДОГОВОРА

Чл. 34. (1) Този Договор се прекратява:

1. с изтичане на срока по чл. 5 от Договора;
2. с изпълнението на всички задължения на Страните по него;
3. при настъпване на пълна обективна невъзможност за изпълнение, за което обстоятелство засегнатата Страна е длъжна да уведоми другата Страна в срок до 10 (десет) дни от настъпване на невъзможността;

4. при прекратяване на юридическо лице – Страна по Договора без правопримство, по смисъла на законодателството на държавата, в която съответното лице е установено;

5. при условията по чл. 5, ал. 1, т. 3 от ЗИФОДРЮПДРКЛТДС.

(2) Договорът може да бъде прекратен:

1. по взаимно съгласие на Страните, изразено в писмена форма;
2. когато за **ИЗПЪЛНИТЕЛЯ** бъде открито производство по несъстоятелност или ликвидация – по искане на всяка от Страните.
3. при виновно неизпълнение на задълженията на една от страните по договора – с 10-дневно писмено предизвестие от изправната до неизправната страна.

Чл. 35. (1) Всяка от Страните може да развали Договора при виновно неизпълнение на съществено задължение на другата страна по Договора, при условията и с последиците съгласно чл. 87 и сл. от Закона за задълженията и договорите, чрез отправяне на писмено предупреждение от изправната Страна до неизправната и определяне на подходящ срок за изпълнение. Разваляне на Договора не се допуска, когато неизпълнената част от задължението е незначителна с оглед на интереса на изправната Страна.

(2) За целите на този Договор, Страните ще считат за виновно неизпълнение на съществено задължение на **ИЗПЪЛНИТЕЛЯ** всеки от следните случаи:

1. когато **ИЗПЪЛНИТЕЛЯТ** не е започнал изпълнението на Услугите в срок до 10 (десет) дни, считано от Датата на влизане в сила;

2. **ИЗПЪЛНИТЕЛЯТ** е прекратил изпълнението на Услугите за повече от 20 (двадесет) дни;

3. **ИЗПЪЛНИТЕЛЯТ** е допуснал съществено отклонение от Условията за изпълнение на поръчката, Техническата спецификация и Техническото предложение.

(3) **ВЪЗЛОЖИТЕЛЯТ** може да развали Договора само с писмено уведомление до **ИЗПЪЛНИТЕЛЯ** и без да му даде допълнителен срок за изпълнение, ако поради забава на **ИЗПЪЛНИТЕЛЯ** то е станало безполезно или ако задължението е трябвало да се изпълни непременно в уговореното време.

Чл. 36. ВЪЗЛОЖИТЕЛЯТ прекратява Договора в случаите по чл. 118, ал. 1 от ЗОП, без да дължи обезщетение на **ИЗПЪЛНИТЕЛЯ** за претърпени от прекратяването на Договора вреди, освен ако прекратяването е на основание чл. 118, ал. 1, т. 1 от ЗОП.

Чл. 37. Във всички случаи на прекратяване на Договора, освен при прекратяване на юридическо лице – Страна по Договора без правоприемство:

1. **ВЪЗЛОЖИТЕЛЯТ** и **ИЗПЪЛНИТЕЛЯТ** съставят констативен протокол за извършената към момента на прекратяване работа и размера на евентуално дължимите плащания; и

2. **ИЗПЪЛНИТЕЛЯТ** се задължава:

а) да преустанови предоставянето на Услугата, с изключение на такива дейности, каквито може да бъдат необходими и поискани от **ВЪЗЛОЖИТЕЛЯ**;

б) да върне на **ВЪЗЛОЖИТЕЛЯ** всички документи и материали, които са собственост на **ВЪЗЛОЖИТЕЛЯ** и са били предоставени на **ИЗПЪЛНИТЕЛЯ** във връзка с предмета на Договора.

Чл. 38. При предсрочно прекратяване на Договора, **ВЪЗЛОЖИТЕЛЯТ** е длъжен да заплати на **ИЗПЪЛНИТЕЛЯ** реално изпълнените и приети по установения ред Услуги.

IX. ОБЩИ РАЗПОРЕДБИ

Чл. 39. (1) Освен ако са дефинирани изрично по друг начин в този Договор, използваните в него понятия имат значението, дадено им в ЗОП, съответно в легалните дефиниции в Допълнителните разпоредби на ЗОП или, ако няма такива за някои понятия – според значението, което им се придава в основните разпоредби на ЗОП.

(2) При противоречие между различни разпоредби или условия, съдържащи се в Договора и Приложенията, се прилагат следните правила:

1. специалните разпоредби имат предимство пред общите разпоредби;

2. разпоредбите на Приложенията имат предимство пред разпоредбите на Договора.

Чл. 40. При изпълнението на Договора, **ИЗПЪЛНИТЕЛЯТ** е длъжен да спазва всички приложими нормативни актове, разпоредби, стандарти и други изисквания, свързани с предмета на Договора, и в частност, всички приложими правила и изисквания, свързани с опазване на околната среда, социалното и трудовото право, приложими колективни споразумения и/или разпоредби на международното екологично, социално и трудово право, съгласно Приложение № 10 към чл. 115 от ЗОП.

Чл. 41. (1) Всяка от Страните по този Договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала ѝ известна при или по повод изпълнението на Договора („**Конфиденциална информация**“). Конфиденциална информация включва, без да се ограничава до: обстоятелства, свързани с търговската дейност, техническите процеси, проекти или финанси на Страните, както и ноу-хау, изобретения, полезни модели или други права от подобен характер, свързани с изпълнението на Договора.

(2) С изключение на случаите, посочени в ал. 3 на този член, Конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата Страна, като това съгласие не може да бъде отказано безпричинно.

(3) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. информацията е станала или става публично достъпна, без нарушаване на този Договор от която и да е от Страните;

2. информацията се изисква по силата на закон, приложим спрямо която и да е от Страните; или

3. предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната Страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 Страната, която следва да предостави информацията, уведомява незабавно другата Страна по Договора.

(4) Задълженията по тази клауза се отнасят до съответната Страна, всички нейни подразделения, контролирани от нея фирми и организации, всички нейни служители и наети от нея физически или юридически лица, като съответната Страна отговаря за изпълнението на тези задължения от страна на такива лица.

Задълженията, свързани с неразкриване на Конфиденциалната информация остават в сила и след прекратяване на Договора на каквото и да е основание.

Чл. 42. ИЗПЪЛНИТЕЛЯТ няма право да дава публични изявления и съобщения, да разкрива или разгласява каквато и да е информация, която е получил във връзка с извършване на Услугата, предмет на този Договор, независимо дали е въз основа на данни и материали на **ВЪЗЛОЖИТЕЛЯ** или на резултати от работата на **ИЗПЪЛНИТЕЛЯ**, без предварителното писмено съгласие на **ВЪЗЛОЖИТЕЛЯ**, което съгласие няма да бъде безпричинно отказано или забавено.

Чл. 43. Никоя от Страните няма право да прехвърля никое от правата и задълженията, произтичащи от този Договор, без съгласието на другата Страна. Паричните вземания по Договора могат да бъдат прехвърляни или залагани съгласно приложимото право.

Чл. 44. Този Договор може да бъде изменян само с допълнителни споразумения, изготвени в писмена форма и подписани от двете Страни, в съответствие с изискванията и ограниченията на ЗОП.

Чл. 45. (1) Страните не отговарят за неизпълнение на задължение по този Договор, когато невъзможността за изпълнение се дължи на непреодолима сила.

(2) За целите на този Договор, „непреодолима сила“ има значението на това понятие по смисъла на чл. 306, ал. 2 от Търговския закон.

(3) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата Страна в срок до 7 (седем) дни от настъпване на непреодолимата сила. Към уведомлението се прилагат всички релевантни и/или нормативно установени доказателства за настъпването и естеството на непреодолимата сила, причинната връзка между това обстоятелство и невъзможността за изпълнение, и очакваното времетраене на неизпълнението.

(4) Докато трае непреодолимата сила, изпълнението на задължението се спира. Засегнатата Страна е длъжна, след съгласуване с насрещната Страна, да продължи да изпълнява тази част от задълженията си, които не са възпрепятствани от непреодолимата сила.

(5) Не може да се позовава на непреодолима сила Страна:

1. която е била в забава или друго неизпълнение преди настъпването на непреодолима сила;
2. която не е информирала другата Страна за настъпването на непреодолима сила; или
3. чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на Договора.

(6) Липсата на парични средства не представлява непреодолима сила.

Чл. 46. В случай, че някоя от клаузите на този Договор е недействителна или неприложима, това не засяга останалите клаузи. Недействителната или неприложима клауза се замества от повелителна правна норма, ако има такава.

Чл. 47. (1) Всички уведомления между Страните във връзка с този Договор се извършват в писмена форма и могат да се предават лично или чрез препоръчано писмо, по куриер, по факс, електронна поща.

(2) За целите на този Договор данните и упълномощените представители на **ВЪЗЛОЖИТЕЛЯ** и **ИЗПЪЛНИТЕЛЯ** са, както следва:

1. За ВЪЗЛОЖИТЕЛЯ:

Адрес за кореспонденция: гр. София, бул. „Княз Ал. Дондуков“ № 1

Тел.: 02/940 2501

e-mail: i.kamburov@government.bg

Лице за контакт: Иван Камбуров - главен сътрудник по управление на европейски проекти и програми в отдел „Информационни системи“, дирекция „Централно координационно звено“

2. За ИЗПЪЛНИТЕЛЯ:

Адрес за кореспонденция: гр. София, бул. Александър Малинов 85, ет. 6, офис 20

Тел.: 02/483 76 90

e-mail: info@servicecentrix.com

Лице за контакт: Владимир Кънчев

(3) За дата на уведомлението се счита:

1. датата на предаването – при лично предаване на уведомлението;
2. датата на пощенското клеймо на обратната разписка – при изпращане по пощата;
3. датата на доставка, отбелязана върху куриерската разписка – при изпращане по куриер;
4. датата на приемането – при изпращане по факс;
5. датата на получаване – при изпращане по електронна поща.

(4) Всяка кореспонденция между Страните ще се счита за валидна, ако е изпратена на посочените по-горе адреси (в т.ч. електронни), чрез посочените по-горе средства за комуникация и на посочените лица за контакт. При промяна на посочените адреси, телефони и други данни за контакт, съответната Страна е длъжна да уведоми другата в писмен вид в срок до 7 (седем) дни от настъпване на промяната. При неизпълнение на това задължение всяко уведомление ще се счита за валидно връчено, ако е изпратено на посочените по-горе адреси, чрез описаните средства за комуникация и на посочените лица за контакт.

(5) При преобразуване без прекратяване, промяна на наименованието, правноорганизационната форма, седалището, адреса на управление, предмета на дейност, срока на съществуване, органите на управление и представителство на **ИЗПЪЛНИТЕЛЯ**,

същият се задължава да уведоми **ВЪЗЛОЖИТЕЛЯ** за промяната в срок до 7 (седем) дни от вписването ѝ в съответния регистър.

Чл. 48. Този Договор, в т.ч. Приложенията към него, както и всички произтичащи или свързани с него споразумения, и всички свързани с тях права и задължения, ще бъдат подчинени на и ще се тълкуват съгласно българското право.

Чл. 49. Всички спорове, породени от този Договор или отнасящи се до него, включително споровете, породени или отнасящи се до неговото тълкуване, недействителност, изпълнение или прекратяване, както и споровете за попълване на празноти в Договора или приспособяването му към нововъзникнали обстоятелства, ще се уреждат между Страните чрез преговори, а при непостигане на съгласие – спорът ще се отнася за решаване от компетентния български съд.

Чл. 50. Този Договор се състои от 10 (десет) страници и е изготвен и подписан в два еднообразни екземпляра – по един за всяка от Страните.

Приложения:

Към този Договор се прилагат и са неразделна част от него следните приложения:

Приложение № 1 – Техническа спецификация;

Приложение № 2 – Техническо предложение на **ИЗПЪЛНИТЕЛЯ**;

Приложение № 3 – Ценово предложение на **ИЗПЪЛНИТЕЛЯ**;

Приложение № 4 – Списък на персонала, който ще изпълнява поръчката;

Приложение № 5 – Гаранция за изпълнение.

ВЪЗЛОЖИТЕЛ:

ВЕСЕЛИН ЧИНОВ

ДИРЕКТОР НА ДИРЕКЦИЯ АПОУС

Чл. 2 ЗЗЛД

РУМЯНА ПЕТРОВА

ДИРЕКТОР НА ДИРЕКЦИЯ

„БЮДЖЕТ И ФИНАНСИ“

Чл. 2 ЗЗЛД

ИЗПЪЛНИТЕЛ:

ВЛАДИМИР КЪНЧЕВ

УПРАВИТЕЛ

Чл. 2 ЗЗЛД

ТЕХНИЧЕСКИ СПЕЦИФИКАЦИИ

РАЗДЕЛ I. ОПИСАНИЕ НА ПРЕДМЕТА НА ПОРЪЧКАТА

1. Предназначение на документа

Настоящият документ съдържа описание на изискванията към дейностите по извършване на одит на сигурността на Информационната система за управление и наблюдение на средствата от ЕС (ИСУН2020) позиционирана в Държавния хибриден частен облак (ДХЧО).

Предмет

Предметът на настоящата поръчка „Одит на информационната сигурност на ИСУН2020“ включва извършването на независим преглед на сигурността с цел осигуряване необходимият постоянен контрол и проверка за адекватност и ефективност на съществуващите контроли по защитата на ИСУН2020. Прегледа цели също така да провери съответствието на информационната система с **Общия регламент за защитата на данните (GDPR)**, като даде предложения за подобрения и да идентифицира нуждите от промени в управлението на информационната сигурност, които трябва да включват политиките за сигурност и съответните контроли.

2. Обхват

Обхватът на одита включва следите основни дейности:

- 2.1. Одит на информационната сигурност на ИСУН2020
- 2.2. Тестове за пробив в сигурността на ИТ системите на ИСУН2020
- 2.3. Преглед на информационната система ИСУН2020 за съответствие с **Общ регламент за защитата на данните (General Data Protection Regulation - GDPR)**

В обхватът на одита са информационни системи (хардуер и софтуер) ситуирани в рамките на отговорност на Възложителя.

3. Срок и място на изпълнение

Срокът за изпълнение на настоящата поръчка е 3 месеца, считано от датата на подписване на договора с избрания изпълнител. Дейностите по тази поръчка трябва да бъдат изпълнени отдалечено в следните локации:

- 3.1. Държавен хибриден частен облак (ДХЧО) към ДАЕУ.
- 3.2. Областна администрация Пловдив, гр. Пловдив, пл. „Никола Мушанов“ № 1;

4. Прогнозна стойност на поръчката.

Общата прогнозна стойност на поръчката е до 69 900.00 лв. (шестдесет и девет хиляди и деветстотин лева и 00 ст.) без включен ДДС. Средствата за изпълнение на дейностите по тази поръчка ще бъдат възстановени от проект BG05SFOP001-4.002-0003-C01 „Повишаване на ефективността и ефикасността на Централното координационно звено“, Дейност 1: „Осигуряване на функционирането на информационните системи“.

5. Актуално състояние

Информационната система за управление и наблюдение на Структурните инструменти на Европейския съюз в България (ИСУН2020) за период 2014-2020 г. осигурява ефективно управление и контрол на средствата от Структурните инструменти на ЕС. В ИСУН2020 се извършва въвеждане и съхранение в компютризирана форма на операциите по изпълнение на Оперативните програми. Чрез нея се извършва кандидатстване, оценка, отчитане, наблюдение и проверки свързани с изразходването на средствата на Структурните и

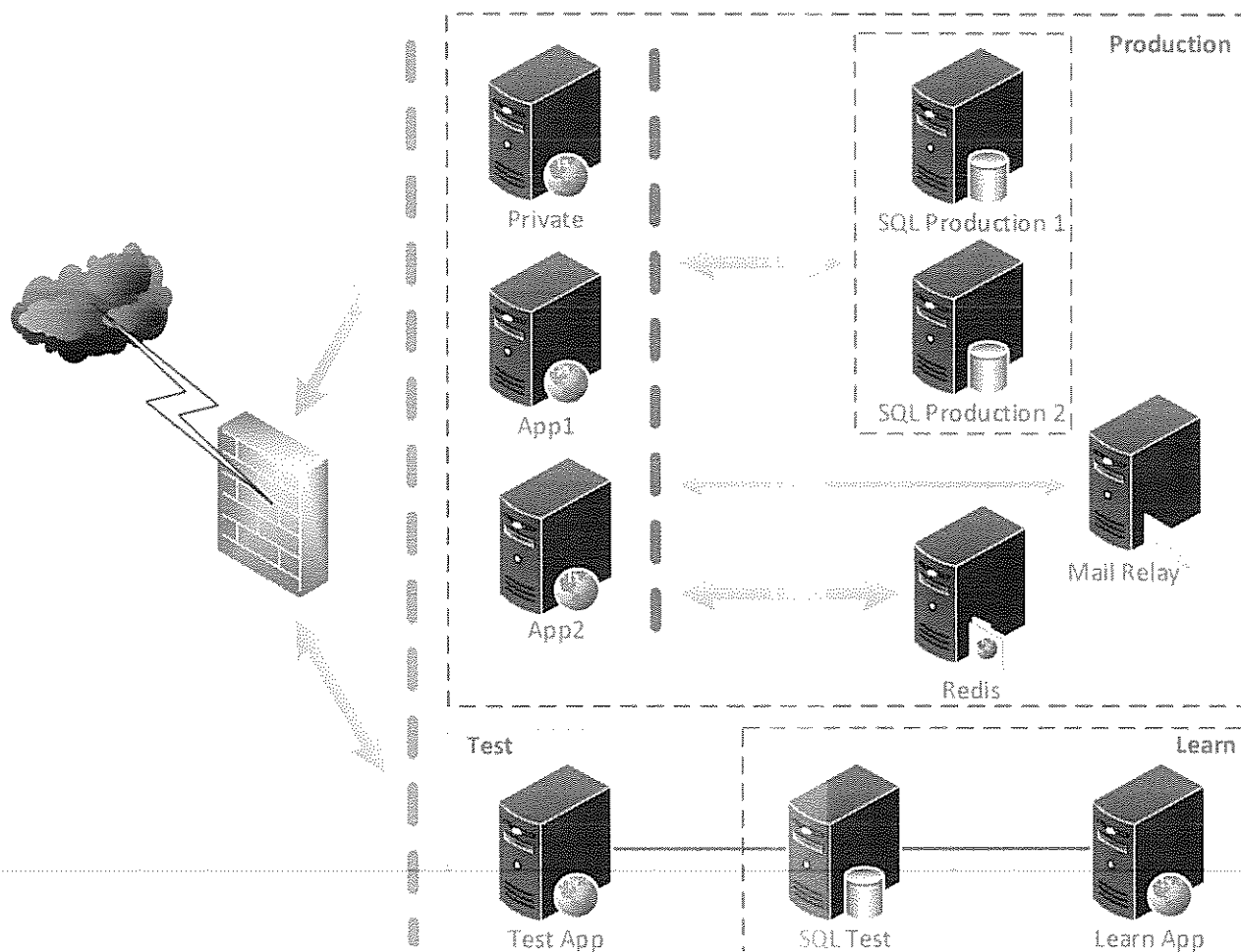
кохезионни фондове на Европейския съюз в България, като се осъществява и обмен на информация през специфичен интерфейс със съответните електронни системи на Европейската комисия. ИСУН2020 е основен инструмент в работните процеси на управляващите органи при изпълнение на ежедневните им задачи.

ИСУН2020 е WEB-базирана информационна система съхраняваща данните в структуриран вид. Електронната системата е изградена на база на технологиите MS dotNET, MS SQL, MS IIS.

Понастоящем ИСУН2020 е позициониран и работи в Държавния хибриден частен облак (ДХЧО) към ДАЕУ като в Областна администрация гр. Пловдив е осигурен Disaster Recovery Center (DRC) с цел осигуряване на висока наличност на услугата и възстановяването ѝ в случай на бедствия и аварии.

Текущият дизайн на ИСУН2020 представен на **Фигура 1.** е наложен от изисквания за високо налично решение и отчитайки добрите практики по отношение на разработване, внедряване и обслужване на ИСУН2020 като включва следните софтуерни среди:

- Продуктивна (работна) среда;
- Тестова среда;
- Среда за обучение.



Фигура 1.

ИСУН2020 на **системно ниво** е изградена на база на MS Hyper-V, Life Migration, и предоставящ възможност за реализиране на високо налично клъстерирано решение (en: failover clustering). Архивирането на електронната система е реализирано с HP Data Protector и HP StoreOne.

В изградена виртуална среда са разположени операционните системи и приложно ниво на системата.

Приложното ниво на ИСУН2020 е изградена изцяло на виртуални машини с операционни системи Microsoft Windows 2012 R2 и Microsoft Windows Server 2016 както следва:

Продуктивна Среда

- **Приложен сървър 1:** APP1 - Microsoft Windows 2012 R2 изпълняващ роля на WEB сървър ,
- **Приложен сървър 2:** APP2 - Microsoft Windows 2012 R2 изпълняващ роля на WEB сървър,
- **Приложен сървър 3:** PRIVATEAPP - Microsoft Windows 2012 R2 изпълняващ роля на WEB сървър,
- **Приложен сървър 4:** SQL Production 1 - Сървър за бази данни MS SQL Server 2016 Ent. Edition, изпълняващ роля на сървър за бази данни и работещ върху MS Windows Server 2016.
- **Приложен сървър 4:** SQL Production 2 - Сървър за бази данни MS SQL Server 2016 Ent. Edition, изпълняващ роля на сървър за бази данни и работещ върху MS Windows Server 2016.
- **Приложен сървър 5:** Regis – Linux Server изпълняващ ролята на система за управление на бази от данни, разположена в оперативната памет с цел оптимизация и бързодействие. Използва се за управление и работа на потребителските сесии.

Тестова среда

- **Приложен сървър 6:** TESTAPP - Microsoft Windows 2012 R2 изпълняващ роля на WEB сървър ,
- **Приложен сървър 7:** LEARNAPP - Microsoft Windows 2012 R2 изпълняващ роля на WEB сървър,
- **Приложен сървър 8:** TEST-SQL - Сървър за бази данни MS SQL Server 2016 Ent. Edition, изпълняващ роля на сървър за бази данни и работещ върху MS Windows Server 2016.

Понастоящем общият обем на базите данни в продуктивна среда е **12 TiB**.

РАЗДЕЛ II. ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

Съобразно определения обхват Изпълнителят трябва да извърши следите дейности:

6. Одит на информационната сигурност на ИСУН2020

Целта на независимия преглед на сигурността е да осигури необходимия постоянен контрол и да се убеди в наличието на адекватност и ефективност на съществуващите контроли за защитата на ИСУН2020. Прегледът цели да се представят предложения за подобрения и да се идентифицират нуждите за промени в управлението на информационната сигурност, които трябва да включват политиките за сигурност и контролите, осигуряващи информационната сигурност.

При извършване на одита на информационната сигурност на ИСУН2020 трябва да се извършат следните основни дейности:

- 6.1. Архитектура и дизайн на решението в областта на Информационната сигурност
 - Анализ на инфраструктурната архитектура
 - Анализ на приложната архитектура
 - Преглед и анализ на архитектурата на мрежово ниво
- 6.2. Извършване на логически одит на контрола на достъп на ИСУН2020 в ДХЧО.
 - Логически контрол на достъпите на ниво операционна система
 - Автентикация
 - Оторизация
 - Логически контрол на достъпите на ниво приложение
 - Автентикация
 - Оторизация
 - Логически контрол на достъпите на ниво мрежа
 - Автентикация
 - Оторизация
- 6.3. Извършване на одит на методите за управление на рисковете в ИСУН2020 в ДХЧО.
 - Методика за управление на риска
 - Наличност на риск списък и план за управление на рисковете
- 6.4. Извършване на одит на методите за криптиране на данните в ИСУН2020 в ДХЧО.
 - Ниво на защита на данните (нива на достъпи, кодиране на критичните данни)
 - кодиране на трафика
- 6.5. Извършване на одит на методите за възстановяване на услугата при настъпване на аварийна ситуация касаеща ИСУН2020 в ДХЧО.
 - Наличие на процедури за възстановяване при бедствия и аварии
 - Тестване на процедурите
- 6.6. Регулаторни изисквания
 - Проверка за наличие и спазване на законовите изисквания за достъп и използване на данните

При констатиране на несъответствия трябва да се документират:

- Евентуални причини за несъответствието;
- Да бъдат оценени действията необходими за тяхното отстраняване;
- Да бъде предложен план за отстраняването им съобразно нивото на риск и усилията за отстраняване на несъответствия;

Одитът трябва да сравни нивата на сигурност с най-добрите практики в областта, както и с приетите политики за сигурност на ИСУН.

7. Тестове за пробив в сигурността на ИТ системите на ИСУН2020 (Penetration Audit)

Целта на тестовете за пробив в сигурността на ИТ системите на ИСУН2020 в ДХЧО е да осигури необходимия постоянен контрол и да се убеди в наличието на адекватност и ефективност на съществуващите контроли по защитата на ИСУН. Прегледът цели също така да даде предложения за подобрения и да идентифицира нуждите за промени в управлението на информационната сигурност, които трябва да включват политиките за сигурност и контролите, осигуряващи информационната сигурност. Тестовете за пробив в ИТ системите на ИСУН2020 в ДХЧО трябва да се извършат като симулация на хакерска атака.

Тестовете за пробив в сигурността на ИТ системите на ИСУН2020 в ДХЧО трябва да се извършат по следния начин:

- 7.1. Определяне на целите на дейностите по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.
 - Информация относно системите, които се тестват;
 - Нива на достъп;
 - Идентификация на Операционни системи, версии, отворени портове и др.;
 - 7.2. Събиране на информация, която да се използва при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.
 - 7.3. Сканиране за уязвимости, които да се използват при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.
 - Сканиране на системите, които се тестват, с инструменти за сканиране на уязвимости;
 - Приготвяне на отчет със списък с откритите уязвимости и препоръки за тяхното отстраняване;
 - 7.4. Сканиране за акаунти с високи привилегии, които да се използват при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.
 - Сканиране на системите, които се тестват, с инструменти за сканиране на акаунти с високи привилегии;
 - Приготвяне на отчет със списък с откритите акаунти с високи привилегии;
 - 7.5. Извършване на тестове за пробив в избрани сървъри от ИТ инфраструктурата на ИСУН2020 в ДХЧО.
 - Използване на различни методи за добиване на достъп до избраните сървъри;
 - 7.6. Извършване на тестове за пробив в уеб приложения от ИТ инфраструктурата на ИСУН2020 в ДХЧО.
 - Използване на различни методи за добиване на достъп до уеб приложенията;
 - 7.7. Извършване на тестове за пробив в избрани сървъри с бази данни от ИТ инфраструктурата на ИСУН2020 в ДХЧО.
 - Използване на различни методи за добиване на достъп до избрани сървъри с бази данни;
 - 7.8. Извършване на тестове за пробив в избрани мрежови устройства от ИТ инфраструктурата на ИСУН2020 в ДХЧО.
 - Използване на различни методи за добиване на достъп до избрани мрежови устройства;
 - 7.9. Изготвяне на отчет от извършените дейности по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.
 - Използване на най-добри практики при приготвяне на отчет от извършените дейности по тестове за пробив в ИТ системите;
 - 7.10. Изготвяне на списък с препоръки по отношение на открити слабости, резултат от извършените дейности по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.
 - Приготвяне на списък с краткосрочни препоръки;
 - Приготвяне на списък с дългосрочни препоръки;
- Ако се открият слабости при извършване на тестове, които могат да се експлоатират успешно, трябва да бъдат посочени:
- Евантуални причини за слабостите;
 - Да бъдат оценени действията необходими за тяхното отстраняване;
 - Да бъде предложен план за отстраняването им съобразно нивото на риск и усилията за отстраняване на несъответствия;
- 8. Преглед на информационната система ИСУН2020 за съответствие с Общия регламент за защитата на данните (General Data Protection Regulation - GDPR)**

Личните данни по същество обхващат цялата информация, с която индивидът може да бъде пряко или непряко идентифициран, а GDPR допълнително включва данни за местоположението, онлайн идентификатори, културната или социална идентичност на дадено лице и т.н. Всички възможни операции по съхранение и манипулация, които могат да бъдат приложени към личните данни, са в обхвата на GDPR. Одита трябва да провери, дали организацията е в състояние да обмисли въздействието от събирането, използването и споделянето на лични данни върху неприкосновеността на личния живот, и че са взети предвид тези въздействия и свързаните с тях рискове за физическите лица.

За да се осигури съответствие с принципа „по подразбиране“ в GDPR, трябва да бъде изследвано къде и каква лична информацията съдържа системата, как тя се достъпва, използва и споделя.

В съответствие с принципа на отчетност съгласно GDPR, всяка организация, независимо дали действа като администратор или преработвател на лични данни, трябва да притежава процедури и документи определящи дейностите както и тяхната проследимост с цел доказване на правилното прилагане на регламента. Изпълнителят трябва да търси подробности за съществуващите политики и процедури, които могат да бъдат използвани за спазване на GDPR, и също така трябва да даде възможност на организацията да определи допълнителни политики и процедури, които биха могли да бъдат от полза за нея, в стремежа си да докаже съответствие.

При извършване на прегледа на ИСУН2020 за съответствие с GDPR изпълнителят трябва да одитира за:

- 8.1. Организация на начина на работа с личните данни
- 8.2. Нива на защита на личните данни
- 8.3. Наличие на процедури за реакция при констатиране на компрометирани лични данни
- 8.4. Процедура на действие при обмен на личните данни с международни инф. системи
- 8.5. Роли и отговорности по защита на личните данни
- 8.6. Преглед на системите от гледна точка за съответствие с GDPR
- 8.7. Изготвяне на GAP анализ и план за действие за покриване на изискванията.

9. Изисквания към реализацията на одита

9.1. На Изпълнителя ще бъде предоставен отдалечен VPN достъп до информационните системи, ситуирани в рамките на отговорност на Възложителя, за извършване на възложените дейности. Тези дейности трябва да бъдат извършвани **след оторизация и от офис** на Възложителя.

9.2. Изисквания при извършване на тестове за пробив в сигурността.

Действията по откриване пробиви в сигурността трябва да включват всички типични тестове обичайно използвани при такъв тип одити. При извършване на тестовите за нерегламентирано проникване трябва да бъдат спазвани следните правила:

- 9.2.1. Атаките „отказ от услуга“(Denial Of Service Aattack) не трябва да бъдат използвани.
- 9.2.2. Да не се използват неизпитани или непознати инструменти или техники.
- 9.2.3. След приключване на тестовите, не трябва да бъдат оставяни активни програми изпълняващи функциите на задни врати (backdoors) или троянски коне (trojan horse).
- 9.2.4. Всички чувствителни данни трябва да останат непокътнати – не трябва да бъдат манипулирани, изтривани, копирани или разрушени.
- 9.2.5. Всички тестове трябва да бъдат извършвани от квалифицирани експерти, за да се сведат до минимум присъщите рискове свързани с проникването и

последващия анализ. Осъдените хакери не трябва да се бъдат допускани през нито една фаза на ангажмента.

9.2.6. Екипите извършващи тестовите за проникване, трябва да се стремят да минимизират влиянието от техните действия върху нормалната работа на информационната система.

9.2.7. Всички тестове по проникване трябва да бъдат извършвани съобразно етичните норми за такива случаи.

9.3. Документация

Изпълнителят трябва да предостави пълен електронен доклад съдържащ резултатите от одита и анализа на данните. Докладът следва да включва следната минимална информация:

9.3.1. Обобщение на извършената работа и на резултатите.

9.3.2. Информация за използваните процеси и инструменти

9.3.3. Списък на констатациите в сравнение с политиките и добрите практики..

9.3.4. Подробен списък с анализирани приложения, оборудване и услуги.

9.3.5. Подробен списък на откритите рискове заедно с анализ на възможните последици и препоръки за корекция.

9.3.6. План за изпълнение на препоръките.

До

Администрация на Министерския
съвет

гр. София, бул. „Дондуков” № 1

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

за участие в обществена поръчка, възлагана чрез събиране на оферти с обява по реда на Глава Двадесет и шеста от ЗОП

От участник:

Сървис Центрикс ООД (наименование на участника), ЕИК/БУЛСТАТ: 200027636 представлявано от Владимир Кънчев Кънчев /трите имена/, в качеството на управител /длъжност, или друго качество/, адрес гр. София, бул. Александър Малинов 85, ет.6, офис 20 телефон: 02/483 76 90 факс, електронна поща info@servicecentrix.com

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

Във връзка с обявената от Вас обществена поръчка по реда на Глава Двадесет и шеста от ЗОП за възлагане на обществени поръчки чрез събиране на оферти с обява с предмет: „Одит на информационната сигурност на ИСУН2020“, представяме нашето техническо предложение за изпълнение на обществената поръчка, както следва (прилага се подробно описание на предложението за изпълнение на поръчката на участника, съобразно Техническата спецификация и изискванията на Възложителя. Техническите предложения на участниците следва да съдържат и предложения, които подлежат на оценяване съобразно методиката за оценка на офертите):

СЪДЪРЖАНИЕ

СЪДЪРЖАНИЕ.....	1
1 ОПИСАНИЕ НА ПОДХОДА ЗА ПРЕДОСТАВЯНЕ НА УСЛУГИ.....	3
1.1 Услуги.....	3
1.2 Клиенти и партньори	4
2 ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИТЕ ПО ПОРЪЧКАТА.....	6
3 ОПИСАНИЕ НА ПОДХОД И МЕТОДОЛОГИЯ ЗА УПРАВЛЕНИЕ НА ПОРЪЧКАТА И ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИТЕ НА ПОРЪЧКАТА.....	21
3.1 Използвани методологии	21

3.2	Методология за управление на проекти.....	21
3.3	Роли и отговорности в проекта.....	28
3.4	Дейности по проекта и график на изпълнение.....	29
3.5	Контрол на качеството	30
4	ИНСТРУМЕНТИ ЗА УПРАВЛЕНИЕ НА КАЧЕСТВОТО	30
	НА КАЧЕСТВОТО	31
5	ОПИСАНИЕ НА ПОДХОДА ЗА УПРАВЛЕНИЕ НА РИСКА ПРИ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА.....	32
5.1	Процес по управление на риска	33
5.2	Регистър на рисковете	36
6	ИЗВЪН ОБХВАТА НА НАСТОЯЩОТО ПРЕДЛОЖЕНИЕ	39

Сървис Центрикс ООД е компания, основана от опитни ИТ професионалисти с многогодишен опит в големи международни компании. Нашият екип е мотивиран да ви предостави комплексни и завършени решения, които да удовлетворяват вашите изисквания, използвайки най-нови технологии с цел оптимизация на цената и подпомагане развитието на бизнеса ви.

Високото ниво на услугите, които предлагаме, е постоянна цел на Сървис Центрикс. Концентрирайки се върху някои от индустриалните стандарти и добри практики, като ITIL, CobIT, ISO20000, ISO 2700x, TOGAF, PMBOK, BABOK, MOF и CMMI, ние предлагаме най-доброто им съчетание за посрещане на конкретните изискванията на клиентите ни. Нашата цел е да открием рисковете, да ги оценим и контролираме за да осигурим надеждността на ИТ операциите, които са критични за бизнес функциите на организацията.

1.1 Услуги

Използвайки добрите практики за управление на ИТ услугите, Сървис Центрикс осигурява консултации от край до край в областта на Информационните Технологии.

От оценката на текущото състояние, през стратегическото планиране и внедряването, нашите висококвалифицирани консултанти работят с вас през всяка една стъпка от проекта.

Нашите консултанти са с дългогодишен опит и притежават следните сертификати:

- ITIL Expert
- ITIL Manager's Certificate
- ITIL ICT Infrastructure Manager
- ISO 20000 Consultant
- Cobit Foundation
- TOGAF Certified
- (ISC)² CISSP (Certified Information Systems Security Professional)
- ISACA CRISC (Certified in Risk and Information Systems Control)
- ISACA CISM - Certified Information Security Manager
- CEH (EC-Council Certified Ethical Hacker)
- ECSA (EC-Council Certified Security Analyst)
- PECB CDPO (Certified Data Protection Officer)
- PMI – PMP
- PRINCE2 Practitioner
- Kepner-Tregoe PSDM
- Cisco – CCIE, CCSP, CCNP, CCSI
- Microsoft Certified Experts – MCT, MCSE, MCSE Messaging, MS IT Pro

„Сървис Центрикс“ ООД предлага консултации и обучение в следните области:

- ИТ Сървис Мениджмънт
- ИТ Архитектура
- Одит на информационната сигурност и оптимизация
- ИТ Инфраструктурен одит и оптимизация
- Моделиране и оптимизация на бизнес процесите

1.2 Клиенти и партньори

Част от нашите клиенти са:

- Виваком
- DTAC – Тайланд (Теленор)
- Теленор България
- Мобилтел
- Мактел (T-Mobile & T-Home)
- Турк Телеком (Турция);
- Уникредит Булбанк;
- Райфайзен Банк – България;
- Райфайзен Банк – Албания;
- Банка ДСК
- Сосиете Женерал ЕкспресБанк
- Комерсиална банка (Сърбия)
- СЕП България;
- Актавис
- Хюлет Пакард - Global Delivery Center;
- Телъс Интернешънъл
- Софика;
- Хюлет Пакард – България
- Хюлет Пакард – Сърбия
- Майкрософт – България
- 4S – Turkey
- Лирекс;
- IBS България
- Български Митници
- Национален Статистически Институт
- Информационно Обслужване

- Министерство на Вътрешните Работи
- Министерство на Външните Работи
- Министерски съвет
- ЕСО

За повече информация:

- Интернет сайт: www.servicecentrix.com
- Емейл адрес: office@servicecentrix.com

В отговор на вашето запитване Сървис Центрикс подготви и предостави настоящата оферта за „ОДИТ НА ИНФОРМАЦИОННАТА СИГУРНОСТ НА ИСУН2020“.

2 ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИТЕ ПО ПОРЪЧКАТА

В тази точка са описани дейностите за изпълнение на поръчката съгласно изискванията на Техническата спецификация (Раздел II от обявата за обществена поръчка).

ИЗИСКВАНИЯ И УСЛОВИЯ НА ВЪЗЛОЖИТЕЛЯ		ПРЕДЛОЖЕНИЕ НА СЪРВИС ЦЕНТРИКС ООД	
6. Одит на информационната сигурност на ИСУН2020			
6.1. Архитектура и дизайн на решението в областта на Информационната сигурност		Сървис Центрикс ще извърши одит на архитектурата и дизайна на решението в областта на Информационната сигурност.	
Дейностите по анализ на ИТ архитектурата на ИСУН2020 в ДХЧО в областта на Информационната Сигурност ще се извършат, като се използва следната методология:			
<ul style="list-style-type: none">Анализ на инфраструктурната архитектураАнализ на приложната архитектураПреглед и анализ на архитектурата на мрежово ниво		<ul style="list-style-type: none">Проучване и анализ на съществуващи документи, описващи ИТ инфраструктурата, както и на среди за инвентаризация на управление на ИТ конфигурациите на ИСУН2020 в ДХЧОСрещи и интервюта с ръководството, собственици на активи и ключови представители на всеки от отделите в дирекция „Информационни системи“Използване на средства за откриване, инвентаризация и анализ на различни групи от инфраструктурни компоненти, като:<ul style="list-style-type: none">Microsoft Baseline Security Analyzer (MBSA) 2.3 – сървъри и работни станции (Microsoft)Microsoft Assessment and Planning Toolkit – сървъри и работни станции (Microsoft)Solarwinds Network Performance Monitor (NPM) – откриване на мрежови устройства; анализ на производителност и надеждност на мрежова свързаностSolarwinds Network Configuration Manager (NCM) – инвентаризация и сваляне на конфигурацията на мрежови устройства	
6.2.Извършване на логически одит на контрола на достъп на ИСУН2020 в ДХЧО.		Сървис Центрикс ще извърши логически одит на контрола на достъп на ИСУН2020 в ДХЧО.	
		Одит на логическия контрол на достъпа на ИСУН2020 в ДХЧО ще бъде извършен след дискусия с представители на организацията, които отговарят за различните видове контрол на достъпа.	

Изисквания и условия на Възложителя	Предложение на Сървис Центрикс ООД
<ul style="list-style-type: none"> • Логически контрол на достъпите на ниво операционна система <ul style="list-style-type: none"> ○ Автентикация ○ Оторизация 	<p>Целта на дискусиите е да се определи как потребителите на ИСУН2020 в ДХЧО получават достъп до работните станции и сървъри, част от организацията, на ниво операционна система и как се ограничават/увеличават правата на отделните потребители според служебните им задължения.</p>
<ul style="list-style-type: none"> • Логически контрол на достъпите на ниво приложение <ul style="list-style-type: none"> ○ Автентикация ○ Оторизация 	<p>Освен на ниво операционна система, трябва да се разгледа и логическият контрол на достъпа на ниво приложение. Това се отнася както за приложения, които използват система за автентикация, различна от тази на операционната система, (т.е. приложения, които не са интегрирани за потребителите и използват отделна/различна система за автентикация и оторизация), така и за приложения, които са интегрирани със системата за автентикация на ниво операционната система.</p>
<ul style="list-style-type: none"> • Логически контрол на достъпите на ниво мрежа <ul style="list-style-type: none"> ○ Автентикация ○ Оторизация 	<p>По подобен начин ще се обсъди и анализира достъпът до мрежови устройства – има ли интеграция със съществуващата система за автентикация и оторизация на потребителите на ниво операционна система (напр. – Активна Директория) или се използва отделна система (локална автентикация, RADIUS, TACACS или ACS и др.).</p> <p>В резултат от горепосочените анализи ще се опишат различните варианти на логически контрол на достъпите за операционна система, приложение, мрежа, които се използват в ИСУН2020 в ДХЧО, като в същото време ще бъдат предложени препоръки за подобряване на процесите по логически контрол на достъпа (ако е необходимо) - според най-добрите практики от гледна точка на ИТ Сигурност.</p>
<p>6.3.Извършване на одит на методите за управление на рисковете в ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> • Методика за управление на риска • Наличност на риск списък и план за 	<p>Сървис Центрикс ще извърши одит на методите за управление на рисковете в ИСУН2020 в ДХЧО. Одитът ще валидира наличието на следните аспекти:</p> <ul style="list-style-type: none"> • Етапи за управление на риска: <ul style="list-style-type: none"> ○ избор на обектите за оценка на риска; ○ идентифициране на информационните активи, свързани с конкретна услуга; ○ идентифициране на заплахите за тези активи и уязвимостите, които могат да бъдат използвани от тях; ○ избор на методология за оценка на риска;

управление на
рисковете

- оценка и приемане на риска;
- избор на защитни мерки и въздействие върху риска;
- реализация и проверка на избраните мерки;
- оценка на остатъчния риск;
- оценка на ефективността на приложените мерки;

• Избор на обектите за оценка на риска

В оценката на риска на конкретна услуга се включват тези активи (информационни системи или други активи), при които са възможни последствия като загуба на поверителност, на цялостност и наличност на информацията; пропуснати ползи, както и потенциални щети или неблагоприятно влияние върху бизнеса вследствие на инцидент, свързан с тях.

За целите на оценката на риска, активите може да бъдат групирани по:

- дейности (информационни системи, процеси);
- информационни активи (т.е. хардуер, софтуер, бази данни, записи с информация),
- хора (т.е. персонал, клиенти, доставчици и др.),
- обкръжаваща среда (т.е. сгради, офиси, съоръжения).

• Методика за оценка на риска

Целта на методиката е да оцени рисковете, на които са изложени активите, за да се установят и изберат подходящи защити на тяхната сигурност. Рисковете са функция на значимостта на активите в опасност, вероятността от поява на заплахи, които да причинят потенциални неблагоприятни бизнес влияния, уязвимостите на установените заплахи и всички съществуващи или планирани защити, които могат да намалят риска.

Какъвто и метод да се приеме, за да се прецени мярката на риска, резултатът от този етап трябва да е списък на установените рискове за сигурността на услугите.

За оценка на риска на активите за сигурността на информацията, свързана с конкретна дейност или услуга се прилага метод, основан на експертната оценка на всички заплахи, свързаните с тях уязвимости за

дадената услуга/актив, както и възможността рискът да бъде установен/определен напълно.

Примерна формула за пресмятане на Приоритета на Риска:

Приоритет на Риска = Вероятност X Влияние (Probability X Severity)

В предложената примерна формула рисковете са функция на:

- значимостта на активите;
- възможните заплахи и свързаната с тях вероятност за появата им, която може да застраши съответните активи;
- свързаните с активите уязвимости и потенциални нежелани въздействия върху активите;
- съществуващите или планирани защиты, които трябва да намалят тежестта на нежеланите въздействия на уязвимостите и свързаните с тях заплахи.

Значимостта на услугите е дадена по-долу. Поради разнообразния характер на активите, изграждащи услугата, възможно е някои от тях да бъдат оценени количествено директно по тяхната финансова стойност, но за други това е невъзможно. Прилагането на качествена оценка на значимостта на активите има универсален характер, като определените стойности могат да варират – например от „много ниска“ до „много висока“ с произволен брой стъпки между тях.

Оценяването на значимостта на активите се извършва под ръководството на Ръководител по сигурността с участието на отговорниците на съответните услуги/ активи. При необходимост може да се потърси съдействието на служителите, които ползват услугите/ активите или участват в дейностите по бизнес планиране, финансиране или поддържане на активите.

Оценяване на значимостта на услугите/ активите се извършва експертно в зависимост от вида на услугата. В зависимост от вида на услугата при оценяването ѝ се отчитат възможните последствия от загуба на поверителност, на цялостност и наличност на информацията, свързана с него или на пропуснатите ползи; потенциалните щети или

неблагоприятното влияние върху бизнеса вследствие на инцидент. Ако е приложимо, при определяне на значимостта на услуга се използва и първичната цена на активите, които я изграждат, стойността им при замяна и възпроизвеждане, а също и значението ѝ за доброто име и репутация на дружествата.

За окончателната стойност на значимостта на услугата се приема максималната от всички възможни стойности на нейната значимост.

Оценяването на значимостта на услугите на ИСУН2020 в ДХЧО може да се извърши с помощта на следните критерии, с които се определя големината на възможните щети в резултат на загуба на поверителност, цялостност или наличност на информацията:

- нарушаване на законовите и други нормативни изисквания;
- загуба на клиенти;
- отрицателен ефект върху репутацията на дружеството;
- инциденти, свързани с личната информация;
- излагане на опасност на личната сигурност;
- инциденти с поверителността на търговските дейности;
- нарушаване на общественения ред;
- финансови загуби;
- влошаване на бизнес дейностите;
- излагане на опасност на сигурността на околната среда.

При определяне на критериите за уязвимост се отчитат всички въведени мерки за защита на оценявания актив, както и адекватността на мерките.

За оценката на риска, съответният актив (или група от активи) се съпоставя с възможната за него заплаха и отговарящата ѝ уязвимост, като се отчитат присъщата му уязвимост.

Заплахите могат да бъдат:

- Форс мажорни събития
- Организационни проблеми
- Човешки грешки
- Технически грешки
- Преднамерени, злоумишлени деяния

Заплахите могат да бъдат случайни или предумишлени. И случайните и предумишлените източници на заплаха трябва да бъдат отчетени и да бъде оценена вероятността за тяхната поява.

ИЗИСКВАНИЯ И УСЛОВИЯ НА ВЪЗЛОЖИТЕЛЯ	ПРЕДЛОЖЕНИЕ НА СЪРВИС ЦЕНТРИКС ООД
	<p>Ако за една услуга са възможни няколко заплахи или няколко уязвимости, свързани с определена заплаха, то рискът се оценява поотделно за всеки отделен случай.</p> <p>Наличието на уязвимост само по себе си не причинява вреда, а трябва да има налична заплаха, която да я използва. Уязвимост, за която няма съответстваща ѝ заплаха, не изисква прилагането на защита, но трябва да бъде разпозната и да се наблюдава за промени. Трябва да се отчете, че неправилно въведените, не функциониращите или неправилно използваните защиты могат сами по себе си да бъдат уязвимост.</p>
<p>6.4. Извършване на одит на методите за криптиране на данните в ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> Ниво на защита на данните (нива на достъпи, кодиране на критичните данни) кодиране на трафика 	<p>Сървис Центрикс ще извърши одит на методите за криптиране на данните в ИСУН2020 в ДХЧО.</p> <p>Процесът по одит на методите за криптиране на данните в ИСУН2020 в ДХЧО ще включва дискусия с представители на Възложителя относно следната тема – кои са критичните данни в организацията. След установяване на критичните данни в ИСУН2020 в ДХЧО, ще бъдат разгледани, обсъдени и проверени различните нива на достъп до тези критични данни, по какъв начин се кодират (подход, шифър и др.) и предоставят за ползване.</p> <p>Ще бъде разгледан и проверен процеса по кодиране на трафика – VPN свързаност, отдалечен достъп, потребителски достъп до услугите за граждани и др.</p>
<p>6.5. Извършване на одит на методите за възстановяване на услугата при настъпване на аварийна ситуация касаеща ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> Наличие на процедури за възстановяване при бедствия и аварии 	<p>Сървис Центрикс ще извърши одит на методите за възстановяване на услугата при настъпване на аварийна ситуация касаеща ИСУН2020 в ДХЧО.</p> <p>Сървис Центрикс ще анализира в детайли практиките за осигуряване на наличността и непрекъснатостта на услугите. Подробно ще бъдат прегледани следните аспекти:</p> <ul style="list-style-type: none"> Изисквания за наличност и цели <p>Изискванията за наличността на услугата трябва да бъдат събрани и оценени съвместно с всички заинтересовани страни и да покриват следните аспекти:</p> <ul style="list-style-type: none"> Максимално време за възстановяване на услугата (дни или часове) Права за достъп до услугата (кой има право да достъпва услугата, кога и от кои локации)

32/6

ИЗИСКВАНИЯ И УСЛОВИЯ НА ВЪЗЛОЖИТЕЛЯ	ПРЕДЛОЖЕНИЕ НА СЪРВИС ЦЕНТРИКС ООД
<ul style="list-style-type: none"> • Тестване на процедурите 	<ul style="list-style-type: none"> ○ Време за отговор при достъп до услугата (в секунди при интерактивна работа, часове или дни при пакетна обработка) ○ Цялостна наличност на услугата (end to end) в проценти през договореното работно време • Дизайн на услугите за висока наличност • Методи за наблюдение и отчетност на наличността • Осигуряване на наличността при промени в системите и услугите • План за непрекъснатост на услугите • Дефиниране на бедствие и комуникации • Приоритети на защита • Налични процедури за бекъп и архивиране на услугите • Налични процедури за възстановяване • План за възстановяване на услугите в резервен дейтацентър • План за възстановяване на услугите обратно в основен дейтацентър • Налични протоколи и записи от тестването на процедурите – реално време за възстановяване, проблеми и актуализиране при промени
<p>6.6. Регулаторни изисквания</p> <ul style="list-style-type: none"> • Проверка за наличие и спазване на законовите изисквания за достъп и използване на данните 	<p>Сървис Центрикс ще извърши одит на спазването на регулаторни изисквания, като Закон за Обществените Поръчки, изисквания за уеб достъпност (WCAG 2.0), и др.</p>
<p>7. Тестове за пробив в сигурността на ИТ системите на ИСУН2020 (Penetration Audit)</p>	
<p>Съществуват няколко основни типа Тестове за пробив в сигурността на ИТ системи:</p> <ul style="list-style-type: none"> • Black-box тест на сигурността на ИТ системи – това е тест на сигурността на ИТ системи, при който екипът, който извършва тестовете, не разполага предварително с информация относно ИТ системите, които ще тества. • Grey-box тест на сигурността на ИТ системи – това е тест на сигурността на ИТ системи, при който екипът, който извършва тестовете, получава предварително малко количество информация относно ИТ системите, които ще тества (напр. мрежови сегменти, които да се тестват, определени приложения или др.). 	

15

3/6

ИЗИСКВАНИЯ И УСЛОВИЯ НА ВЪЗЛОЖИТЕЛЯ		ПРЕДЛОЖЕНИЕ НА СЪРВИС ЦЕНТРИКС ООД	
<ul style="list-style-type: none"> White-box тест на сигурността на ИТ системи – това е тест на сигурността на ИТ системи, при който екипът, който извършва тестовете, получава предварително сериозно количество информация относно ИТ системите, които ще тества (напр. конкретни работни станции, които да се тестват, определени приложения, определени акаунти за работа и др.). 			
<p>7.1. Определяне на целите на дейностите по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> Информация относно системите, които се тестват; Нива на достъп; Идентификация на Операционни системи, версии, отворени портове и др.; 		<p>Сървис Центрикс ще извърши определяне на целите на дейностите по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <p>При извършване на тестове за пробив в сигурността на ИТ системите на ИСУН2020 в ДХЧО, екипът на Сървис Центрикс ще започне със събиране на възможно най-много и най-ценна информация относно тези ИТ системи – това включва тип и версия на Операционна система, отворени портове за комуникация, други налични услуги. Ще бъдат обсъдени с представители на организацията различните нива на достъп в ИТ системите, за да се извършат тестове за повишаване на нивото на достъп на потребител, без необходимото разрешение и настройки.</p>	
<p>7.2. Събиране на информация, която да се използва при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p>		<p>Сървис Центрикс ще извърши събиране на информация, която да се използва при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <p>В допълнение към предходната точка, се събира всякакъв вид полезна информация, която би могла да се използва от екипа на Сървис Центрикс по време на тестовете за пробив (напр. съобщения за грешки, които разкриват поверителна информация, банери и др.).</p>	
<p>7.3. Сканиране за уязвимости, които да се използват при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> Сканиране на системите, които се тестват, с инструменти за 		<p>Сървис Центрикс ще извърши сканиране за уязвимости, които да се използват при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <p>ИТ системите ИСУН2020 в ДХЧО ще бъдат сканирани за уязвимости с различни инструменти за сканиране на уязвимости. Екипът на Сървис Центрикс ще използва следните инструменти за сканиране на уязвимости (част от тези инструменти се използват и при събирането на информация за ИТ системите, които ще бъдат обект на тестове):</p> <ul style="list-style-type: none"> Вградени инструменти на дистрибуцията Kali-Linux-2017.3 като – openvas, nmap и др. 	

ИЗИСКВАНИЯ И УСЛОВИЯ НА ВЪЗЛОЖИТЕЛЯ	ПРЕДЛОЖЕНИЕ НА СЪРВИС ЦЕНТРИКС ООД
<p>сканиране на уязвимости;</p> <ul style="list-style-type: none"> Приготвяне на отчет със списък с откритите уязвимости и препоръки за тяхното отстраняване; 	<ul style="list-style-type: none"> Инструмент Angry IP Scanner Инструмент Ivanti Patch Management Инструмент Microsoft Baseline Security Analyzer Инструмент Solarwinds NPM, NCM <p>Екипът на Сървис Центрикс ще приготви отчет с откритите уязвимости и съответните препоръки за тяхното отстраняване.</p>
<p>7.4. Сканиране за акаунти с високи привилегии, които да се използват при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> Сканиране на системите, които се тестват, с инструменти за сканиране на акаунти с високи привилегии; Приготвяне на отчет със списък с откритите акаунти с високи привилегии; 	<p>Сървис Центрикс ще извърши сканиране за акаунти с високи привилегии, които да се използват при тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <p>ИТ системите на ИСУН2020 в ДХЧО ще бъдат сканирани за акаунти с високи привилегии. Екипът на Сървис Центрикс ще използва следните инструменти за сканиране на акаунти с високи привилегии:</p> <ul style="list-style-type: none"> Инструмент CyberArk Discovery and Audit (CyberArk DNA) <p>Екипът на Сървис Центрикс ще приготви отчет с откритите акаунти с високи привилегии и съответните препоръки за тяхното отстраняване. Отчетът ще съдържа и информация относно опасност от атаки тип Pass-The-Hash и Golden Ticket.</p>
<p>7.5. Извършване на тестове за пробив в избрани сървъри от ИТ инфраструктурата на ИСУН2020 в ДХЧО.</p>	<p>Сървис Центрикс ще извърши тестове за пробив в избрани сървъри от ИТ инфраструктурата на ИСУН2020 в ДХЧО.</p> <p>Върху избрани сървъри от ИТ инфраструктурата на ИСУН2020 в ДХЧО ще бъдат извършени тестове за пробив с различни инструменти за тестове за пробив. Тези сървъри ще бъдат определени според резултатите от сканиране за уязвимости и/или ще бъдат изрично</p>

5/10

ИЗИСКВАНИЯ И УСЛОВИЯ НА ВЪЗЛОЖИТЕЛЯ	ПРЕДЛОЖЕНИЕ НА СЪРВИС ЦЕНТРИКС ООД
<ul style="list-style-type: none"> • Използване на различни методи за добиване на достъп до избраните сървъри; 	<p>посочени от представители на Възложителя. Екипът на Сървис Центрикс ще използва следните инструменти за тестове за пробив:</p> <ul style="list-style-type: none"> • Вградени инструменти на дистрибуцията Kali-Linux-2017.3 като – Metasploit Framework и др. <p>Екипът на Сървис Центрикс ще приготви отчет с резултати от тестовете за пробив и съответните препоръки за отстраняване на уязвимости, които са използвани успешно при тестовете за пробив.</p>
<p>7.6. Извършване на тестове за пробив в уеб приложения от ИТ инфраструктурата на ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> • Използване на различни методи за добиване на достъп до уеб приложенията; 	<p>Сървис Центрикс ще извърши тестове за пробив в уеб приложения от ИТ инфраструктурата на ИСУН2020 в ДХЧО.</p> <p>Върху определени уеб приложения от ИТ инфраструктурата на ИСУН2020 в ДХЧО ще бъдат извършени тестове за пробив с различни инструменти за тестове за пробив. Тези уеб приложения ще бъдат определени според резултатите от сканиране за уязвимости и/или ще бъдат изрично посочени от представители на Възложителя. Екипът на Сървис Центрикс ще използва следните инструменти за тестове за пробив:</p> <ul style="list-style-type: none"> • Вградени инструменти на дистрибуцията Kali-Linux-2017.3 като – Metasploit Framework, BurpSuite, OWASP-ZAP, paros, sqlmap и др. <p>Екипът на Сървис Центрикс ще приготви отчет с резултати от тестовете за пробив и съответните препоръки за отстраняване на уязвимости, които са използвани успешно при тестовете за пробив.</p>
<p>7.7. Извършване на тестове за пробив в избрани сървъри с бази данни от ИТ инфраструктурата на ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> • Използване на различни методи за добиване на достъп до избрани сървъри с бази данни; 	<p>Сървис Центрикс ще извърши тестове за пробив в избрани сървъри с бази данни от ИТ инфраструктурата на ИСУН2020 в ДХЧО.</p> <p>Върху избрани сървъри с бази данни от ИТ инфраструктурата на ИСУН2020 в ДХЧО ще бъдат извършени тестове за пробив с различни инструменти за тестове за пробив. Тези сървъри с бази данни ще бъдат определени според резултатите от сканиране за уязвимости и/или ще бъдат изрично посочени от представители на Възложителя. Екипът на Сървис Центрикс ще използва следните инструменти за тестове за пробив:</p> <ul style="list-style-type: none"> • Вградени инструменти на дистрибуцията Kali-Linux-2017.3 като – Metasploit Framework, BurpSuite, OWASP-ZAP sqlninja, mdb-sql, sqlmap и др. • Инструмент Havij

Изисквания и условия на Възложителя	Предложение на Сървис Центрикс ООД
	<p>Екипът на Сървис Центрикс ще приготви отчет с резултати от тестовете за пробив и съответните препоръки за отстраняване на уязвимости, които са използвани успешно при тестовете за пробив.</p>
<p>7.8. Извършване на тестове за пробив в избрани мрежови устройства от ИТ инфраструктурата на ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> • Използване на различни методи за добиване на достъп до избрани мрежови устройства; 	<p>Сървис Центрикс ще извърши тестове за пробив в избрани мрежови устройства от ИТ инфраструктурата на ИСУН2020 в ДХЧО.</p> <p>Върху избрани мрежови устройства от ИТ инфраструктурата на ИСУН2020 в ДХЧО ще бъдат извършени тестове за пробив с различни инструменти за тестове за пробив. Тези мрежови устройства ще бъдат определени според резултатите от сканиране за уязвимости и/или ще бъдат изрично посочени от представители на Възложителя. Екипът на Сървис Центрикс ще използва следните инструменти за тестове за пробив:</p> <ul style="list-style-type: none"> • Вградени инструменти на дистрибуцията Kali-Linux-2017.3 като – Metasploit Framework, armitage, cisco-auditing-tool, cisco-global-exploiter, cisco-ocs, cisco-torch и др. <p>Екипът на Сървис Центрикс ще приготви отчет с резултати от тестовете за пробив и съответните препоръки за отстраняване на уязвимости, които са използвани успешно при тестовете за пробив.</p>
<p>7.9. Изготвяне на отчет от извършените дейности по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> • Използване на най-добри практики при изготвяне на отчет от извършените дейности по тестове за пробив в ИТ системите; 	<p>Сървис Центрикс ще изготви отчет от извършените дейности по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <p>Екипът на Сървис Центрикс ще приготви отчет с резултати от всички гореизброени тестове за пробив и конкретни препоръки за отстраняване на уязвимости, които са открити и/или използвани успешно при тестовете за пробив.</p>

Изисквания и условия на Възложителя	Предложение на Сървис Центрикс ООД
<p>7.10. Изготвяне на списък с препоръки по отношение на открити слабости, резултат от извършените дейности по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <ul style="list-style-type: none"> • Приготвяне на списък с краткосрочни препоръки; • Приготвяне на списък с дългосрочни препоръки; 	<p>Сървис Центрикс ще изготви списък с препоръки по отношение на открити слабости, резултат от извършените дейности по тестове за пробив в ИТ системите на ИСУН2020 в ДХЧО.</p> <p>Екипът на Сървис Центрикс ще приготви отчет с резултати от всички гореизброени тестове за пробив и конкретни препоръки за отстраняване на уязвимости, които са открити и/или използвани успешно при тестовете за пробив. Ще бъде изготвен списък с краткосрочни препоръки и дългосрочни препоръки, които се определят според нивото на риск и усилията за отстраняване на откритите несъответствия/уязвимости.</p>
<p>8.Преглед на информационната система ИСУН2020 за съответствие с Общия регламент за защитата на данните (General Data Protection Regulation - GDPR)</p>	
<p>При прегледа на ИСУН2020 за съответствие с GDPR регламента екипът на Сървис Центрикс ще използва метода Планиране – Изпълнение – Проверка – Внедряване (Plan-Do-Check-Act). Методът гарантира цялостен подход към прилагане на изискванията на регламента, и ще бъде използван за оценка на текущата готовност, предприетите мерки, конфигурацията на услугите и нивото на информираност на служителите, поддържащи и развиващи ИСУН.</p> <p>Сървис Центрикс ще проведе поредица от срещи и интервюта със служителите, преглед на цялата налична документация и конфигурация на системите, съгласно изискванията на регламента.</p>	
<p>8.1. Организация на начина на работа с личните данни</p>	<p>Сървис Центрикс ще извърши одит на организацията на начина на работа с личните данни:</p> <ul style="list-style-type: none"> • Ще бъде анализирана организационната структура, отговорна за управление и обработка на личните данни • Ще бъдат анализирани всички процеси, които използват лични данни в някаква форма • Ще се провери изготвен ли е каталог на данните и неговата пълнота

55/16

Изисквания и условия на Възложителя	Предложение на Сървис Центрикс ООД
	<ul style="list-style-type: none"> • Ще бъдат анализирани всички документи, съдържащи клаузи за поверителност и обработка на лични данни, за пълнота и коректност • Ще бъдат анализирани всички форми и текстове за даване, промяна и оттегляне на съгласие за обработка на лични данни • Ще се оцени възможностите по реализиране на правото на субект да бъде забравен и заличаване на личните му данни • Ще се оцени възможността да се предоставят лични данни на субектите в електронно четим формат
8.2. Нива на защита на личните данни	<p>Сървис Центрикс ще извърши одит на нивата на защита на личните данни:</p> <ul style="list-style-type: none"> • Ще бъдат анализирани правилата за класификация на информация и документи, и рестрикциите, произлизащи от това • Ще бъде анализиран каталога на личните данни за различните видове данни, които се обработват • Ще бъдат анализирани идентифицираните рискове относно всеки вид лични данни • Ще бъдат оценени мерките за защита и методите за обработка съгласно идентифицираните рискове
8.3. Наличие на процедури за реакция при констатиране на компрометирани лични данни	<p>Сървис Центрикс ще извърши одит на наличните процедури за реакция при констатиране на компрометирани лични данни:</p> <ul style="list-style-type: none"> • Ще бъде анализирани текущите процедури за обработка на инциденти и пробиви съгласно стандарта ISO 27035 • Ще се ревизират методите за разпознаване на инцидент или пробив, известяването (нотификации) и съдържанието на отчета, който се изпраща • Ще се ревизира процесът на ескалация и уведомление на съответните заинтересовани страни и органи • Ще се ревизират стъпките за обработване и разрешаване на инцидентите
8.4. Процедура на действие при обмен на личните данни с международни инф. системи	<p>Сървис Центрикс ще извърши одит на процедурата на действие при обмен на личните данни с международни инф. системи:</p> <ul style="list-style-type: none"> • Ще се ревизират текущите договори и съответните клаузи, дефиниращи правата и задълженията на страните, спрямо член 47 от регулацията

21

Изисквания и условия на Възложителя	Предложение на Сървис Центрикс ООД
	<ul style="list-style-type: none">• Ще се ревизират дефинициите на организационните правила за обмен• Проверяване за трансфери извън обхвата на европейските закони• Проверяване за ситуации, покривани от член 49 и 50
8.5. Роли и отговорности по защита на личните данни	<p>Сървис Центрикс ще извърши одит на ролите и отговорностите по защита на личните данни:</p> <ul style="list-style-type: none">• Ще бъдат анализирани дефинираните роли и функции• Ще бъдат анализирани дефинираните задължения като Администратор на лични данни – регулярни и планирани (ако е приложимо)• Ще бъдат анализирани дефинираните задължения като Оператор на лични данни – регулярни и планирани (ако е приложимо)• Ще бъде анализиран изборът на ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ (DPO) – задължения, отговорности, правомощия, необходими експертни познания по информационна сигурност и защита на данните, ниво на съдействие и коопериране с компетентните органи• Преглед на записи за изпълнението на различни дейности
8.6. Преглед на системите от гледна точка за съответствие с GDPR	<p>Сървис Центрикс ще извърши преглед на системите от гледна точка за съответствие с GDPR:</p> <ul style="list-style-type: none">• Анализ на изготвените съпоставки на данните (data mapping)• Анализ на хранилищата на данни и нивото на тяхната защита• Анализ на ролите и отговорностите за управление на личните данни и необходимите им нива на достъп в системата• Анализ на методите за криптиране на данните• Анализ на методите за трансфер на чувствителни данни
8.7. Изготвяне на GAP анализ и план за действие за покриване на изискванията.	<p>Сървис Центрикс ще изготви GAP анализ и план за действие за покриване на изискванията:</p> <ul style="list-style-type: none">• След оценката на текущото състояние и разбиране за нивото на зрялост на текущите процеси, ще бъдат ясно дефинирани целите и очакваните крайни резултати от подготовката за спазване на регулацията. На тази база GAP анализът ще извърши съпоставка на текущото състояние спрямо изискванията на регламента, на базата

5/2/16

ИЗИСКВАНИЯ И
УСЛОВИЯ НА
ВЪЗЛОЖИТЕЛЯ

ПРЕДЛОЖЕНИЕ НА СЪРВИС ЦЕНТРИКС ООД

на което ще се изготвят отчет за несъответствията и план за тяхното преодоляване.

- GAP анализът ще се извърши посредством интервюта спрямо изискванията на всеки един член на регламента във формат:

Технически и организационни метрики	Изискване	Описание на текущото състояние	Текущо ниво на зрялост	Желано ниво на зрялост	Анализ на несъответствието	Отговорно лице

- Изготвяне на отчет от GAP анализа, съдържащ описание на GDPR изискванията и нивото на зрялост по категории
- На базата на GAP анализа ще се изготви детайлен план за имплементация, съдържащ:
 - Създаване на рамка за отчетност и управление
 - Дефиниране на обхват и планиране на проектите
 - Провеждане на инвентаризация на данните и одит на потоците от данни
 - Провеждане на подробен анализ на несъответствията
 - Разработване на оперативни политики, процедури и процеси
 - Комуникации и обучение
 - Непрекъснат мониторинг и одит на съответствието

9. Изисквания към реализацията на одита

Сървис Центрикс ще изпълни всички изисквания към реализацията на одита, съгласно точки 9.1 и 9.2 от Техническата спецификация.

Сървис Центрикс ще предостави пълен електронен доклад съдържащ резултатите от одита и анализа на данните, съгласно точка 9.3 от Техническата спецификация.

53/8

3 ОПИСАНИЕ НА ПОДХОД И МЕТОДОЛОГИЯ ЗА УПРАВЛЕНИЕ НА ПОРЪЧКАТА И ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИТЕ НА ПОРЪЧКАТА

Целта на тази точка е да опише подхода на изпълнителя към изпълнението на Обществена поръчка с предмет с предмет: „Одит на информационната сигурност на ИСУН2020“.

Използваният подход се основава на натрупания опит и знания на Участника от изпълнението на р азлични по обхват и сложност проекти, свързани с анализ, проектиране, разработване, тестване и в недряване на комплексни информационни системи в големи организации и държавната администрация.

За нуждите на настоящия проект използваният подход се адаптира в зависимост от спецификата н а обществената поръчка и нуждите на Възложителя.

3.1 Използвани методологии

За реализирането на изискванията от техническата спецификация на Възложителя предлагаме да се използва методологията за цялостно управление на проекти на PMI (Project Management Institute).

3.2 Методология за управление на проекти

Въз основа на натрупания опит ние предлагаме използването на методологията на PMI (Project Management Institute) за цялостното управление на проекта. По-долу са описани принципите на тази методология, базирана на Project Management Body Of Knowledge (PMBOK).

Project Management Body Of Knowledge (PMBOK) е сбор от процеси и сфери на знание, широко приети като най-добра практика в дисциплината "Управление на проекти". Този международно признат стандарт (IEEE Std 1490-1998) е в основата на управлението на проекти. Според PMBOK съществуват 5 основни групи процеси (стартиране, планиране, изпълнение, проследяване и контрол, приключване) и 9 сфери на знание (управление на интеграцията на проекта, на обхвата, на времето, на разходите, на качеството, на човешките ресурси, на комуникациите, на риска и на доставките). Във всеки проект или фаза процесите се застъпват и си взаимодействат. Те се описват от гледна точка на вход (документи, планове, проекти), инструменти и техники (механизми, прилагани върху входящите данни) и изход (документи, продукти, резултати).

Основните цели на методологията на PMI са:

- Контролиране на обхвата, графика, разходите и качеството
- Намаляване и управляване на риска
- Управление на ресурсите
- Идентифициране на дейностите по проекта

24

5/5/16

- Координиране на комуникациите между заинтересованите страни
- Съобразяване на работата с бизнес целите на Възложителя.

За постигане на горните цели методологията е съсредоточена върху следните 9 сфери на знание:

- Управление на интеграцията
- Управление на обхвата
- Управление на времето
- Управление на разходите
- Управление на качеството
- Управление на човешките ресурси
- Управление на комуникациите
- Управление на риска
- Управление на доставките

Процесите по управление на проекта са организирани в пет групи:

- Стартирането включва процесите, които се изпълняват при възлагането на роли и определянето на обхвата на нова фаза или проект.
- Планирането включва процесите, които се изпълняват при определянето и промяната на обхвата на проекта, разработването на плана за управление на проекта и планирането на дейностите по проекта.
- Изпълнението включва процесите по извършване на зададената работа и постигане на целите на проекта, залегнали в обхвата.
- Проследяването и контролът включва процесите, необходими за стартирането, планирането, изпълнението и приключването на проекта в съответствие с целите, зададени в обхвата и плана за управление на проекта.
- Приключването включва процесите, които се изпълняват при официалното прекратяване на всички дейности по дадена фаза или проект и предаването на готовия продукт.

Всяка група процеси се състои от един или повече управленски процеси. Групите са свързани — често изходът на даден процес се превръща във вход на друг. При централните групи процеси има итерация на връзките — планирането осигурява на изпълнението първоначален документиран план на проекта, след което осигурява актуализации на плана в хода на работата. Кратко описание на деветте сфери на знание съгласно методологията на PMI:

- Управление на интеграцията

Процесите по управление на интеграцията гарантират правилната координация на различните елементи на проекта. Те включват балансиране на целите и алтернативите с



 25

25/6

оглед на нуждите и очакванията на заинтересованите страни. Описаните в тази глава процеси са предимно интегративни.

- Разработване на план на проекта

При разработването на плана на проекта се използват резултатите от други планиращи процеси, включително стратегическо планиране, за да се създаде един ясен и последователен документ, който да насочва и изпълнението, и контрола на проекта. Този процес минава през няколко итерации. Сборът от всички интегрирани планове за управленски контрол съставлява обхвата на проекта.

- Изпълнение на плана на проекта

Изпълнението на плана на проекта е основен процес при осъществяването на плана - преобладаваща част от бюджета и усилията по проекта се изразходват при извършването на този процес. Чрез него ръководителят на проекта и неговия екип координират и насочват техническите и организационните интерфейси. В рамките на този процес фактически се създава продуктът на проекта. Изпълнението постоянно ще се сравнява с основния план на проекта, за да се вземат своевременни корективни мерки. В подкрепа на анализа ще се правят периодични прогнози за окончателните разходи и резултати.

- Интегриран контрол на промените

Интегрираният контрол на промените се занимава с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат. Първоначално дефинираният обхват и интегрираният основен план на проекта се поддържат чрез постоянно управление на възникналите промени чрез приемане или отхвърляне на промените и включването им в актуализираната версия на основния план. Интегрираният контрол на промените изисква:

- Поддържане интегритета на базовите измерители на изпълнението.
- Отразяване на промените в обхвата на продукта във вече дефинирания обхват.
- Координиране на промените във всички сфери на знание.

- Управление на обхвата

Управлението на обхвата на проекта включва процесите, които гарантират, че проектът включва цялата необходима работа и само необходимата работа за успешното осъществяване на проекта. То се занимава най-вече с определянето и контролирането на това какво е включено и какво не е включено в проекта. Стартирането е процесът на официалното възлагане на нов проект. Официалното възлагане на този проект ще бъде подписването на договор, което ще свърже проекта с работата на изпълнителя. Планирането на обхвата е процесът на детайлизиране и документиране на работата по проекта (обхвата на проекта), чийто резултат ще бъде продуктът на проекта. Описанието на продукта обхваща изискванията, които отразяват съгласуваните нужди на клиента, и дизайн, който отговаря на тези изисквания. Резултатите от планирането на обхвата са Дефиниция на обхвата и План за управление на обхвата.

25/6

26

Дефиницията на обхвата е основата за постигане на споразумение между възложителя и изпълнителя, чрез идентифициране на целите и резултатите по проепа. След стартирането на проекта екипите разработват множество дефиниции на обхвата, в съответствие с нивото на детайлизиране на работата (напр. Анализ на текущото състояние, подробен график и др.). Определянето на обхвата включва разбиването на основните резултати, посочени в Дефиницията на обхвата, на по-малки, по-управляеми елементи. Целта е:

- Подобряване на прогнозите за разходи, продължителност и ресурси.
- Определяне на основни параметри за измерване на изпълнението и контрол.
- Ясно разпределяне на отговорностите.

Потвърждаването на обхвата е процесът по официално приемане на обхвата на проекта от заинтересованите страни. Той изисква преглед на резултатите от работата и потвърждение, че всичко е свършено както трябва. Ако проектът се прекратява преждевременно, потвърждението на обхвата трябва да документа нивото и степента на завършеност. Контролът на промените в обхвата се занимава с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат.

- Управление на времето

Управлението на времето по проекта включва следните процеси, необходими за навременното приключване на проекта:

- Определяне на дейностите — идентифициране и документиране на конкретните дейности, необходими за постигане на набелязаните резултати и под-резултати. Определянето на дейностите се съгласува с Дефиницията на обхвата и включва детайлизиране, предположения и ограничения.
- Последователност на дейностите - идентифициране и документиране на логическите взаимозависимости. Дейностите трябва да бъдат в правилна последователност, за да спомогнат за разработването на реалистичен и постижим график. Последователността може да следва критичната пътека. В резултат се определя график със съответните контролни точки и зависимости.
- Продължителност на дейностите — определя се въз основа на информацията за обхвата на проекта и ресурсите. Предварителната оценка ще се детайлизира в хода на работата, предвид наличието и качеството на входящите данни. Оценката се прави по методологията на критичната пътека.

- Определяне на график — задава се началната и крайната дата на дейностите по проекта. Процесът преминава през няколко итерации преди окончателното определяне на графика на проекта.
- Контрол на графика — занимава се с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат.

- Управление на разходите

Планирането на ресурсите включва определяне на количеството и качеството на необходимите ресурси (хора, техника, материали), както и сроковете на тяхното използване. То е тясно свързано с оценката на разходите. Оценката на разходите включва прогнозно определяне на разходите за необходимите ресурси. Вземат се предвид причините за отклонение от окончателната прогноза, за да се осигури по-добро управление на проекта.


Бюджетирането на разходите включва разпределяне на общите прогнозни разходи по дейности или групи дейности, за да се установи базовата цена, спрямо която ще се измерва изпълнението. Действителността може да наложи изготвяне на прогнози след одобрението на бюджета, но по възможност те трябва да се правят предварително. Контролът на разходите се занимава с факторите, които влияят върху пораждането на промени, грижи се за съгласуването на промените, констатира наличието на промени и ги управлява, когато възникнат. Контролът на разходите включва:

- Проследяване изпълнението на бюджета, за да се открият и разберат разминаванията с плана.
- Точно отразяване на необходимите промени в базовата цена.
- Предотвратяване на включването на ненужни или неразрешени промени в базовата цена.
- Информирание на съответната страна за одобрени промени.
- Осъществяване на очакваните разходи в приемливи граници.

- Управление на качеството

Целта на процесите по управление на качеството е да бъдат задоволени нуждите, заради които е предприет проекта. Тези процеси включват всички дейности от цялостното управление на проекта, които определят политиката, целите и отговорностите по качеството и ги осъществяват чрез планиране на качеството, гарантиране на качеството, качествен контрол и подобряване на качеството в рамките на системата за качество. Идентифициране на стандартите за:

- Планиране на качеството за конкретния проект и начините за спазването им. Това е един от ключовите процеси при планиране на качеството и ще се извършва редовно, успоредно с останалите процеси по планиране на проекта.

- 
- Гарантиране на качеството — всички планирани и систематични действия в рамките на системата за качество, които дават увереност, че проектът ще отговаря на съответните стандарти. ще се извърша в хода на целия проект от вътрешни Специалисти по качеството.
 - Качествен контрол — проследяване на конкретни резултати, за да се определи дали отговарят на зададените стандарти и да се набележат начини за отстраняване на причините за незадоволителните резултати. Ще се извърша в хода на целия проект. Резултатите включват както доставката на конкретен резултат/продукт, така и резултати от управлението на проепа (изпълнение на бюджета и графика). Би било полезно да се знае разликата между:

- Предотвратяване (недопускане на грешки в процеса) и проверка (недопускане на грешки от страна на клиента).
- Изпробване на атрибути (резултатът отговаря или не отговаря) и изпробване на променливи (резултатите се измерват по прогресивна скала за степен на съответствие).
- Специални причини (необичайни събития) и случайни причини (нормално отклонение от процеса).
- Допустимост (резултатът е приемлив, ако попада в посочения обхват на допустимост) и контролни граници (процесът е под контрол, ако резултатът е в рамките на контролните граници).

- Управление на човешките ресурси

Управлението на човешките ресурси включва процесите, които осигуряват най-ефективното използване на хората, участващи в проепа. То обхваща всички заинтересовани страни — клиенти, партньори, индивидуални изпълнители и др. Състои се от:

- Идентифициране, документиране и организационно планиране
- Определяне на роли, отговорности и канали за отчитане
- Осигуряване на необходимите човешкиресурси и включването им в работата по проекта
- Набиране на персонал
- Развитие на екипа — развиване на индивидуални и групови умения, с цел подобряване на изпълнението.

- Управление на комуникациите

Процесите по управление на комуникациите осигуряват навременното и адекватно генериране, събиране, разпространение, съхранение и унищожаване на информацията по проекта. Те осъществяват критичната за успеха връзка между хора, идеи и данни. Всеки участник в проекта трябва да е готов да изпраща и приема комуникации и трябва да разбира как каналът на комуникация, в която участва, се отразява на целия проект.

Планиране на комуникациите определяне на нуждите на заинтересованите страни от информация и комуникации: кой от каква информация се нуждае, как ще я получи и от

кого. Нуждата от предоставяне на информация за проекта е общовалидна, но информационните нужди и методите на разпространение са различни за всеки проект. Идентифицирането на нуждата от информация и разпространяването ѝ по подходящ начин е важен фактор за успех на проекта.

- Разпространение на информацията — своевременното достигане на информацията до заинтересованите страни. Включва прилагането на Плана за комуникация и откликването на неочаквани искания на информация.
- Отчитане на изпълнението — събиране и разпространение на данни за изпълнението, показателни за използването на ресурсите за постигане на целите на проекта. Този процес включва:
 - Отчитане на състоянието — описва докъде е стигнал проектът в дадения момент
 - Отчитане на напредъка — описва какво е постигнал екипът по проекта
 - Прогнозиране — предполага бъдещото състояние и напредък по проекта. — данни за обхвата, графика
 - Отчитане на изпълнението разходите и качеството.
- Административно приключване: след постигане на целите или след прекратяване по други причини, проектът или фазата трябва да приключи. Административното приключване се състои от документиране на резултатите, с цел официалното приемане на продукта от страна на клиента. То включва събиране на проектната документация, която отразява окончателните спецификации, анализ на успеха и ефективността на проекта и на извлечените поуки, и архивиране на тази информация за бъдещо ползване. Дейностите по административното приключване не се отлагат до приключването на проекта. Всяка фаза трябва да бъде надлежно приключена, за да не бъде загубена тази важна и полезна информация.

Комуникационен план - Добрата комуникация по време на проекта води до постигане на резултатите на проекта. По-долу е представен образец на комуникационен план, който ще се използва в рамките на изпълнение на проекта.

Какво	Кой/за кого	Цел	Кога/ Честота на изпълнение	Тип/Метод

- Управление на доставките

30

Управлението на доставките от трети лица се занимава с придобиването на стоки и услуги от външни за изпълнителя организации. Този процес се състои от:

- Планиране на доставките
- Планиране на търсенето
- Избор на източник
- Администриране на договори
- Приключване на договори

3.3 Роли и отговорности в проекта

От страна на Сървис Центрикс в проекта ще бъдат включени следните участници със съответните роли:

Роля	Експерт
Ръководител проект	Сертифициран ръководител проекти с дългогодишен опит в проекти по информационна сигурност
Експерт по информационна сигурност 01 (Експерт ИС 01)	Експерт, притежаващ CISSP и CDPO сертификации
Експерт по информационна сигурност 02 (Експерт ИС 02)	Експерт, притежаващ CRISC и ECSA сертификации
Инфраструктурен експерт	Експерт с познания по операционни системи и мрежова инфраструктура

3.4 Дейности по проекта и график на изпълнение

Дейност	Роли	Седмица от проекта (общо 12)											
		1	2	3	4	5	6	7	8	9	10	11	12
Стартираща среща	Ръководител проект												
Създаване на организация за работа и подготовка	Ръководител проект; Инфраструктурен експерт												
Одит на информационната сигурност на ИСУН2020	Експерт ИС 01; Експерт ИС 02; Инфраструктурен експерт												
Тестове за пробив в сигурността на ИТ системите на ИСУН2020	Експерт ИС 02; Инфраструктурен експерт;												
Преглед на информационната система ИСУН2020 за съответствие с GDPR	Експерт ИС 01; Инфраструктурен експерт												
Анализ и изготвяне на доклади и планове	Експерт ИС 01; Експерт ИС 02; Инфраструктурен експерт												
Среща за приключване на проекта и представяне на резултатите	Ръководител проект; Експерт ИС 01; Експерт ИС 02;												

Handwritten signature

3.5 Контрол на качеството

Фокусът на контрола върху качеството е върху резултатите от проекта. Контролът на качеството следи резултатите от проекта, за да се увери, че продуктите са с приемливо качество и клиентът е удовлетворен.

Следващата таблица идентифицира:

- Основните резултати от проекта, които ще бъдат тествани за изискваното ниво на качество (Дефинират се от Възложителя при стартиране на проекта)
- Стандартите за качество и критериите за удовлетвореност на Възложителя, определени за проекта. Включени са всички организационни стандарти, които трябва да се спазват.
- Дейностите по контрол на качеството, които ще бъдат изпълнени, за да се наблюдава качеството на продуктите.
- Колко често или кога ще се извършва дейността по качествен контрол.
- Името на лицето, отговорно за извършването и отчитането на дейността по контрол на качеството.


Резултат от проекта	Стандарти за качество на резултатите (Определят се от Възложителя) / Ниво на удовлетвореност на клиента	Дейности по контрол на качеството	Честота на извършване/ интервал	Отговорник

По-долу са дадени примери за инструменти, които могат да бъдат използвани за подпомагане на изпълнението на управлението на качеството.

Инструмент	Предназначение/ Използване
------------	----------------------------

Handwritten signature

Handwritten signature




Анализ на съотношение цени / ползи	За контрол на качеството
Цена на качеството	За контрол на качеството
Одити на качеството	За оценка на качеството и тестване
Анализ на процеси за управление на проекта	За оценка на качеството и тестване

5 ОПИСАНИЕ НА ПОДХОДА ЗА УПРАВЛЕНИЕ НА РИСКА ПРИ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

Управлението на риска е систематичният процес по идентифициране, анализиране и реагиране на рисковете по проекта. То включва максимизиране на вероятността и последствията от благоприятни събития и минимизиране на вероятността и последствията от нежелателни за проекта събития. Проектният риск е несигурно събитие или състояние, което, ако се случи, има положително или отрицателно влияние върху целите на проекта.

Рискът има причина и, ако се материализира, последствие.

- Планиране на управлението на риска - процесът на определяне на подхода и дейностите по управление на риска. Важно е да се планират и последващите процеси по управление на риска, за да има съизмеримост между нивото, вида и прозрачноста на управление на риска от една страна и самия и риск и важноста на проекта за организацията от друга.
- Идентификация на риска — определяне на рисковете, които могат да повлияят на проекта, и документирането на техните характеристики. Участници в процеса на определяне на риска са: екипът по проекта, екипът по управление на риска, специалисти от други клонове на фирмата, клиенти, крайни потребители, други ръководители на проекти и външни експерти. Определянето на риска е итеративен процес. Първата итерация може да се осъществи от част от екипа по проекта или от екипа по управление на риска. Целият екип по проекта и основните заинтересовани лица могат да осъществят втора итерация. Щом бъде идентифициран даден риск, се разработват и внедряват прости и ефективни мерки за преодоляването му.
- Качествен анализ на риска — оценка на влиянието и вероятността от даден риск. Този процес приоритизира рисковете според евентуалното им влияние върху целите на проекта. Качественият анализ на риска е един от начините за определяне важноста на дадени рискове и насочване на усилията към справяне с тях. Времето за реакция може да е критичен фактор при някои рискове. Оценката на качеството на наличната информация също спомага при преоценката на риска. Качественият анализ на риска изисква оценка на вероятностите и последствията, чрез установени методи и инструменти.
- Количественият анализ на риска е цифровото изражение на вероятността от даден риск и последствията му върху целите на проекта. В този процес ще се използва техника, базирана на опростяване на симулацията "Монте карло" и анализ на решенията, с цел:
 - Определяне на вероятността за постигане на дадена цел по проекта.
 - Изчисляване на вероятностите за излагане на проекта на риск и определяне на резервни разходи и график.

- 
- Откриване на рисковете, които изискват най-голямо внимание, чрез изчисляване на относителната им тежест за проекта.
 - Идентифициране на реалистични и постижими разходи, график или обхват.
 - Планирането на реакции на риска е процесът на разработване на и определяне на действия, варианти които увеличават възможностите и намаляват заплахите за осъществяване целите на проекта. Той включва възлагане на отговорности на отделни лица или групи във връзка с действията при отделните рискове. Този процес гарантира адекватна реакция на идентифицираните рискове. Ефективността на планирането на реакции е пряко свързана с увеличаването или намаляването на рисковете по проекта.
 - Наблюдението и контролът на риска е процесът по проследяване на идентифицираните рискове, наблюдаване на остатъчни рискове и откриване на нови рискове. Той спомага за осъществяването на плановете за риска и оценката на ефективността им. Това е постоянен процес в хода на проекта. С времето рисковете се променят, появяват се нови, някои очаквани рискове не се материализират. Доброто наблюдение и контрол на рисковете дава и информация, която подпомага взимането на ефективни решения преди материализирането на риска.

Контролът на риска може да включва избор на алтернативна стратегия, прибягване до резервен план, извършване на коригиращи действия или повторно планиране на проекта. Ръководителят на проекта и ръководителят на екипа за риска периодично получават информация за ефективността на плана и наличието на неочаквани влияния и взимат съответните мерки в хода на проекта.

5.1 Процес по управление на риска

- Идентифициране на рисковете - Тази стъпка идентифицира потенциалните рискове на проекта. Основни методи за идентифициране на рисковете са:
 - Периодична проверка и анализ на вътрешни и външни фактори, които имат пряка или косвена зависимост с резултати от проекта;
 - Следене за възникване на събития, свързани с:
 - ✓ други проекти
 - ✓ промени в законодателството
 - ✓ отклонения от спецификациите
 - ✓ предоставяне на информация необходима на продукт на проекта
 - ✓ взимане на решения
 - ✓ отделени ресурси и внимание от участниците в проекта
 - ✓ промени в процедурите

- ✓ техническата среда
- ✓ сигурност на информация

25

Веднъж идентифицирани, рисковете се въвеждат в Регистъра на рисковете (Risk register). Той съдържа детайли за всички рискове, тяхната оценка, собственици и статус.

В регистъра на рисковете се използвани следните понятия:

- Риск - условие (източник на риска) и последствия
- Вероятност – вероятността рискът да се случи (Висока (H), Средна (M) и Ниска (L))
- Въздействие – ниво на относителни загуби (Високо (H), Средно (M) и Ниско (L))
- Мерки за избягване/ смекчаване – дейности за предотвратяване на риска
- План за възстановяване – дейности, планирани в отговор на сбъдването на риска или свързано събитие

Ще бъде създаден регистър на рисковете, който ще използва следния формат:

Риск	Вероятност	Въздействие	Приоритет	Мерки за избягване/ смекчаване/ възстановяване	План за възстановяване	Собственик на риска

- Оценка на рисковете - Оценката на рисковете се прави на база оценка на възможността да се случат, влияние, взаимна връзка между отделните рискове:
 - Възможността е оценена вероятност да се появи риска.
 - Влиянието е преценения ефект или резултат от появата на риска.
 - Влиянието се оценява на база на:
 - ✓ време
 - ✓ разход
 - ✓ качество
 - ✓ обхват
 - ✓ ползи
 - ✓ хора/ресурси.

Рамката за категоризиране на рисковете може да бъде високо, средно или слабо влияние.

- Определяне на стратегии за управление на рисковете - Биват 5 типа:

26

27

- Предпазване – преустановяване на риска чрез избиране на действия, които го предотвратяват.
 - Ограничаване – предприемане на действия, които или намаляват вероятността за появата на риска, или намаляват неговото влияние върху проекта до приемливи нива.
- Трансфериране – специална форма на ограничаване на риска, когато рискът се трансферира на трета страна, например чрез застраховане.
 - Приемане – допускане на риска поради най-вероятно невъзможността да се предприеме друго действие на приемлива цена.
- Овластяване – действия, които са планирани и организирани да бъдат предприети при случайно възникване на рисковата ситуация
- Избор - Изборът на действие е баланс между множество фактори. След идентифицирането и оценката на рисковете, е необходимо да се изготви и план за управление на риска, в които са описани контролните действия. Всяко контролно действие, от своя страна, е обвързано с асоцииран разход. Контролното действие е такова, че разходът за него трябва да е по-приемлив от риска, който контролира.
- Планиране и ресурсно обезпечение. Планирането включва:
 - Определяне на количеството и типа ресурси, необходими за извършване на споменатите дейности
 - Разработване на подробен план за действие;
 - Потвърждение на желанието за извършване на дейностите, идентифицирани по време на оценка на рисковете
 - Получаване на одобрение от ръководството
 - Определяне и възлагане на задачи на ресурси за извършване на определените дейности
 - Ресурсите, необходими за дейностите по превенция, редуциране и прехвърляне на рисковете, следва да се финансират от бюджета на проекта.
- Мониторинг и отчитане - Изпълнителят ще обърне специално внимание на мониторинга и отчитането на дейностите по рисковете. Някои от дейностите ще включват наблюдение на идентифицираните рискове за промени в техния статус, а други ще включват:
 - Проверка, че планираните дейности имат очаквания ефект
 - Наблюдение за ранни сигнали за поява на риск
 - Моделиране на насоки за предсказване на потенциални рискове
 - Проверка, че цялостното управление на риска се прилага ефективно


5.2 Регистър на рисковете

Риск	Вероятност	Въздействие	Приоритет	Мерки за избягване/ смекчаване/ възстановяване	План за възстановяване	Собственик на риска
Недобра комуникация между екипите на Възложителя и Изпълнителя по време на различните етапи на изпълнение на проекта, в резултат на което може да се получи непостигане на целите на проекта;	Ниска	Високо	Среден	Детайлен анализ на всички заинтересовани страни при стартирането на проекта; Дефиниране на роли и отговорности; Изготвяне на подробен план за комуникация; Периодични прегледи на обратната връзка и нивата на удовлетвореност при изпълнение на изискванията на проекта.	Извършване на повторно планиране и включване на изпуснатите дейности в проекта.	Ръководител на проекта
Недостатъчна яснота по правната рамка и/или променяща се правна рамка по време на изпълнение на проекта, което може да доведе до концептуални непълноти и разминавания между цели и резултати;	Ниска	Средно	Нисък	Включване на експерти с юридически познания с цел анализ на правната рамка и събиране на допълнителни изисквания. Анализ на заинтересованите страни и включване на допълнителни участници от страна на Възложителя	Извършване на повторно планиране и включване на изпуснатите дейности в проекта.	Представител на Възложителя

33

34

Риск	Вероятност	Въздействие	Приоритет	Мерки за избягване/ смекчаване/ възстановяване	План за възстановяване	Собственик на риска
Неправилно и неефективно разпределяне на ресурсите и отговорностите по предоставянето на услугата;	Ниска	Високо	Среден	Ясно дефиниране на организационна структура на проекта, роли и отговорности; Назначаване на Ръководител проект от страна на Възложителя с достатъчно високи правомощия;	Извършване на повторно планиране, включване на допълнителни ресурси и корекция на графика на проекта.	Ръководител на проекта
Забавяне при изпълнение на проектните дейности, опасност от неспазване на срока за изпълнение на настоящата поръчка;	Ниска	Високо	Среден	Дефиниране и прилагане на ефективен план за комуникация; Свеовременна ескалация при откриване на забавени задачи;	Извършване на повторно планиране, включване на допълнителни ресурси и корекция на графика на проекта.	Ръководител на проекта
Липса на задълбоченост при изследването и описанието на	Ниска	Високо	Среден	Прецизиране на изискванията от заинтересованите страни; Свеовременна ескалация при	Включване на експерти с богат опит по	Представител на Възложителя –



Риск	Вероятност	Въздействие	Приоритет	Мерки за избягване/ смекчаване/ възстановяване	План за възстановяване	Собственик на риска
нормативните документи и бизнес процесите;				откриване на некачествено изпълнени задачи;	информационна сигурност и анализ на данни и процеси.	отговорник по качеството
Неинформиране на Възложителя за всички потенциални проблеми, които биха могли да възникнат в хода на изпълнение на дейностите.	Ниска	Високо	Среден	Задаване на ясни критерии и съдържание на отчети, съобщения и др. в плана за комуникация; Свеовременна ескалация при откриване на нови рискове, потенциални проблеми, неясни резултати и т.н.;	Коригиране на планът за комуникация; Предефиниране на критериите за оценка на ефективността на проектното управление.	Висш представител на ръководството на Възложителя

6 ИЗВЪН ОБХВАТА НА НАСТОЯЩОТО ПРЕДЛОЖЕНИЕ

Следните дейности се считат извън обхвата на офертата:

- промени по текущата ИТ инфраструктура

Срокът за изпълнение на настоящата поръчка е 3 месеца, считано от датата на подписване на договора.

Срокът на валидност на настоящото техническо предложение е 90 (деветдесет) дни след изтичане на срока за подаване на оферти.

Декларираме, че при изготвяне на офертата са спазени задълженията, свързани с данъци и осигуровки, опазване на околната среда, закрила на заетостта и условията на труд, които са в сила в страната.

Гарантираме, че сме в състояние да изпълним качествено и в срок поръчката, в пълно съответствие с гореописаното предложение и с Техническата спецификация.

ПОДПИС и ПЕЧАТ:

Владимир Кънчев (име и фамилия)

управител (длъжност на представляващия участника)

Дата: 23.04.2018

До
Администрация на Министерския
съвет
гр. София, бул. „Дондуков” № 1

ЦЕНОВО ПРЕДЛОЖЕНИЕ

за обществена поръчка, възлагана чрез събиране на оферти с обява по реда на
Глава Двадесет и шеста от ЗОП

От участник:

Сървис Центрикс ООД (наименование на участника), ЕИК/БУЛСТАТ: 200027636
представявано от Владимир Кънчев Кънчев /трите имена/, в качеството на управител
/длъжност, или друго качество/, адрес гр. София, бул. Александър Малинов 85, ет.6, офис
20 телефон: 02/ 483 76 90 факс, електронна поща
info@servicecentrix.com

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

Във връзка с обявената от Вас обществена поръчка по реда на Глава Двадесет и
шеста от ЗОП с предмет: „Одит на информационната сигурност на ИСУН2020”
представяме нашата ценова оферта за изпълнение на обществената поръчка, както
следва:

Общата предлагана от нас цена за изпълнение на поръчката възлиза на 69
400 (шестдесет и девет хиляди и четиристотин) лева без ДДС или 83 280 (осемдесет
и три хиляди двеста и осемдесет) лева с ДДС.

Декларирам, че посочената цена е крайна и включва всички разходи, свързани с
качественото изпълнение на поръчката, в това число разходи за транспорт, консумативи,
такси, възнаграждения на екипа на участника и други разходи.

Срокът на валидност на настоящата оферта е 90 (деветдесет) дни след изтичане
на срока за подаване на офертата.

ПОДПИС и ПЕЧАТ:

Владимир Кънчев (име и фамилия)

Управител (длъжност на представляващия участника)

Дата: 23.04.2018



43

Приложение № 4

Списък на персонала по чл. 64, ал. 1, т. 6 от ЗОП,

за който ще изпълнява обществена поръчка по чл. 20, ал. 3 от ЗОП с предмет: „Одит на информационната сигурност на ИСУН2020“.

„Сървис Центрик“ ООД разполага с екип от експерти, с образование и професионална квалификация, в съответствие с изискванията на Възложителя, както следва:

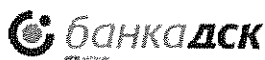
№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение																								
1	Владимир Кънчев Кънчев	Образование: Магистър Изчислителна техника, № 003536/януари, 1995 Технически университет – град Русе	Общ професионален опит: 22 години Професионален опит в изпълнението на проекти, включващи анализ, разработка и внедряване на система за управление на информационната сигурност Сертификати: - Сертификат CISSP (Certified Information Systems Security Professional) с № 71322 Валидност на сертификата: 31.05.2020 - Сертификат CDPO (Certified Data Protection Officer) № DPCDPO1022713-2017-09 Дата на издаване: 19.09.2017 Валидност на сертификата: 19.09.2020 Проекти: <table><tr><th>Период</th><th>Проект</th><th>Роля</th></tr><tr><td>- 07.2011 - 12.2017</td><td>Проект в МВР, ДКИС – “Разширяване на съществуващата РКІ инфраструктура в мрежата за предаване на данни в МВР”</td><td>Проект: Внедряване на ITSM роля;</td></tr><tr><td>- 2016-2017</td><td>Societe Generale Експресбанк, Проект: Внедряване на ITSM роля;</td><td>Проект: Внедряване на Agile най-добри проектни практики;</td></tr><tr><td>- 2015-2016</td><td>Борика Банксервис; Проект: Одит Информационна Сигурност;</td><td>Проект: Внедряване на ISO 20000; роля:</td></tr><tr><td>- 2015</td><td>Министерство на Външните Работи, Проект: Внедряване на ISO 20000; роля:</td><td>Проект: Внедряване на ITIL процеси и архитектурни практики</td></tr><tr><td>- 2015 - Скейл Фокус; Проект: Внедряване на ISO 20000;</td><td>Проект: Автоматизация на процес;</td><td></td></tr><tr><td>- 2015</td><td>Министерство на Външните Работи; Проект: Автоматизация на процес;</td><td>Проект: Внедряване на нови технологии за подобряване на сигурността на министерството;</td></tr><tr><td>- 2014</td><td>Министерство на Външните Работи; Проект: Внедряване на нови технологии за подобряване на сигурността на министерството;</td><td></td></tr></table>	Период	Проект	Роля	- 07.2011 - 12.2017	Проект в МВР, ДКИС – “Разширяване на съществуващата РКІ инфраструктура в мрежата за предаване на данни в МВР”	Проект: Внедряване на ITSM роля;	- 2016-2017	Societe Generale Експресбанк, Проект: Внедряване на ITSM роля;	Проект: Внедряване на Agile най-добри проектни практики;	- 2015-2016	Борика Банксервис; Проект: Одит Информационна Сигурност;	Проект: Внедряване на ISO 20000; роля:	- 2015	Министерство на Външните Работи, Проект: Внедряване на ISO 20000; роля:	Проект: Внедряване на ITIL процеси и архитектурни практики	- 2015 - Скейл Фокус; Проект: Внедряване на ISO 20000;	Проект: Автоматизация на процес;		- 2015	Министерство на Външните Работи; Проект: Автоматизация на процес;	Проект: Внедряване на нови технологии за подобряване на сигурността на министерството;	- 2014	Министерство на Външните Работи; Проект: Внедряване на нови технологии за подобряване на сигурността на министерството;		Сертифициран експерт
Период	Проект	Роля																										
- 07.2011 - 12.2017	Проект в МВР, ДКИС – “Разширяване на съществуващата РКІ инфраструктура в мрежата за предаване на данни в МВР”	Проект: Внедряване на ITSM роля;																										
- 2016-2017	Societe Generale Експресбанк, Проект: Внедряване на ITSM роля;	Проект: Внедряване на Agile най-добри проектни практики;																										
- 2015-2016	Борика Банксервис; Проект: Одит Информационна Сигурност;	Проект: Внедряване на ISO 20000; роля:																										
- 2015	Министерство на Външните Работи, Проект: Внедряване на ISO 20000; роля:	Проект: Внедряване на ITIL процеси и архитектурни практики																										
- 2015 - Скейл Фокус; Проект: Внедряване на ISO 20000;	Проект: Автоматизация на процес;																											
- 2015	Министерство на Външните Работи; Проект: Автоматизация на процес;	Проект: Внедряване на нови технологии за подобряване на сигурността на министерството;																										
- 2014	Министерство на Външните Работи; Проект: Внедряване на нови технологии за подобряване на сигурността на министерството;																											

№	Три имена на експерта	Образование / Квалификация	Професионален опит	Позиция в екипа за изпълнение
2	Станимир Иванов Сотиров	образование: магистър специалност: Автоматика, информационна и управляваща техника. № 82245/29.11.2002 г. Технически университет София	<p>Общ професионален опит: 11 години Професионален опит в изпълнението на проекти, включващи анализ, разработка и внедряване на система за управление на информационната сигурност</p> <p>Сертификати</p> <ul style="list-style-type: none"> - Сертифициран ISACA CRISC с № 1519225 Дата на издаване: 22.09.2015 Дата на валидност: 31.01.2019 - Сертифициран EC-Council ECSA v9 с № ECC62374876689 Дата на издаване: 17.03.2017 Дата на валидност: 16.03.2020 <p>Проекти</p> <ul style="list-style-type: none"> 06.2015, Проект в Hamilton Data Services: "Тест и одит на уеб приложение – с цел повишаването на нивото на ИТ сигурност и намаляване на риска." 12.2015, Проект в Транскарт ЕАД: "Тест и одит на уеб приложение – с цел повишаването на нивото на ИТ сигурност и намаляване на риска." 01.2016, Проект в EOS Матрикс: "Планиране, доставка, имплементиране и тестове на Next Generation Firewall устройство - според най-добри практики за ИТ сигурност и риск." 02.2016, Проект в TELUS International Бигоре: "Планиране, доставка, имплементиране и тестове на прокси устройства - според най-добри практики за ИТ сигурност и риск." 09.2016, Проект в АктивТрейдс: "Анализ и препоръки за текущата ИТ инфраструктура по отношение на риск, сигурност и производителност." 12.2016, Проект в АктивТрейдс: "Планиране, доставка, имплементиране и тестове на Next Generation Firewall устройство - според най-добри практики за ИТ сигурност и риск." 07.2017- 12.2017 Проект в МВР, ДКИС – "Разширяване на съществуващата РКІ инфраструктура в мрежата за предаване на данни в МВР" 	Сертифициран експерт

14.05.2018г.

Полпис и печат:
Владимир Кръчев
Управляещ





ИЗДАДЕН БЮДЖЕТЕН ПРЕВОД

ОВ61405180016829

Уникален регистрационен номер:

Статус: Осчетоводен

14.05.2018

Платете на - Име на получателя АДМИНИСТРАЦИЯ НА МИНИСТЕРСКИЯ СЪВЕТ				
IBAN / Сметка на получателя BG38BNBG96613300157901			BIC на банката на получателя BNBGBGSD	
При банка - име на банката на получателя БЪЛГАРСКА НАРОДНА БАНКА			Вид плащане***	
АВИЗО ЗА ИЗДАДЕН ПРЕВОДНО НАРЕЖДАНЕ / ВНОСНА БЕЛЕЖКА за плащане от/към бюджета			Вид валута BGN	Сума 3470.00
Основание за превод ГАРАНЦИЯ ЗА ДОБРО ИЗПЪЛНЕНИЕ				
Още пояснения ПО ДОГОВОР				
Вид* 9	номер на документа, по който се плаща		Дата (дд.мм.гггг) на документа	
Период, за който се плаща-от дата (дд.мм.гггг)		Период, за който се плаща-до дата (дд.мм.гггг)		
Задължено лице - наименование на юридическо лице или трите имена на физическо лице СЪРВИС ЦЕНТРИКС ООД				
Булстат на Задължено лице 200027636		ЕГН на задължено лице	ЛНЧ на задължено лице	
Наредител - наименование на юридическо лице или трите имена на физическо лице СЪРВИС ЦЕНТРИКС ООД				
IBAN на наредителя BG57STSA93000021890800			BIC на банката на наредителя STSBGSGF	
Платежна система BISERA	Такси** 2	Размер на такса 0.45 BGN	Дата Осчетоводяване 14.05.2018	Вид плащане***
Референция на наредителя 20180514029980033599			ДСК регистрация ОВ61405180016829	
<div> <div> *Вид документ: 1 - декларация 2 - ревизионен акт 3 - наказ. постановление 4 - авансова вноска </div> <div> 5 - парт. номер на имот 6 - постановление за принудително събиране 3 - други </div> <div> **Такси: 1 - за сметка на наредителя; 2 - споделена; 3 - за сметка на получателя </div> <div> ***Вид плащане: ползват се за сметки на администратори на приходи и на Централния бюджет </div> </div>				

Подпис и Печат ДСК: