



ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

ЗА

**„Разработване и внедряване на Система за управление на качеството и
информационната сигурност (СУКИС) и сертифицирането ѝ по ISO 9001:2008 и ISO
27001:2006“**

ПО

**Обособена позиция № 1: „Разработване и внедряване на Система за управление на качеството
и информационната сигурност (СУКИС) в МРРБ“**



I. ВЪВЕДЕНИЕ

1 Обща информация

Министерство на регионалното развитие и благоустройството (МРРБ) е бенефициент по проект „МРРБ – ефективна, модерна и прозрачна приходна администрация в услуга на гражданите и бизнеса”, (наричан по-долу „Проекта”), осъществяван с финансовата подкрепа на Оперативна програма „Административен капацитет” (ОПАК), съфинансирана от Европейския съюз чрез Европейския социален фонд” съгласно Договор № 10-31-7/25.02.2011г. сключен с Управляващия орган на ОПАК.

Чрез проекта ще се оптимизира вътрешноведомствената комуникация като се подобряват действащите информационни системи и се изграждат връзки между тях, подобрява се качеството на обслужване на гражданите и се повишава събираемостта на приходите чрез внедряване на удобни за потребителя електронни услуги и регистри.

Една от основните дейности от проекта е разработването и внедряването на системи за управление в съответствие с изискванията на наложили се международно признати ISO стандарти, включващи както система за управлението на качеството на предоставяните от Министерство на регионалното развитие административни услуги, така и системи за управление на информационната сигурност, значението на които е критично за дейността на администрацията.

Определени са 13 основни дейности по проекта, като с настоящата процедура са свързани дейности 7 и 9 , както следва:

Дейност 7: Внедряване на Система за Управление на Качеството и Информационната Сигурност по стандартите БДС ISO/IEC 9001:2008 и БДС ISO/IEC 27001:2006.



Дейност 9: Сертификация на Система за управление на качеството и информационната сигурност по стандартите БДС ISO/IEC 9001:2008 и БДС ISO/IEC 27001:2006.

Връзка между дейностите по проекта и предмета на настоящата процедура.

Съгласно българското законодателство и условията на Проекта, изпълнението на тези дейности се възлага чрез провеждането на открита процедура по реда на Закона за обществените поръчки (ЗОП).

Основните дейности са предмет на две обособени позиции от настоящата обществена поръчка с предмет: **„Разработване и внедряване на Система за управление на качеството и информационната сигурност (СУКИС) и сертифицирането ѝ по ISO 9001:2008 и ISO 27001:2006“**, както следва:

Обособена позиция № 1: „Разработване и внедряване на Система за управление на качеството и информационната сигурност (СУКИС) в МРРБ“, включваща:

Дейност 7 от проектното предложение: Внедряване на Система за Управление на Качеството и Информационната Сигурност по стандартите ISO 9001:2008 и ISO 27001:2005.

Обособена позиция № 2: „Сертифициране на Система за управление на качеството и информационната сигурност внедрена в МРРБ по стандартите БДС ISO/IEC 9001:2008 и БДС ISO/IEC 27001:2006“, включваща:

Дейност 9: Сертификация на Система за Управление на Качеството и Информационната Сигурност по стандартите БДС ISO/IEC 9001:2008 и БДС ISO/IEC 27001:2006.



2 Цел на проекта и очаквани резултати.

Обща цел на проекта е изграждане на модерна, ефективна и ориентирана към потребителите администрация на МРРБ и повишаване на събираемостта на приходи в бюджета на държавата чрез развитие на качествени електронни административни услуги за гражданите и бизнеса.

Специфичните цели са:

1) Оптимизация на вътрешноеведомствената комуникация чрез усъвършенстване на съществуващите информационни системи и изграждане на връзки между тях;

2) Подобряване на качеството на обслужване и повишаване на събираемостта на приходи чрез внедряване на удобни за потребителя електронни услуги и изграждането на публични регистри;

3) Подобряване на качеството на административните услуги чрез изграждане на устойчива система за управление на качеството и информационната сигурност във всички териториални звена на МРРБ. Системата за управление на качеството и информационната сигурност е предназначена, за да осигури избор на подходящи механизми за контрол, които да защитават информационните активи и да дават увереност в заинтересованите страни.

Експертна консултантска помощ обхващаща експертно съдействие на служителите в МРРБ и ще допринесе за повишаване сигурността на информационните активи в организацията чрез внедряване и сертификация на система за управление на качеството и информационната сигурност по стандартите БДС ISO/IEC 9001:2008 и БДС ISO/IEC 27001:2006.

Чрез повишаването на стандартите на услугите, предоставяни в публичния сектор, се цели достигане на степен на ефикасност и прозрачност на държавната администрация, която способства за повишаването на конкурентоспособността на българския бизнес и в средносрочен мащаб би довела до постигане на целите, заложи



в Лисабонската стратегия. Проектът е насочен към изграждането на иновативна, конкурентна и ориентирана към изпълнението администрация, която е в състояние да изпълнява заложените политически и икономически цели и приоритети на Европейския съюз.

В резултат на изпълнение на специфичните цели свързани с:

- защита на информацията и личните данни на гражданите;
- защита на вътрешната информация;
- увеличаване ефективността на работните процеси;

ще се увеличи ефективността на процесите в организацията, като ще се усъвършенстват съществуващите процедури във връзка с предоставянето на по-качествени административни услуги. Успешното внедряване на системата и сертифициране по съответния стандарт ще повиши доверието в гражданите.

II. МОТИВИ ЗА ИЗБОР НА СТАНДАРТИ БДС ISO/IEC 9001:2008, БДС ISO/IEC 27001:2006 ПО НАСТОЯЩАТА ПРОЦЕДУРА

1. Избор на стандарт БДС ISO/IEC 9001:2008

Използването на стандарти за системите за управление на качеството (т.е. БДС ISO/IEC 9001:2008) като фундамент за „системи за управление” е доказан успешен инструмент за осигуряване на ефективен процес на предоставяне на услуги, както и стимул и гаранция за непрекъснатото усъвършенстване на организациите в публичния сектор. Това се отнася за всички нива на управление – централно, областно и общинско. Въвеждането на система за управление на качеството в съответствие с изискванията на стандарта БДС ISO/IEC 9001:2008 е силен мотивиращ фактор за служителите и безспорно доказателство за ангажираност на ръководството в посока ефективна и прозрачна администрация. Фокусът тук е поставен върху управлението на качеството на предлаганите от организацията административни услуги. Дейностите по разработването и внедряването на системи за управление в съответствие с изискванията



на БДС ISO/IEC 9001:2008 са съвместими с прилагани други инструменти за усъвършенстване на управлението, в това число CAF, EFQM и BSC.

2. Избор на стандарт БДС ISO/IEC 27001:2006.

Стандартът БДС ISO/IEC 27001:2006 поставя изисквания към системите за управление на информационната сигурност и е приложим както за правителствения, така и за неправителствен сектор и за бизнеса. Системата за управление на информационната сигурност е подход за управление на чувствителната информация по начин, който съответства на нуждите на организацията и гарантира запазването на сигурността и целостта на информацията, с която всяка организация оперира. Прилагането на стандарта гарантира, че информационният риск се управлява ефективно от гледна точка на съхраняване, както на собствената информация, така и на информацията, предоставена от различни други източници. С оглед прилагането на разпоредбите на Закона за електронното управление и все по-широкото предоставяне на услуги на гражданите по електронен път внедряването на стандарти в сферата на информационната сигурност е ключово за ефективното и безпрепятственото функциониране на административните звена. Внедрената и функционираща Система за информационна сигурност гарантира осигуряването на непрекъсваемостта на административния процес в случаи на извънредни ситуации и кризи. Фокусът тук е поставен върху аспектите на управлението на информационната сигурност, като от организацията се изисква задължително висока степен на ангажираност в тази посока и необходимия организационен и технически капацитет и съответна инфраструктура.

III. ОПИСАНИЕ НА ПРОЕКТНИТЕ ДЕЙНОСТИ

1. В обхвата на проекта изпълнителят трябва да предостави консултантска помощ при изграждането и внедряването на интегрирана система за управление на качеството и информационната сигурност (СУКИС), отговаряща на изискванията на стандартите БДС ISO/IEC 9001:2008 и БДС ISO/IEC 27001:2006. Успешното внедряване на СУКИС следва да бъде предпоставка за сертифициране на системата по съответните международни стандарти.



Съгласно проектното предложение етапите са следните

Етап 1: Анализ на текущото състояние

- Получаване на първоначална информация за наличните управленски процеси и вече въведените в МРРБ вътрешни системи за управление по обхват и функции.
- Провеждане на одит за първоначално установяване на съответствието на процесите и системите, свързани с информационните активи, с изискванията на стандарта

Етап 2: Подготовка за внедряване на СУКИС

- Изготвяне на План за изграждане и внедряване на СУКИС;
- Определяне на структурата и обхвата на системата;
- Изготвяне на основната политика за управление на качеството и информационната сигурност;
- Разработване на декларация за приложимост, определяща конкретните изисквания за МРРБ от стандарта за информационна сигурност БДС ISO/IEC 27001:2006;
- Определяне на процесите в организацията, тяхната последователност и взаимодействие;
- Определяне на ролите и отговорностите, както и идентифициране на необходимите ресурси за въвеждане на СУКИС;

Етап 3: Внедряване и функциониране на СУКИС

- Разработване на Наръчник, процедури, инструкции, правила, планове, заповеди, списъци и др. документи, необходими за внедряването на Системата за управление на качеството и информационната сигурност.
- Избор на механизми за контрол на въздействието върху риска;



- Внедряване на механизмите за контрол, избрани за постигане на целите по контрола;
- Определяне на методика за измерване ефикасността на избраните единични или групи от механизми за контрол с цел получаване на сравними и възпроизводими резултати.
- Оценка на риска на информационните активи;
- Одобрението от ръководството за предложените остатъчни рискове;
- Разработване на план за третиране на риска, който идентифицира подходящите управленски действия, ресурси, отговорности и приоритети за управлението на рисковете, свързани със сигурността на информацията;
- Изготвяне и утвърждаване на заповед за внедряване на СУКИС от ръководството на МРРБ;

Етап 4 Контрол на внедрената система

- Провеждане на вътрешни одити за съответствие и покриване на изискванията на СУКИС по отношение на стандартите БДС ISO/IEC 9001:2008 и БДС ISO/IEC 27001:2006;
- Отстраняване на констатираните несъответствия и изпълнение на коригиращите и превантивните действия, отразени в докладите от вътрешните одити на СУКИС - при установена необходимост;
- Провеждане на Преглед от Ръководството по СУКИС за оценка на готовността за провеждане на сертификационен одит от независима сертифицираща страна (одит от трета страна).

Етап 5: Обучение на служители на МРРБ

- Обучение на 6 служители на МРРБ по изискванията на СУКИС.
- Обучение 4 служители на МРРБ за вътрешни одитори на СУКИС.

2. Конкретни дейности по компонентите на консултантската помощ, изискуеми при въвеждането на стандартите



2.1 Преглед на текущото състояние

Необходимо е да бъде направен анализ на съществуващото положение в МРРБ, включващ:

- анализ на текущото състояние на процесите и информационните връзки;
- анализ на вътрешните документи;
- анализ на организацията;
- анализ на извършваните дейности.

Анализите имат за цел да разкрият състоянието на организацията и необходимите предпоставки за внедряване на СУКИС.

2.2 Определяне на обхвата на СУКИС

В зависимост от идентифицираните дейности и процеси в организацията трябва да бъде определен обхвата и границите на системата за управление на информационната сигурност по отношение на характеристиките на дейността, организацията, нейното местоположение, активи и технологии. Обхватът трябва да бъде съобразен с наличните процеси в организацията както и с предлаганите продукти и услуги за гражданите.

2.3 Категоризиране на информационните активи

Изпълнителят трябва да идентифицира типовете информационни активи, които ще бъдат обект на системата за управление на информационната сигурност в организацията. Идентифицираните информационни активи следва да бъдат категоризирани като е необходимо да бъде предложена система за лесното им и удобно съхранение и управление.

2.4 Оценка на риска



Изпълнителят следва да предложи методология за оценка на риска на идентифицираните информационни активи, следвайки утвърдени добри практики в извършването на оценка на риска. Методологията трябва да определя критерии за приемане на рисковете като идентифицира приемливите нива на риск. Предложената методика трябва да гарантира, че преценяването дава сравними и възпроизводими резултати.

Изпълнителят трябва да асистира на възложителя при извършването на оценката на рисковете за организацията, а именно при:

- оценяване на вредата за дейностите на организацията вследствие на пробиви в сигурността, като се вземат предвид потенциалните последици от загубата на поверителност, цялостност и наличност на активите;
- оценяване на практическата вероятност да възникне пробив в сигурността от гледна точка на преобладаващите заплахи, уязвими места и въздействия, свързани с тези активи и прилаганите механизми за контрол;
- оценяване на нивата на рисковете.

2.5 Изготвяне на документи

Изпълнителят трябва да консултира и окаже съдействие на Възложителя при изготвянето на документите и записите, изграждащи системата за управление на качеството и информационната сигурност в съответствие с изискванията на стандартите БДС ISO/IEC 9001:2008 и БДС ISO/IEC 27001:2006. В дейностите се включват:

- консултиране при изграждане на общата политика по сигурността;
- консултиране при документирането на процесите;
- предложения за шаблони, бланки, регистри, записи по качеството;
- предложения за политики, правила, процедури и инструкции;
- оказване на съдействие при попълването на шаблоните и регистрите;



- оказване на съдействие при въвеждането на изискуеми записи по качеството с цел осигуряване на доказателства за съответствие с изискванията и ефикасното функциониране на СУКИС.

Наличните документи да бъдат преглеждани и привеждани в състояние, отговарящо на изискванията. При нужда, наличната документация да бъде обновявана.

2.6 Внедряване на СУКИС

Необходимо е да бъде изготвен подробен план-програма за внедряване на Системата за управление на качеството и информационната сигурност (СУКИС).

Изпълнителят трябва да съдейства при внедряването на процедурите и другите механизми за контрол с цел успешното постигане на планираните цели по съответния контрол. Изпълнителят трябва още да даде насоки за измерване на ефикасността на избраните единични или групи от механизми за контрол с цел получаване на сравними и възпроизводими резултати.

2.7 Анализ на готовността за сертифициране

След внедряването на системата да бъде извършен предварителен анализ за проверка на съответствието на системата с изискванията на стандартите ISO 9001 и ISO 27001 и готовността на системата за сертификация от акредитиран орган.

Резултатите от анализа трябва да спомогнат за точната оценка за зрелостта на внедрената система, като трябва да бъдат направени препоръки за корекции на тези части на системата, които не съответстват на изискванията.

IV. ОРГАНИЗАЦИЯ И МЕТОДОЛОГИЯ

Конкретната методология за изпълнение на дейностите по проекта е предмет на техническото предложение на участника. Предлагащата методология трябва да се базира на утвърдени стандарти и добри практики. Като минимум методологията трябва да включва подробно описание на:



- Общата организация на проекта – структура на управленския екип, начин на взаимодействие, механизми за контрол и отчетност;
- Времеви график на проекта и начин за отчитане и контрол;
- Документация – периодичност, съдържание;
- Методика за изпълнение на дейностите по изграждането на системата.

Навсякъде, където е споменат модел, източник, процес, търговска марка или др. следва да се счита „или еквивалентен“.

Участниците трябва да предложат комплексно решение, което в максимална степен да удовлетвори реализацията на параметрите на необходимата на Възложителя услуга. Това решение трябва да бъде съобразено с техническите спецификации, да включва най-новите постижения на съвременните технологии, представеното решение следва да бъде описано в техническото предложение и то трябва да гарантира наличността на услугата в изискваните параметри.

Срок за изпълнение – до 21.1.2013 г.