



## ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ ЗА ИЗВЪРШВАНЕ НА ДЕЙНОСТИ ПО СЕРТИФИКАЦИЯ

Референтен № 4747 BGR  
07 октомври, 2019, София

До: МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО НА РЕПУБЛИКА БЪЛГАРИЯ

На вниманието на г-н Данаил Кирилов

Министър на правосъдието

*Копие до: г-н Николай Зашев*

Уважаеми г-н КИРИЛОВ,

Във връзка с обявената покана за участие в предстояща обществена поръчка с предмет: „Сертифициране на система за управление на сигурността на информацията в Министерство на правосъдието в съответствие с изискванията на международният стандарт ISO/IEC 27001:2013“ с рег. номер 90-00-62 / 30.09.2019 г., представяме на вниманието Ви нашата оферта за **акредитирана** сертификация по стандарта **ISO/IEC 27001:2013**.

В съответствие с условията, посочени в техническата спецификация на публичната покана, дейностите по предмета на обществената поръчка ще бъдат извършени по следния начин:

### **I. ПРОВЕЖДАНЕ НА ПРОЦЕС ПО СЕРТИФИЦИРАНЕ ОТ НЕЗАВИСИМ АКРЕДИТИРАН ОРГАН НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА В МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО В СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА НА МЕЖДУНАРОДНИЯТ СТАНДАРТ ISO/IEC 27001:2013”**

Сертификационната услуга ще включва (но не само):

- Сертификационен одит – етап 1 – проверка дали документацията на системата за управление е изготвена в съответствие с изискванията на международния стандарт ISO/IEC 27001:2013.
- Сертификационен одит – етап 2 – проверка на място как е внедрена и функционира системата за управление на сигурността на информацията.
- Отстраняване на евентуално констатирани несъответствия и последващ одит (при необходимост).
- Изготвяне на финален доклад и решение за сертификация.
- Издаване и предоставяне на акредитиран сертификат под международната акредитация на Италия ACCREDIA (EA MLA), съгласно международния стандарт ISO/IEC 27001:2013.

Изпълнението на всички дейности в обхвата на предоставяната услуга ще бъдат синхронизирани с утвърден от МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО график за изпълнение и във взаимодействие с упълномощените от него лица.



При положителна оценка от проведен сертификационен одит, организацията се препоръчва за сертификация и се издава акредитиран сертификат в съответствие с изискванията на международният стандарт ISO/IEC 27001:2013.

## **II. ОПИСАНИЕ НА ТЕХНОЛОГИЧНАТА МЕТОДОЛОГИЯ НА УСЛУГАТА**

### **1. ОЦЕНКА НА СЪОТВЕТСТВИЕТО (ЕТАП 0) / Срок: 1 календарен ден**

Оценката на съответствието се извършва на базата на попълнен информационен въпросник на РИНА, в който се съдържат общи и технологични въпроси. На базата на предоставената информация се определя комплексния клас съгласно провизиите на стандарта ISO/IEC 27006 и предварителния обхват по стандарта ISO/IEC 27001:2013, и се определя обема работа и технологичните характеристики.

### **2. ДОКУМЕНТАЛЕН ПРЕГЛЕД (ЕТАП 1 – ISO/IEC 17021) / Срок: 1 календарен ден**

Одитът обхваща преглед на документацията на системата за управление и проверка на нейната адекватност спрямо изискванията на стандарта ISO/IEC 27001:2013. На този етап се проверяват документацията, инфраструктурата, резултатите от вътрешните одити, прегледа от ръководството, методиката за оценка на риска, доклада от оценката на риска, плановете за третиране, декларацията за приложимост и се прави общ преглед на инфраструктурата. Крайната цел на този етап е да се определи готовността на МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО за следващия етап. Дейността се извършва в централното управление на министерството в гр. София. След приключване на етапа се изготвя подробен доклад с направените забележки, препоръки и заключения, както и подробен план за следващия етап.

### **3. СЕРТИФИКАЦИОНЕН ОДИТ (ОСНОВЕН ОДИТ - ЕТАП 2 – ISO/IEC 17021) / Срок: 3 календарни дни**

Одитът обхваща преглед на същинската дейност на МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО спрямо описаните и оценени на първия етап процедури, инструкции, регламенти и действието на внедрените контролни механизми. По време на тази оценка се провеждат интервюта със служителите, проверяват се документи, записи и се извършват наблюдения на дейността. Целта е събирането на обективни доказателства, че дейността се извършва съгласно документираните правила на министерството. Дейността се извършва в централното управление и посочените от министерството локации на извадков принцип. След приключване на проверката се предоставя подробен доклад.

### **4. ОТСТРАНЯВАНЕ НА ЕВЕНТУАЛНО КОНСТАТИРАНИТЕ НЕСЪОТВЕТСТВИЯ / Срок: 1 календарен ден**

Евентуално констатираните несъответствия се отстраняват в оперативен порядък, като в случай на необходимост се извършва последващ одит.

### **5. АКРЕДИТИРАНА СЕРТИФИКАЦИЯ / Срок: 5 календарни дни**

След отстраняване на евентуалните несъответствия с изискванията на стандарта, МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО се препоръчва за сертификация и след решение на техническия комитет се издават двуезични сертификати с валидност 3 (три) години. Сертификатите на РИНА се издават под международната акредитация на Италия – ACCREDIA (пълноправен член на IAF и EA), както е показано по-долу. Сертификатите ще бъдат безусловно признати от всички институции в целия свят съгласно





споразумението за взаимно признаване EA MLA. Всички сертификати на РИНА имат уникален номер и холограма за автентичност. Информация за МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО ще бъде публикувана на Интернет страницата на РИНА и ACCREDIA и може да се използва сертификационния знак на РИНА и да се рекламира сертификацията на МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО в световен мащаб.

## 6. НАДЗОР

След получаване на сертификатите RINA ще извършва годишни надзорни проверки до изтичане на срока на валидност на сертификатите. Съгласно международните правила тези проверки ще обхващат различни процеси на системата за управление на Вашата организация, съгласно предварително изготвен принципен план. След всяка проверка предоставяме подробен доклад с направените препоръки, забележки и заключения.

## 7. СЕРТИФИКАЦИОНЕН ПОРТАЛ (MEMBER AREA)

РИНА разполага с автоматизирана и интерактивна Интернет система, която служи за комуникация с организациите. Всяка организация индивидуално получава име и парола за достъп до системата на Интернет адрес <http://portal.rina.org>, генерирани и изпратени до организацията директно от системата. Системата дава възможност за автоматизирано управление на несъответствията и препоръките, дава достъп до всички доклади от одити, които се актуализират в реално време, дава възможност да се видят програмите и плановете за одит и надзор, сертификатите на организацията, сертификационните знаци на РИНА и правилата за тяхното използване, както и актуална информация по отношение на правилата, стандартите и сертификацията като цяло.

## 8. КОНТРОЛ ПО ИЗПЪЛНЕНИЕТО / ОСИГУРЯВАНЕ НА КАЧЕСТВОТО

По време на изпълнението на услугите, компетентните органи на РИНА ще извършват дистанционен контрол в реално време предвид факта, че докладите от одита се изготвят по време на проверката в защитена Интернет среда. От друга страна системата за докладване на РИНА (ASCESI) извършва редица автоматични проверки и по този начин елиминира възможността от пропуски по време на проверката, технически и административни грешки и прави логическа проверка на записаните резултати. След всеки етап се извършва и независим преглед на доклада от независим и компетентен персонал, който в рамките на 24 часа ще предприеме необходимите мерки в случай на нужда.

## 9. ПЛАН ЗА ИЗВЪРШВАНЕ НА ДЕЙНОСТИТЕ

№	РОЛЯ	ДЕЙНОСТ
1	РЪКОВОДИТЕЛ НА ПРОЕКТА	Координиране на комуникацията с МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО. Проверка и контрол на качеството на докладите в реално време. Оказване на съдействие на МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО при изготвяне на детайлни графици. Съдействие при извършване на оценката на съответствието.
2	ВОДЕЩ ОДИТОР	Извършване на етап едно от одита. Изготвяне на план за одита. Извършване на одитни дейности при етап две от одита. Ръководене и координация на одитните дейности. Закриване на евентуални несъответствия.
3	ОДИТОР	Извършване на одитни дейности при етап две от одита. Оказване на съдействие на водещия одитор. Придържана към плана за одит.



		Изготвяне на детайлни записки за нуждите на одитния доклад.
4	ТЕХНИЧЕСКИ ЕКСПЕРТ (при необходимост)	Технологична експертиза в сферата на ИТ и информационната сигурност при необходимост. Съдействие при проверка на ИТ системи и конфигурации. Комуникационни и ИТ анализи в контекста на проекта.

### 10. УПРАВЛЕНИЕ НА РИСКА

Резултатът от направената оценка на риска за изпълнение на сертификационната услуга, вземайки предвид внедрените механизми за контрол и дублиране е, че нивото на риска е НИЩОЖНО. По-долу са изложени заплахите и методите за въздействие върху риска:

№	Заплаха	Съществуващи мерки	риск
1	Отказ на системите	Дублираща система за докладване	НИЩОЖЕН
2	Липса на одитори от екипа	Еквивалентни дублиращи екипи	НИЩОЖЕН
3	Конфликт на интереси	Етичен кодекс / Проверки	НИЩОЖЕН
4	Закъснения / Пропуски	Контрол в реално време	НИЩОЖЕН
5	Загуба на поверителност	Криптиране / Декларации / Проверки	НИЩОЖЕН
6	Влошено качество	Автоматични проверки / Мониторинг	НИЩОЖЕН

### 11. ДЕМОНСТРАЦИОННИ ЕКРАНИ ОТ СИСТЕМА ASCESI

The screenshot displays the ASCESI software interface. At the top, there are navigation links: Functions, Reports, Ascesi Manual, Surveyor Manual, My Profile, RINA PORTAL, HOME, LOG OUT, and INFO. The main window is titled 'Process List' and contains several sections:

- Search Criteria:** Client Code: 159603, Client Name: GENERAL LABOUR INSPECTORATE EXECUTIVE AGENCY, Site Code, Site Name, Rule (ISO/IEC 20000:12011, ISO/IEC 27001:2005, ISO/IEC 27001:2013, ISO/TS 16949:1999), EA (33 - Information technology, 34 - Engineering and technical, 35 - Firm professional services), Planned date (PVP) from to, Type (Certification, Supervision, Repeat assessment, Additional audit, Expansion), Status (Planned, In Process, Closed, Certified, Cancelled).
- Details:** A table with columns: Seq., Description, MD Done, Begin, End. It lists 9 steps of a process, including 'Transmission of STAGE 1 audit date and plan', 'Stage 1 audit', 'Audit Plan', 'Audit plan sending', 'Stage 2 audit', 'Surveillance audit programme', 'Technical committee approval', 'Communication of Certification / Validation', and 'Publication of certificate / validation and documents on the member area'.
- Table:** A table with columns: Rule, Client, Client name, Site, Site name, Client Office, Program Reviewer, Type, 1° after cert., Status. It shows two records for rule 9001:2008 and client 159603.
- Accreditation Sectors:** A list of sectors including AS (Aerospace sector), BFAS (Banking, finance, assurance sector), CPHS (Chemical and pharmaceutical sector), and CPS (Coke and petroleum sector).
- Process Technical Area:** A list of areas including GBS (Generic business Sector) and ITS (Information technology sector).

At the bottom, there are buttons for Open, Close, ReOpen, Delete, Send to Certify Process, Sort, Excel, Print, and Exit.



Certification Process Client:159603 Site:159603 Name:GLAVNA INSPEKTZIA PO TRUDA File N°:14 BG 78 MQ Contract: 2014/X8Q/-1

Contract: 2014/X8Q/-1

Company & Representatives Production Site Reference Document Audit Report Info Sheet Conclusions

Main Other sites

Scope (local) for this audit  
ОСЪЩЕСТВЯВАНЕ НА КОНТРОЛНА ДЕЙНОСТ И АДМИНИСТРАТИВНО ОБСЛУЖВАНЕ ОТНОСНО СПАЗВАНЕ НА ЗАКОНОДАТЕЛСТВОТО В ОБЛАСТТА НА ТРУДА, ЗАЕТОСТТА И ДЪРЖАВНАТА СЛУЖБА  
Address of head office  
3, KNYAZ ALEXANDER DONDUKOV FLOOR 1 SOFIA, BULGARIA

Scope (english) for this audit  
IMPLEMENTATION OF CONTROL ACTIVITIES AND ADMINISTRATIVE SERVICES ON THE COMPLIANCE WITH THE LEGISLATION IN THE FIELD OF LABOUR, EMPLOYMENT AND PUBLIC SERVICE

VITIES AND COMPLIANCE WITH LABOUR, EMPLOYMENT

Name and business name  
3, KNYAZ ALEXANDER DONDUKOV FLO

Company & Representatives Production Site Reference Document Audit Report Info Sheet Conclusions

Results of the audit for each process identified by the Organisation and assessed during the audit (evidence, strong points and positive elements)  
ДОКУМЕНТАЦИЯ  
След първоначалния одит е извършено изменение в документацията на ИА ГИТ, като са актуализирани Наръчника и Процедура за управление на документите, като същите са с нова вер. 3 от 06/03/14. Останалите процедури от СУК са с вер. 2

Improvement opportunities  
Документирани в Доклада.

Degree of effectiveness of the internal audits/management reviews  
ПРЕГЛЕД ОТ РЪКОВОДСТВОТО  
По време на одита беше проверен документирания преглед в Протокол от 24/01/2014. Бяха проверени и Обобщена информация от подадените анкетни карти в ИА ГИТ през 4-тото тримесечие на 2013г., както и сравнителен анализ по

Sign Cancel Save Save/Subject Print Refresh Exit

Paragraph	Status	Type	Description
4	Checked		Context of the organization
5	Checked		Leadership
6	To Be Corrected	C	Planning
7	Checked		Support
8	Checked		Operation
9	To Be Corrected	C	Performance evaluation
10	Checked		Improvement
A.5	Checked		Information security policies
A.6	Checked		Organization of information security
A.7	Checked		Human resource security
A.8	Checked		Asset management

### III. ОБОСНОВКА ЗА ИЗБОР НА ТЕХНОЛОГИЧНАТА МЕТОДОЛОГИЯ НА УСЛУГАТА

1. Възможност за постигане на системен и процесен подход за организиране на дейностите по сертифициране на система за управление на сигурността на информацията в МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО.
2. Прилагане на „планиране-извършване-проверка“ модел към решаване на проблемите.
3. Възможност за повишаване нивото на ангажиране, съпричастност и решаваща отговорност на ръководството на МИНИСТЕРСТВО НА ПРАВОСЪДИЕТО.
4. Възможност за дефиниране на политика за сигурност на информацията.
5. Организиране на сигурността на информацията.
6. Постигане на реална и обективна оценка на риска и управление на риска.
7. Предоставяне на възможност за внедряване на обосновани и ефективни механизми за контрол.
8. Измерване на ефективността и обективна оценка на всички процеси в системата за управление на сигурността на информацията.
9. Прецизно документиране на дейността и поддържане на записи.



10. Осигуряване на непрекъснатост на бизнес процесите.

11. Навременно изпълнение на поръчката в съответствие с изискванията на международния стандарт ISO/IEC 27001:2013, както и отчитане на спецификата на всеки от етапите, дейностите и поддейностите в тях, и възможните зависимости между тях.

#### IV. СРОК ЗА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

Срокът за изпълнение на поръчката е заложен в Техническата спецификация на обществената поръчка: до 6 месеца (шест месеца), считано от датата на сключване на договора. Гарантираме, че сме в състояние да изпълним качествено поръчката в пълно съответствие с гореописаната оферта.

#### V. ЦЕНИ

RINA е организация с идеална цел, работеща в полза на обществото. Сред основните приоритети на нашата компания е осигуряване на качество, безопасност и живот в социално справедлива среда, като финансовата печалба не е основен приоритет още от създаването на RINA през 1861. Поради тези причини RINA е в състояние да предложи изгодни цени за акредитирана сертификация, съобразени с пазара и икономическите условия във всяка страна.

ИКОНОМИЧЕСКО И ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ				
EA/RINA CODING: 36	СЕРТИФИКАЦИЯ 2019	ПЪРВИ НАДЗОР 2020	ВТОРИ НАДЗОР 2021	ОБЩО ЗА ТРИ ГОДИНИ
Цена	6,750.00 лв.	2,250.00 лв.	2,250.00 лв.	11,250.00 лв.
Словом	Шест хиляди седемстотин и петдесет лева	Две хиляди двеста и петдесет лева	Две хиляди двеста и петдесет лева	Единадесет хиляди двеста и петдесет лева

- Посочените цени включват всички разходи за акредитирана оценка и издаване на сертификатите.
- Безплатна употреба на сертификационния логотип на RINA.
- Сумите се фактурират след приключване на услугите и са платими в 90 дневен срок.
- Към посочените цени се начислява ДДС съгласно действащите ставки в момента на фактуриране.
- Разходи за транспорт и настаняване на одиторите НЕ се начисляват.

С уважение и желание за бъдещо сътрудничество,

Заличено съгл. чл. 36а, ал.3 от ЗОП

инж. Калин Панев  
Управител  
РИНА България

