МЕТОДИКА

за оценка на риска и одит на мрежовата и информационната сигурност, на общинско ниво

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

1.Настоящата методика е разработена в съответствие с предвиденото за изпълнение в рамките на дейност II. „Разработване на методика за оценка на риска и одит на общинско ниво, приложими съгласно Наредбата за минималните изисквания за мрежова и информационна сигурност“. по проект BG05SFOP001-2.025, с наименование „Повишаване на общото ниво на мрежова и информационна сигурност в общински администрации“.

Съгласно със съществуващи добри практики и по аналогия с други методики, тя съдържа: Глава първа - Общи положения; Глава втора – Одит на мрежова и информационна сигурност на общинско ниво; Глава трета – Оценка на риска; Глава четвърта – Заключение и Глава пета – Методологически напътствия за прилагане на Методиката.

2. Тази методика е предназначена да подпомогне общините при подготовката и провеждането на оценка на риска и одит на състоянието на мрежовата и информационната сигурност (МИС) в общините в съответствие с разпоредбите на Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМС).

Същността на този вид одит е, че при провеждането му състоянието на МИС в общините се сравнява основно с определено абстрактно описание, дадено в НМИМС.

На база на установеното състояние на МИС се извършва и оценка на риска за МИС в общината.

Вътрешният одит (одит от първа страна) се организира от всяка община и се извършва от нейни служители или от трета страна но от нейно име и следва да се извършва ежегодно, съгласно чл.35, ал.3, т1 от НМИМИС.. Одита се регулира от вътрешни документи в рамките на общината. Те определят начина, по който се обработват данните и се осъществяват процесите в нея.

3. За целите на настоящата методика се използват следните определения и съкращения:

а). Одит на МИС на общинско ниво (одитиране) – процес за оценка степента на съответствие на състоянието на МИС в общините с разпоредбите на НМИМИС, а така също и установяване на уязвимости и възможни заплахи за МИС. В този случай одитът се свежда основно до проверка на системата за МИС и сравняване на нейните резултати с НМИМИС

б). Информационни активи – Съгласно . определението, дадено в международния стандарт ISO / IEC 13335- 1:2004 "актив е нещо, което има стойност за организацията". Съвкупност от активи обикновено включва:информация - бази данни, системна документация, ръководства за потребителя, счетоводни материали, процедури за работа или поддръжка на обекта на одитиране, планове за осигуряване на непрекъснатостта на работата на информационната поддръжка и друга документация); софтуерни активи – приложен и системен софтуер, помощни програми; физически активи – ИТ оборудване;

услуги хората с тяхната квалификация, умения и опит; неосезаеми активи – например репутация на организацията.

в) Мрежова и информационна сигурност е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях"

г) Мрежа и информационна система" е:

- електронна съобщителна мрежа по смисъла на § 1, т. 15 от допълнителните разпоредби на Закона за електронните съобщения;

- всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които по програма обработва автоматично цифрови данни, или

- цифрови данни, съхранявани, обработвани, извличани или пренасяни от елементи, обхванати от букви "а" и "б", с цел обработванеоди, използване, защита и поддръжка

д) Оценка на риска за МИС - процес на определяне на стойности на вероятността и последствията от риск при установени несъответствия в рамките на одита.

е.) Уязвимост на МИС на общините - недостатък в МИС, който може да наруши обичайните дейности на общината, или да доведе до неоторизиран достъп до чувствителни информационни активи, заобикаляйки използваните инструменти за МИС.

ж.) Събиране на информация - набор от организационни и технически мерки, насочени към: изучаване, анализиране и оценяване на наличната в общините организационна, разпоредителна и техническа документация изискуема по НМИМИС;; провеждане на интервюта, с различни категории служители на общините за проучване на състнеоянието на организацията на работа за изпълнение на разпоредбите на Наредбата; извършване на проверки по извадков метод.

з.) съществено несъответствие - една или повече основни разпоредби на НМИМИС не са изпълнени или се прилагат неадекватни мерки за гарантиране на поверителност, цялостността или наличието на критична общинска информация, което води до неприемлив информационен риск; несъществено несъответствие - частично не са изпълнени някои разпоредби,на Наредбата, което увеличава информационните рискове за общините или намаляват ефективността на мерките за осигуряване на МИС; **зони за** подобрение – некачествено са из.пълнени някои от разпоредбите и/или не са приложени препоръчителните мерки от НМИМИС.

4. В тази Методика са използва следните нормативни правни актове

а) Закон за киберсигурност - Обн. ДВ. бр.94 от 13 Ноември 2018г., изм. ДВ. бр.69 от 4 Август 2020г., изм. и доп. ДВ. бр.85 от 2 Октомври 2020г., изм. и доп. ДВ. бр.15 от 22 Февруари 2022г., изм. ДВ. бр.25 от 29 Март 2022г.

б) Наредба за минималните изисквания за мрежова и информационна сигурност - приета с РМС№186 от 26.07.2019 г., обн. ДВ бр.59 от 26.07.2019 г.

в) ISO/IEC 27007 - Information technology - Security techniques - Guidelines for informationsecurity management systems auditing (Информационни технологии- Методи за сигурност-Указания за одит на системи за управление на сигурността на информацията – допълнение към насоките, съдържащи се в стандартISO19011) .

г) БДС EN ISO 19011 – Указания за извършване на одит на системи за управление

д)БДС EN ISO/IEC 17020 – Оценяване на съответствието - Изисквания за дейността на различни видове органи, извършващи контрол.

е) БДС EN ISO/IEC 27000 – Информационни технологии – Методи за сигурност – Системи за управление на сигурността на информацията – Общ преглед и речник.

ж) БДС ISO/IEC 27004 – Информационни технологии- Методи за сигурност-Управление на сигурността на информацията-Наблюдение,измерване,анализ и оценяване.

з) БДС ISO/IEC 27005 – Информационни технологии- Методи за сигурност-Управление на риска за сигурността на информацията.

е) ISO 31000:2011 Управление на риска. Принципи и указания

ж) ISO TR 31004:2013 Управление на риска. Указания за внедряване на ISO 31000

В някои случаи са използвани отделни приложими положения залегнали в стандарти посочени в Приложение 1, на НМИМИС.

Глава втора

ОДИТ НА МИС НА ОБЩИНСКО НИВО

Добра практика е одитираното за съответствие на състоянието на МИС в общините с разпоредбите на НМИМИС, да се провежда на следните етапи:

I. Подготвителен етап

По време на етапа се препоръчва изпълнението на следните дейности:

1.1 Изготвяне на инициращ доклад за провеждането на одита

Доклада се изготвя от служителя по МИС. В случай, че такъв не е назначен - от служител на общината определен от нейното ръководство.

1.2 Утвърждаване на Доклада, от кмета или от друго служебно лице съгласно установените правила в общината;

1.3 Отдаване на Заповед за провеждането на одита. Заповедта следва да съдържа но не само:

- Основание за извършване на одита;
- Задачи за изпълнение по време на одита;
- Отговорности, правомощия и отчетност на одитния екип;
- Време за провеждане на одита (начална и крайна дата);
- Изисквания към екипа за професионално поведение и етика;
- Изисквания и ред за осигуряване на условия за провеждане на одита;
- Представител на Ръководството за контрол, по време на одита.

Общата компетентност на одитния екип трябва да включва:

- адекватни знания и разбиране на управлението на риска за МИС, явяващи се достатъчни за оценка на използваните и проверими методи за осигуряване на МИС в общините;

- адекватни знания и разбиране на необходимостта от осигуряване на МИС и управление на МИС, явяващи се достатъчни за оценка на комплекса от мерки и средства за контрол и управление, а така също планиране, реализация поддържане на ефективността на МИС.

1.4 Екипът за извършване на одита (одитния екип), разработва Програма за извършване на одит(Одитна програма).

1.5 Програмата за извършване на одита включва, но не само;

- Кратко описание на работата. Тук следва да се посочи цялата необходима информация за реда на работа;

-- Въведение. Основание за провеждане на одита на ИС, вида на одита, характеристиките и изискванията към процедурата на одит, характеристиките на обекта на изследване, цели на одита, (Основните цели на одита на МИС са да потвърди, че: състоянието на МИС в общините е в съответствие с вътрешните и външните регулации и всички МИС рискове се управляват адекватно);

- Обхват на одита, (определя се от целта) - би бил по-ефективен ако е съобразен с оценка на риска;

- Конкретни задачи за всеки член от одитния екип и срок за тяхното изпълнение, одитни помещения;

- Одитни критерии. Например – информационните и комуникационни системи (ИКС) са в състояние да предоставят качествени продукти и услуги; - приложените мерки за МИС изискуеми от НМИМИС са ефективни и са в състояние да създадат условия за безпроблемно осъществяване на основните дейности в общината;

- Основните задачи, които трябва да бъдат решени, ограниченията, изпълняваните функции и критериите за оценка на нивото на МИС, за извършване на преглед на институцията, нормативните документи (ЗКС и НМИМИС) за чиито изисквания ще се провежда одита. Определят се качествени и количествени параметри за получаване на обективни оценки за нивото на МИС в общините;

- Ред за преглед на документацията, изискуема по НМИМИС, за събиране на информация и доказателства, за провеждане на интервюта с представители на ръководството на общината, на ИТ персонала и на останалия персонал за да се определи съответствието с одитните критерии и да се подкрепи изготвянето на одитния доклад;

– Ред за съхраняване, работа и класификация на информацията събрана по време на одита от одитния екип.

- Ред за съдействие от административния и ИТ персонал в общините;.

- Други, по усмотрение на общините.

1.6 Организиране и провеждане на встъпителна среща

Ръководителят на одитния екип следва да организира подготовка и провеждане на официална встъпителна среща, с участието на служителя по МИС, ИТ персонала и ръководството на общината. На участниците в срещата се предоставя информация отнасяща се до:

- Програмата за одит;

- Методите, които ще се използват в одитния процес;

- Процедурата за установяване на несъответствие с изискванията за МИС и необходимите за отстраняването им действия;

- Причините поради които въз основа на резултатите от одита могат да се правят забележки и възможни реакции към тях;

- Насоките, използвани от одиторите;

- Възможните трудности, които могат да възникнат в процеса на работа - отсъствие на водещи специалисти и др.;

- Организацията на работа с класифицираната по смисъла на чл.6 от НМИМИС информация.

II. Етап - Провеждане на одит

По време на етапа се препоръчва изпълнението на следните дейности:

2. Събиране на информация

По време на тази дейност, одиторите събират необходимата им информация и документират своята работа. Откритите слабости или отклонения се документират за да бъдат приложени в одитния доклад. Одиторът има за цел да документира пропуските, като приложи подходящи доказателства. Също така той трябва да категоризира установените несъответствия с НМИМИС, какви са рисковете за общините които произтичат от това както и приоритетът за тяхното отстраняване и да препоръча решение за елиминиране на проблема или минимизиране на риска, до ниво „приемлив“ .

Източници на доказателства могат да бъдат:

- Резултати от преглед на изискуемите по НМИМИС документи, извършен от одиторите;

- Резултати от интервютата със служителите – Ръководен състав, технически ИТ персонал и друг персонал, потребител на ИТ ресурси на общината;

- Информация от кореспонденция и/или друга документация;

- Резултати от преглед на проверими мерки (чл.2, ал.5, т.5 от НМИМИС). Проверимите мерки се определят по извадков метод (Sampling), като се извършва и оценка на риска.

Този етап се явява основополагащ за началото на одита. По времето на етапа се събира основната информация, която се отнася до дейността на общината, до нейните стратегически цели, до заповеди и други документи отнасящи се до МИС, така също и информация относно хардуерното и софтуерното осигуряване на ИКС, топология на мрежата. Важен момент се явява и наличието, актуалността и пълнотата на събраната информация, тъй като неспазването на всяко едно от тези изисквания е признак за недостатъци в общината, което следва да бъде отчетено от одиторите, тъй като всеки елемент на одита трябва да бъде напълно описан и документиран.

2.1. Предварително проучване на структурата на общината (извършва се при необходимост, т.е. ако се извършва от трета страна но от името на общината);

а) Извършва се, за да се определят характеристиките на функционирането на общината и да се получи обща информация за наличните хардуер и софтуер, друга релевантна инфраструктурата, технологиите и процедурите за МИС, използвани в общината.

б).Включва запознаване със следната документация, като минимум:

- Обща функционална и локална схема на общината (или други подобни документи);

- Списък на софтуера и хардуера, използвани в общината;

- Договори с доставчици на услуги имащи пряко и косвено отношение към ИКТ инфраструктурата. Например - Поддръжка на сайт или поддръжка на климатична техника).

2.2 Проучване, анализ и оценка за съответствие на наличната в общината изискуема документация по НМИМИС с нейните разпоредби.

Проучването, анализът и оценката на документацията се извършва с цел определяне на пълнотата, уместността и коректността на предвидените и приложени мерки в общината в съответствие с разпоредбите на НМИМИС.

2.3 На проучване, анализ и оценка за съответствие с разпоредбите на НМИМИС, подлежат следните документи: :

2.3.1.Политика за информационна сигурност (наричана по-долу Политиката)

: 2.3.1.1. Проучването, анализът и оценката на Политиката се извършват с цел определяне на пълнотата, уместността и коректността на основните разпоредби на Политиката и се състои в извършване на работа за определяне на наличие и качествена оценка за съответствие с изискванията на чл.4, от НМИМИС.

2.3.1.2. Въз основа на резултатите от проучването, анализа и оценката на Политиката в протокола за одитното проучване се вписва едно от следните решения:

- Политиката отговаря на разпоредбите на НМИМИС, ако е налична цялата информация, изискуема по чл.4 от Наредбата;

- Политиката не отговаря на разпоредбите на НМИМИС – при липса на част или цялата информация, посочени в чл.4 от НМИМИС, или ако Политиката не отговаря на тези изисквания и на общите изисквания по чл.5от НМИМИС.

2.3.2 Предвидените в чл.5 „Документирана информация“ от НМИМИС – опис на информационните активи; физическа схема на свързаност; логическа схема на информационните потоци; документация на структурната кабелна система; техническа,

експлоатационна и потребителска документация на ИКС и техните компоненти; вътрешни правила за служителите указващи правата и задълженията като потребители на услугите предоставяни чрез ИКС, като използване на персонални компютри, достъп до ресурсите на електронната поща, системи за документооборот и други вътрешно ведомствени системи, принтиране, факс, използване сменяеми носители на информация в електронен вид, използване на преносими записващи устройства; инструкции и правила за всяка дейност свързана с администрирането, експлоатацията и поддръжката на хардуер.

2.3.2.1 Проучването, анализът и оценката на Документираната информация се извършват с цел определяне на нейната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие с изискванията на чл.5, от НМИМИС (наричани по-нататък в Методиката „общи изисквания“).

2.3.2.2. Въз основа на резултатите от проучването, анализа и оценката на Документите по чл.5, ал.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Документите отговарят на разпоредбите на НМИМИС - ако са налични всички документи и те съответстват на изискванията предвидени в чл.5, ал,2, ал.3 и ал.4 от Наредбата;

- Документите не отговарят на разпоредбите на НМИМИС – ако липсват един или повече документи и/или документите не съответстват на изискванията предвидени в чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.3. Вътрешни правила за класификация на информацията

2.3.3.1. Проучването, анализът и оценката на Вътрешните правила за класификация на информацията се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.6, във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.3.2. Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила по чл.6, ал.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила отговарят на разпоредбите на НМИМИС - ако са налични самите правила и те съответстват на специфичните изисквания предвидени в чл. 6, ал,2, ал.3, ал.4, ал.5, ал.6 и ал.7 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила не отговарят на разпоредбите на НМИМИС – ако самите правила не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 6, ал,2, ал.3, ал.4, ал.5, ал.6 и ал.7 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.4. Управление на риска (изискуеми документи – анализ и оценка на риска за МИС, Методика за анализ и оценка на риска и плана за намаляване на неприемливите рискове)

2.3.4.1. Проучването, анализът и оценката на Документите по управление на риска се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие с изискванията на чл.6, във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.4.2. Въз основа на резултатите от проучването, анализа и оценката на документите по управление на риска по чл.7 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Документите по управление на риска отговарят на разпоредбите на НМИМИС - ако са налични самите документи и те съответстват на специфичните изисквания предвидени в чл. 7 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Документите по управление на риска не отговарят на разпоредбите на НМИМИС – ако самите правила не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 7 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.5 Вътрешни правила за процеса на управление жизнения цикъл на ИКС

23.5.1. Проучването, анализът и оценката на Вътрешните правила за управление жизнения цикъл на ИКС се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.8, във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.5.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила по чл.8, ал.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила отговарят на разпоредбите на НМИМИС - ако са налични самите правила и те съответстват на специфичните изисквания предвидени в чл. 8, ал,2 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила не отговарят на разпоредбите на НМИМИС – ако самите правила не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 8, ал,2 и на общите изисквания по чл.5, ал.2,
ал.3 и ал.4 от Наредбата.

2.3.6. Опис на информационните активи

2.3.6.1. . Проучването, анализът и оценката на Описа на информационните активи се извършва с цел определяне на неговата пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.8 и с общите изисквания по чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.6.2 Въз основа на резултатите от проучването, анализа и оценката на Описа на информационните активи по чл.8, ал.2 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Описа на информационните активи отговаря на разпоредбите на НМИМИС - ако е наличен самия опис и той съответства на специфичните изисквания предвидени в чл. 8, ал,2 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Описът на информационните активи не отговаря на разпоредбите на НМИМИС – ако самия опис не е наличен и/или не съответства на специфичните изисквания предвидени в чл. 9, ал,2 и на общите изисквания по чл.5, а2, ал.3 и ал.4 от Наредбата.

. 2.3.7.Вътрешни правила и инструкции относно човешките ресурси

2.3.7.1. Проучването, анализът и оценката на Вътрешните правила и инструкции относно човешките ресурси се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.9 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.7.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила по чл.9, ал.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила и инструкции отговарят на разпоредбите на НМИМИС - ако са налични самите правила и те съответстват на специфичните изисквания предвидени в чл. 9, ал,2, ал.3 и ал.4 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила не отговарят на разпоредбите на НМИМИС – ако самите правила не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 9, ал,2, ал.3 и ал.4 и на общите изисквания по чл.5, а2, ал.3 и ал.4 от Наредбата.

2.3.8. Договори със трети страни (тук може да се приложи извадков принцип за одит) и План за действие в случай на неспазване на уговорките, дейности и клаузи от третата страна (Плана).

2.3.8.1. Проучването, анализът и оценката на Договорите с трети страни и Плана се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.10 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.8.2 Въз основа на резултатите от проучването, анализа и оценката на договорите с трети страни по чл.9, ал.1 и на Плана по чл.9, ал.3 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Договорите и Плана отговарят на разпоредбите на НМИМИС - ако са налични текстове свързани с МИС, ако е наличен План и ако те съответстват на специфичните изисквания предвидени в чл. 10 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

- Договорите и Плана не отговарят на разпоредбите на НМИМИС – ако в Договорите няма текстове относно МИС, Плана не е наличен и/или не съответстват на специфичните изисквания предвидени в чл. 10 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.9. Вътрешни правила за изменение на важните за дейността на общината информационни активи

2.3.9.1. Проучването, анализът и оценката на Вътрешните правила за изменение на важните за дейността на общината информационни активи се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.11 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.9.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила по чл.11, ал.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила отговарят на разпоредбите на НМИМИС - ако са налични самите правила и те съответстват на специфичните изисквания предвидени в чл.11, ал,2, ал.3 и ал.4 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила не отговарят на разпоредбите на НМИМИС – ако самите правила не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 9, ал,2 и ал.3 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.10. План за връщане на системите в предишното им състояние

2.3.10.1. Проучването, анализът и оценката на Плана разза връщанене на системите в предишното им състояние се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.11 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.10.2 Въз основа на резултатите от проучването, анализа и оценката на Плана по чл.11, ал.4 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Планът отговаря на разпоредбите на НМИМИС - ако е наличен самия тплан и той осигурява връщането на системите безпроблемно, в предишното им състояние и съответства на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Планът не отговаря на разпоредбите на НМИМИС – ако самият план не е наличен и/или не съответства на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.11. Документи доказващи изпълнение на разпоредбата на чл.12 от НМИМС относно „Сигурност при разработване и внедряване на ИКС

2.3.11.1. Проучването, анализът и оценката на документите доказващи изпълнението на разпоредбата на чл.12 от НМИМИС, се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.11 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.11.2 Въз основа на резултатите от проучването, анализа и оценката на документите доказващи изпълнението на разпоредбата на чл.12 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Документите отговарят на разпоредбите на НМИМИС - ако са налични и обезпечават сигурността при разработване и внедряване на ИКС и съответстват на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Документите не отговарят на разпоредбите на НМИМИС – ако не са налични и/или не съответства на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.12. Политики и Вътрешни правила относно използването на лични технически срЕдства и преносими записващи устройства.

2.3.12.1. Проучването, анализът и оценката на Политиките и Вътрешните правила относно използването на лични технически средства и преносими записващи устройства се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.15 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.12.2 Въз основа на резултатите от проучването, анализа и оценката на Политиките и Вътрешните правила по чл.15, ал.1 и ал.3 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Политиките и Вътрешните правила отговарят на разпоредбите на НМИМИС - ако са налични самите политики и правила и те съответстват на специфичните изисквания предвидени в чл. 15 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Политиките и Вътрешните правила не отговарят на разпоредбите на НМИМИС – ако самите политики и правила не са налични и/или не съответстват на специфичните изискваия предвидени в чл. 15 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.13. Политики и Вътрешни правила относно криптография.

2.3.13.1 Проучването, анализът и оценката на Политиките и Вътрешните правила относно криптографията се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.16 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.13.2 Въз основа на резултатите от проучването, анализа и оценката на Политиките и Вътрешните правила по чл.16 ал.1, т.3 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Политиките и Вътрешните правила отговарят на разпоредбите на НМИМИС - ако са налични самите политики и правила и те съответстват на специфичните изисквания предвидени в чл. 16 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Политиките и Вътрешните правила не отговарят на разпоредбите на НМИМИС – ако самите политики и правила не са налични и/или не съответстват на специфичните изисквния предвидени в чл. 16 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.14. Списък на администраторските профили за ИКС и техните компоненти;

2.3.14.1.Проучването, анализът и оценката на Списъка на администраторските профили за ИКС и техните компоненти се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.17, ал.1, т.7във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.14.2 Въз основа на резултатите от проучването, анализа и оценката на Списъка по чл.17, ал.1, т.7 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Списъкът отговаря на разпоредбите на НМИМИС - ако е наличен самия списък той съответства на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Списъкът не отговаря на разпоредбите на НМИМИС – ако самият списък не е наличен и/или не съответстват на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.15. Документация относно всички операции, процеси и дейности извършени с администраторски права..

2.3.15.1. Проучването, анализът и оценката на Документация относно всички операции, процеси и дейности извършени с администраторски права се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.17 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.15.2 Въз основа на резултатите от проучването, анализа и оценката на Документацията по чл.17, от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Документацията отговаря на разпоредбите на НМИМИС - ако е налична самата документация и тя съответства на специфичните изисквания предвидени в чл. 17, ал.4 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

-Документацията отговаря на разпоредбите на НМИМИС – ако самата Документация не е налична и/или не съответстват на специфичните изисквания предвидени в чл. 17, ал.4 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.16. Вътрешни правила за управление на достъпите.

2.3.16.1 Проучването, анализът и оценката на Вътрешните правила за управление на достъпите се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.19, във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.16.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила по чл.19, т.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила отговарят на разпоредбите на НМИМИС - ако са налични самите политики и правила и те съответстват на специфичните изисквания предвидени в чл. 19 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила не отговарят на разпоредбите на НМИМИС – ако самите политики и правила не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 19 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.17. Вътрешни правила и инструкции относно защитата на софтуер и фърмуер (включително Библиотека с дистрибутиви на използвания софтуер и фърмуер)

2.3.17.1 Проучването, анализът и оценката на Вътрешни правила и инструкции относно защитата на софтуер и фърмуер се извършва с цел определяне на нейната пълнота, точност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието и, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.22 ал.3 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.17.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешни правила и инструкции относно защитата на софтуер и фърмуер по чл.22 ал.3 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешни правила и инструкции относно защитата на софтуер и фърмуер отговаря на разпоредбите на НМИМИС - ако е налична самите правила и инструкции и съответстват на специфичните изисквания предвидени в чл. 22, ал.3 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешни правила и инструкции относно защитата на софтуер и фърмуер не отговаря на разпоредбите на НМИМИС – ако самите вътрешни правила и инструкции не са налични и/или не съответстват на специфичните изисквния предвидени в чл. 22, ал.3 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.18.Вътрешни правила и инструкции относно защитата на софтуер и фърмуер

2.3.18.1 Проучването, анализът и оценката на Вътрешните правила и инструкции относно защитата на софтуер и фърмуер се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.22, ал.5 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.18.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила и/или инструкциите по чл.28 ал.5 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила и/или инструкциите отговарят на разпоредбите на НМИМИС - ако са налични самите правила и/или инструкции и те съответстват на специфичните изисквания предвидени в чл. 22, ал.5 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила и/или инструкциите не отговарят на разпоредбите на НМИМИС – ако самите правила и/или инструкции не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 22, ал5 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.19. Документи доказващи, че се използва одобрен софтуер в ИКС

2.3.19.1. Проучването, анализът и оценката на документит доказващи, че се използва одобрен софтуер в ИКС се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне нааличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.22, ал.2 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

3.19.2 Въз основа на резултатите от проучването, анализа и оценката на Документите доказващи, че се използва одобрен софтуер в ИКС по чл.22 ал.2 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Документите доказващи, че се използва одобрен софтуер в ИКС отговарят на разпоредбите на НМИМИС - ако са налични самите документи и те съответстват на специфичните изисквания предвидени в чл. 22 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Документите доказващи, че се използва одобрен софтуер в ИКС не отговарят на разпоредбите на НМИМИС – ако самите документи не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 28 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.20. Документи доказващи, че в общината се прави регулярна проверка на конфигурационните файлове, настройките на системите и устройствата за нерегламентирани изменения.

2.3.20.1.. Проучването, анализът и оценката на Документи доказващи, че в общината се прави регулярна проверка на конфигурационните файлове, настройките на системите и устройствата за нерегламентирани изменения в съответствие с Наредбата и се състои в извършване на работа за определяне нааличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.22, ал.8 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.20.2 Въз основа на резултатите от проучването, анализа и оценката на Документи доказващи, че в общината се прави регулярна проверка на конфигурационните файлове, настройките на системите и устройствата за нерегламентирани изменения по чл.22 ал.8 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Документите доказващи, че в общината се прави регулярна проверка на конфигурационните файлове, настройките на системите и устройствата за нерегламентирани изменения отговарят на разпоредбите на НМИМИС - ако са налични самите документи и те съответстват на специфичните изисквания предвидени в чл. 22 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Документите доказващи, че в общината се прави регулярна проверка на конфигурационните файлове, настройките на системите и устройствата за нерегламентирани изменения не отговарят на разпоредбите на НМИМИС – ако самите документи не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 22 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.21.Документи доказващи извършването на периодична оценка на ефективността на мерките за защита от зловреден софтуер.

2.3.21.1. Проучването, анализът и оценката на Документи доказващи извършването на периодична оценка на ефективността на мерките за защита от зловреден софтуер в съответствие с Наредбата се състои в извършване на работа за определяне нааличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.23, ал.4 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.21.2 Въз основа на резултатите от проучването, анализа и оценката на Документи доказващи извършването на периодична оценка на ефективността на мерките за защита от зловреден софтуер. по чл.23 ал. 4 на НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Документите доказващи извършването на периодична оценка на ефективността на мерките за защита от зловреден софтуер. отговарят на разпоредбите на НМИМИС - ако са налични самите документи и те съответстват на специфичните изисквания предвидени в чл. 22 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Документите доказващи извършването на периодична оценка на ефективността на мерките за защита от зловреден софтуер. не отговарят на разпоредбите на НМИМИС – ако самите документи не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 23 на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.22. Вътрешни правила и/или инструкции за наблюдение.

2.3.22.1. Проучването, анализът и оценката на Вътрешните правила и/или инструкции за наблюдение се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.28, ал.2 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.22.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила и/или инструкциите по чл.28 ал.2 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила и/или инструкциите отговарят на разпоредбите на НМИМИС - ако са налични самите правила и/или инструкции и те съответстват на специфичните изисквания предвидени в чл. 28 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила и/или инструкциите не отговарят на разпоредбите на НМИМИС – ако самите правила и/или инструкции не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 28 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.23. Документи доказващи, че информацията за системните записи се съхранява за период не по-малък от 12 месеца

2.3.23.1. Проучването, анализът и оценката на Документи доказващи, че информацията за системните записи се съхранява за период не по-малък от 12 месеца в съответствие с Наредбата се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.29, ал.3, б.а, т.5 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.23.2 Въз основа на резултатите от проучването, анализа и оценката на Документи доказващи, че информацията за системните записи се съхранява за период не по-малък от 12 месеца . по чл.29, ал.3, б.а, т.5 ал. 4 на НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Документи доказващи, че информацията за системните записи се съхранява за период не по-малък от 12 месеца, отговарят на разпоредбите на НМИМИС - ако са налични самите документи и те съответстват на специфичните изисквания предвидени в чл. 29 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Документи доказващи, че информацията за системните записи се съхранява за период не по-малък от 12 месеца. не отговарят на разпоредбите на НМИМИС – ако самите документи не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 29 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.24. Вътрешни правила за управление на инциденти с МИС.

2.3.24.1 Проучването, анализът и оценката на Вътрешните правила за управление на инциденти с МИС се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.30 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.24.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила по чл.30, ал.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила отговарят на разпоредбите на НМИМИС - ако са налични самите правила и те съответстват на специфичните изисквания предвидени в чл. 30, ал.2 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила не отговарят на разпоредбите на НМИМИС – ако самите и правила не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 30, ал.2 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.25. План за справяне с инциденти (Планът трябва да съдържа Приложение Стратегия за комуникация, съгласно чл.30, ал.4 от НМИМИС).

2.3.25.1.Проучването, анализът и оценката на Плана за справяне с инциденти се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.30, ал.3 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.25.2 Въз основа на резултатите от проучването, анализа и оценката на Плана чл.30, ал.3 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Планът отговаря на разпоредбите на НМИМИС - ако е наличен самия План и той съответства на специфичните изисквания предвидени в чл. 30, ал.3 и ал.4 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Планът не отговаря на разпоредбите на НМИМИС – ако самия не е наличен и/или не съответства на специфичните изисквания предвидени в чл.30, ал.3 и ал.4 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.3.26. Вътрешни правила и/или инструкции за устойчивост

2.3.26.1.Проучването, анализът и оценката на Вътрешните правила и/или инструкции за устойчивост се извършват с цел определяне на тяхната пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието им, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.32, ал.2, ал.3 и ал.4, във връзка с чл.5, ал.1, т.6 и т.7 от НМИМИС.

2.3.26.2 Въз основа на резултатите от проучването, анализа и оценката на Вътрешните правила и/или инструкциите по чл.32 ал.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Вътрешните правила и/или инструкциите отговарят на разпоредбите на НМИМИС - ако са налични самите правила и/или инструкции и те съответстват на специфичните изисквания предвидени в чл. 32 , ал.2, ал.3 и ал.4, и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Вътрешните правила и/или инструкциите не отговарят на разпоредбите на НМИМИС – ако самите правила и/или инструкции не са налични и/или не съответстват на специфичните изисквания предвидени в чл. 32 ал.2, ал.3 и ал.4 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата

2.3.27. План за непрекъсваемост

2.3.27.1. Проучването, анализът и оценката на Плана за непрекъсваемост се извършват с цел определяне на неговата пълнота, точност, императивност, коректност в съответствие с Наредбата и се състои в извършване на работа за определяне на наличието му, пълноценен анализ и качествена оценка за съответствие със специфичните изисквания на чл.34, ал.2 и ал.3 във връзка с чл.5, ал1, т.6 и т.7 от НМИМИС.

2.3.27.2 Въз основа на резултатите от проучването, анализа и оценката на Плана чл.34 ал.1 от НМИМИС в протокола за одитното проучване се вписва едно от следните решения:

- Планът отговаря на разпоредбите на НМИМИС - ако е наличен самия план и той съответства на специфичните изисквания предвидени в чл. 34 , ал.2, ал.3 и ал.4, и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата;

- Планът не отговаря на разпоредбите на НМИМИС – ако самия план не е наличен и/или не съответства4на специфичните изисквания предвидени в чл. 34 ал.2, ал.3 и ал.4 и на общите изисквания по чл.5, ал.2, ал.3 и ал.4 от Наредбата.

2.4.Други източници за събиране на информация:

2.4.1. Интервюта с:

- Ръководен състав на общината;

- Персонал отговорен за прилагане на процедурите за МИС и с персонал отговорен за процеса на експлоатация и поддържане на ИКС;

- Други служители, на общината.

2.4.1.1.1. Проучването, анализа и оценката на резултатите от проведените интервюта с ръководен състав на общината (кмет, главен секретар, представител на ръководството по въпросите на МИС) се извършват с цел установяване степента на изпълнение на изискуемите дейности по НМИМИС (например по чл.3) и на други планирани управленски действия за постигане на целите на МИС;др. регулярни дейности по въпросите на МИС (административна практика към служители на общината свързана с поощряване и/или наказания по повод на МИС; непланирани проверки и др.); Добрата практика е този тип интервю да се извършва от ръководителя на одиторския екип

2.4.1.1.2 Въз основа на резултатите от проучването, анализа и оценката на резултатите от проведените интервюта в протокола за одитното проучване се вписва едно от следните решения:

- Резултатите от проведените интервюта с ръководния състав на общината отговарят на разпоредбите на НМИМИС, ако ръководния състав е изпълнил вменените му с чл.3 от Нардбата отговорности, като наличност, цялостност, срочност, ефективност;

- Резултатите от проведените интервюта с ръководния състав на общината не отговарят на разпоредбите на НМИМИС – ако ръководния състав не е е изпълнил изцяло или частично (например над 30%) вменените му от Нардбата отговорности, като наличност, цялостност, срочност, ефективност.

2.4.1.2.1.Проучването, анализа и оценката на резултатите от проведените интервюта с персонал отговорен за прилагане на процедурите за МИС и с персонал отговорен за процеса на: експлоатация и поддържане на ИКС, и за въвеждане в експлоатация на нови ИКС в общината се извършват с цел установяване степента на изпълнение на изискуемите дейности по НМИМИС (например Раздел II Защита);

2.4.1.2.2. Въз основа на проучването, анализа и оценката на резултатите от проведените интервюта в протокола за одитното проучване се вписва едно от следните решения:

- Резултатите от проведените интервюта с персонал отговорен за прилагане на процедурите за МИС и с персонал отговорен за процеса на: експлоатация и поддържане на ИКС и въвеждане в експлоатация на нови ИКС в общината отговарят на разпоредбите на НМИМИС, ако персоналът е декларирал, че е изпълнява всички изисквания на Раздел III Защита от Наредбата;

- Резултатите от проведените интервюта с с персонал отговорен за прилагане на процедурите за МИС и с персонал отговорен за процеса на: експлоатация и поддържане на ИКС и въвеждане в експлоатация на нови ИКС не отговарят на разпоредбите на НМИМИС – ако персонала не е е изпълнил изцяло или частично (например над 30%) вмененията му с Нардбата отговорности, като наличност, цялостност, срочност, ефективност.

2.4.1.3.1. Проучването, анализа и оценката на резултатите от проведените интервюта с други служители, относно спазване на правилата за МИС, в общината включително използването на лични технически средства и записващи устройства; дейности по повишаване на осведомеността им по въпросите на МИС и др. се извършват с цел установяване степента на изпълнение на изискуемите дейности по НМИМИС (например чл.15);

2.4.1.3.2. Въз основа на резултатите от проучването, анализа и оценката на резултатите от проведените интервюта в протокола за одитното проучване се вписва едно от следните решения:

- Резултатите от проведените интервюта с други служители, относно спазване на правилата за МИС, в общината включително използването на лични технически средства и записващи устройства; дейности по повишаване на осведомеността им по въпросите на МИС и др. изцяло отговарят на разпоредбите на НМИМИС, ако другите служители са декларирали, че изпълняват всички релевантни изисквания на Наредбата;

- Резултатите от проведените интервюта с други служители, относно спазване на правилата за МИС, в общината включително използването на лични технически средства и записващи устройства; дейности по повишаване на осведомеността им по въпросите на МИС и др. не отговарят на разпоредбите на НМИМИС – ако другите служители са декларирали, че не изпълняват изцяло или частично (например над 30%) вмененията му с Наредбата релевантни изисквания.

2.4.2 Събиране на информация по извадков метод

2.4.2.1.Проучване, анализ и оценка на събраната информация чрез проверка по извадков метод се извършват с цел установяване степента на изпълнение на релевантните и иискуемите дейности по НМИМИС чрез преглед на няколко избирателно определени по извадков метод мерки (в зависимост от капацитета на одитния екип). Определените за преглед мерки следва да отговарят на общите изисквания по чл.2, ал.5, на релевантните специфични изисквания по съответния член от Раздел II „Защита“ на НМИМИС, както и на релевантните изисквания по Приложение 4 и Приложение 5 от Същата наредба.

2.4.2.2. Въз основа на проучването, анализа и оценката на резултатите от събраната информация чрез проверка по извадков метод в протокола за одитното проучване се вписва едно от следните решения:

- Резултатите от събраната, чрез извадков метод информация относно спазване на общите изисквания по чл.5, ал.2, на релевантните специфични изисквания по съответния член от Раздел II „Защита“ на НМИМИС, както и на релевантните изисквания по Приложение 4 и Приложение 5 от същата наредба отговарят на разпоредбите на НМИМИС, ако прегледа на мерките установи, че те са приложени съгласно всички релевантни изисквания на Наредбата;

- Резултатите от събраната, чрез извадков метод информация относно спазване на общите изисквания по чл.5, ал.2, на релевантните специфични изисквания по съответния член от Раздел II „Защита“ на НМИМИС, както и на релевантните изисквания по Приложение 4 и Приложение 5 от същата наредба не отговарят на разпоредбите на НМИМИС, ако прегледът на мерките установи, че те не са приложени изобщо или са приложени частично (например до 70%).

При извършване на анализа и оценките по т.2.3 и т.2.4 добра практика е анализа да съдържа –констатции, изводи и където е необходимо препоръки, като препоръките не следва да бъдат свързвани само с отрицателни констатации и изводи;

Глава трета

ОЦЕНКА НА РИСКА

3. Общи положения

Извършването на оценка на риска е съществена част от етап „Провеждане на одит“, но с оглед ключовото й място в процеса на одитиране е изведена в отделна глава.

Оценката на риска следва да се разглежда и като процес, обединяващ идентификацията, анализа и сравнителната оценка на риска.

В същото време следва да се има предвид и че оценката на риска е един основен елемент от процеса на управление на риска. От тази гледна точка при оценка на риска е препоръчително одитните екипи да имат предвид в ***приложимата степен*** 11-те принципа за управление на риска съдържащи се в ISO 31000:2011 Управление на риска. Принципи и указания и ISO TR 31004:2013 Управление на риска. Указания за внедряване на ISO 31000 – Приложение №2. Независимо от факта, че тези принципи не са 100% приложими за оценка на риска, екипът счита, че те биха били полезни в дейността както на ръководствата на общините , така и в дейностите та одитните екипи.

В процеса на одитиране следва внимателно да се прави разлика между оценка на риска от една страна и от друга страна анализ и оценка на изискуемата от НМИМИС документация (т.2.3.) и от тпридобитата от други източници на информация (т.2.4.).

Добра практика в процеса по оценка на риска е:

- Да се използва методологията на начините за увеличаване на привилегиите Например, наличието на установена уязвимост в ИКС (софтуе или хардуер)а не винаги води автоматично до пробив в сигурността, тъй като част от тези уязвимости могат да бъдат успешно визползвани само с определена комбинация от фактори. Теоретично е възможно използването на стандартни способности (именно способности, а не софтуерни или конфигурационни грешки) на ИКС в определена комбинация може да доведе до нарушаване на МИС. Идентифицирането на такива ситуации е невъзможно без използването на задълбочен и професионален подход към анализа на МИС;

- Одитният екип след преглед на събраните доказателства, следва да анализира и оценява дали прегледаните основните бизнес процеси в общината са обхванати от регулярен и многопластов контрол от гледна точка на МИС. В някои случай контрол в една област може да компенсира слабост в друга област;

- Да се извършва анализ и връзка между контролите;

- Одиторът трябва да използва своя опит и преценка, за да отсъди кои доказателства и на какво ниво да представи на Ръководството;

Препоръчително е резултата от анализа да се изчисляват с помощта на математически инструментариум (Виж пример за такъв инструментариум в глава пета „Методологически напътствия за прилагане на Методиката“).

3.2 Същност и особености при оценка на риска в процеса на одитиране

Оценката на риска се определя чрез определяне на вероятността за уязвяване въз основа на ефективността на съществуващи и/или планирани мерки за МИС

Целта на оценката на риска е да се определят характеристиките на рисковете за МИС. В резултат на оценката на риска става възможно да се изберат средствата за осигуряване на желаното ниво на МИС на общината.

В процеса на оценка на риска е необходимо да се има предвид и следната класификация на възможни типове риск за МИС в общините:

- Присъщ(допустим) риск - вероятността определени характеристики на ИКС по своята същност да водят до негативно въздействие върху изпълнението на функциите на одитираната община. Например присъщ риск за дадена информационна система, която има за цел да предоставя информация на обществото, е след достигане на определен таван от потребителски заявки, системата да блокира и да не предостави желаната информация на гражданите. В такъв случай общината може да въведе контроли за смекчаване на този

риск, но може и да прецени, че това по-скоро биха били изолирани случаи, които да ги приеме за допустими, като ги ограничи до някакво приемлива ниво определено на базата на съществуваща статистика.

- Контролиран риск – свежда се до вероятността въведените от общината ИТ контроли да не успеят да смекчат негативното въздействие, което целят да ограничат. Например в информационната която трябва да гарантира ограничен достъп до конфиденциална информация единствено за оторизираните лица, може да се въведе контрола под формата на изискване за представянето на потребителско име и парола за вход. Тук контролираният риск се състои в това потребителското име и парола да не са достатъчно сигурни и да могат да бъдат възпроизведени от неоторизрани служители (след използването на неоторизирани инструменти за генериране на пароли и потребителски имена), което би довело до разкриване на конфиденциална информация и потенциален негативен ефект. Ако общината изисква да бъдат използвани сигурни и комплексни пароли, съдържащи комбинация от различни азбуки, числа и специални символи и ИКСса настроени така, че да не допускат повече от „N“ на брой опити за въвеждане на парола за даден потребителски профил, тя би имала по-нисък контролен риск в сравнение с общините където не се прилагат подобни практики.

- Рискът от неразкирване представлява вероятността одиторът да не успее да установи отсъствието, неуспешното действие или неадекватността на ИТ контролите, въведени от общината, което би имало негативно въздействие за нея.

В процеса на извършване на одита следва да се има предвид и дали в одитираната община е отчетен факта за неразривната връзка на оценката на риска с анализа на риска. Процесът на анализ на риска, показва необходимостта от идентифициране на риска за определени информационни активи, на потенциалните заплахи и източници на заплаха, потенциалните уязвимости и потенциалните последици и въздействия, ако рисковете се материализират.

3.2.1. Подход за оценка на риска

На практика биха могли да се използват различни подходи и методи за оценка и управление на риска за МИС в общините.

Одиторът следва да одитира и избора на конкретен подход към оценката, като съществена част от одитния процес в една община. Подхода не следва да бъде ограничен от различни критерии, стига да е приемлив и стига да отговаря на общинските изисквания.

Одиторът трябва да провери дали избрания подход за оценка на риска е в съответствие с текущия/общ подход към оценка на рисковете за основните дейности в общината и с предприемането на подходящи мерки във връзка с установените рискове.

Дефиницията на подхода включва разглеждане на съответствието с изискванията на нормативните документи, както и други изисквания, важни във връзка с рисковете и активите, които общината трябва да управлява стратегически, в контекст на ежедневната си дейност и оценка на риска. По време на одита трябва да се потвърди, че подходът се прилага и изпълнява, както се изисква от НМИМИС.

Одиторът трябва да се увери, че подходът позволява всякакви служители. отговорни за оценката на риска могат да да стигнат до същите резултати независимо от това, кой и кога извършва оценка на риска, при условие че имат определено ниво на компетентност в областта на оценката на риска и провеждане на оценки на същите активи в съответствие с процесите и процедурите, определени в подхода. Ако се получи различен резултат, трябва да е възможно да се установи къде и кога е възникнала разликата в оценката на риска. Също така е необходимо една община да има подход, способен да доведе до еднакъв избор на контроли за третиране на риска, ако оценените рискове са

еднакви, т.е. със същото ниво на риск и характеристики (активи и изисквания за сигурност).

3.2.2. Стъпки които следва да се изпълняват при оценка на риска в процеса на извършване на одита:

3.2.2.1. Проверка дали са идентифицирани и определени значимите за общината информационни активи;

Одиторът следва да провери дали количествените показатели на информационните активи са оценени по резултатите от отговорите на собствениците на активи, т.е. от длъжностни лица които могат да определят ценността на информацията, нейните характеристики и степен на критичност, изхождайки от фактическото състояние на нещата.

Одиторът следва да провери и дали процеса на получаването на количествени показатели е допълнен, с подходящи методи за оценка на други критични активи на общините, като:

- Безопасност на персонала;
- Разкриване на лична информация;
- Спазване на законите и установените в общината разпоредби;
- Ограничения, произтичащи от законодателството;
- Финансови загуби и нарушения в ежедневната дейност;
- Връзки с обществеността;;
- Загуба на обществен имидж на общините.

Допълнителни количествени показатели следва да се използват там, където има допустими и обосновани критерии, а качествени - където количествените оценки са трудно реализуеми поради ред причини.

В повечето случаи значимите за общините информационни активи са подложени на риск и/или по отношение на тях съществуват едни или други заплахи. т.е., рисковете характеризират опасности, отнасящи се до ИКС и техните компоненти. При това рисковете за МИС зависят от:

- Показатели за стойността на информационните активи;
- Вероятност за реализиране на заплахи за ресурсите;
- Ефективност на съществуващите или планираните средства за МИС.

Важно е одитният екип да гарантира, че оценката на риска взема предвид всички критични активи, в рамките на обхвата на МИС и че оценката на заплахата/уязвимостта на активите е съобразена с организацията, а не само с използване на стандартни списъци със заплахи и уязвимости. Също така е важно, екипът да наблюдава рискове, които по своята същност са идентифицирани погрешно или омаловажавани, например, ако подходящите контроли са скъпи или трудни за прилагане, или ако рисковете са били разбрани погрешно.

Одиторът трябва да потвърди върху извадката, че всички значими активи, изброени в описа на информационните активи, са включени в оценката на риска.

Наличието на високо професионално подготвен и компетентен по въпросите на обезпечаването на МИС, персонал е от съществено значение за доброто функциониране на МИС.

Одиторът трябва да оцени, че доказателствата за средносрочните и дългосрочните рискове свързани със загубата на работоспособен персонал, са адекватно оценени от и преразгледани, като се вземат предвид последните корекции и че са въведени от общината.

Не на последно място при идентифицирането на риска е оценка на ефективността на съществуващите и/или планирани финансови средства за осигуряване на МИС.

Одиторът следва да прецени дали съществуващите и/или планирани финансови средства в общината са достатъчни за да се поддържат експлоатират и развиват информационните активи в състояние да осигурят високо ниво на МИС, да се осигури

повишаване на знанията и уменията на персонала отговорен за състоянието на МИС и за други дейности изискуеми от НМИМИС за които е необходимо финансиране (специфични за различните общини).

Одиторът трябва да оцени доказателствата за средносрочните и дългосрочните рискове свързани с провеждането на подходящ контрол и контрол на МИС за подобряване на устойчивостта на организацията срещу подобни загуби.

Одиторът трябва да прегледа възможностите за третиране на риска на организацията.Трябва да се провери дали за всички идентифицирани рискове е предвидено целесъобразно „третиране“ (т.е. намаляване на риска чрез прилагане на подходящи контроли насочени към предотвратяване на риска, прехвърляне на риск към трети страни или съзнателно поемане на рискове, ако са в рамките на „допустимите“ такива).

Одиторът трябва да търси несъответствия и други аномалии и да проверява. дали е имало скорошни промени (например нови ИТ системи или бизнес процеси) включени по подходящ начин в решенията за оценка на риска и лечение на риска.

3.2.2.2. Анализ на риска

Анализът на риска обичайно включва оценка на диапазона на възможни последствия от събития, ситуации или обстоятелства вследствие на осъществените и/или планирани дейности в общините за осигуряване на МИС и съответно тяхната вероятност за определяне на нивото на риска.

Одиторът следва да провери дали за всеки тип заплаха и свързаната с него група активи, нивата на вероятността заплахите да бъдат реализирани, а нивата на уязвимост като степента на лекота, с която реализираната заплаха може да доведе до отрицателно въздействие. При оценяването биха могли да се използват класификации базирани на установеното качество. (Виж Прил.№3 от НМИМИС например).

Одиторът следва да анализира дали възможността за реализиране на заплаха е оценена от нейната вероятност за реализиране в рамките на даден период от време спрямо някои от информационните активи на общината. А при оценка на вероятността, заплахата да бъде реализирана, дали са взети предвид следните ключови показатели:

- Място на информационния актив в ИКС и степен на неговата значимост – използва се при разглеждане възможни заплахи от злоумишлено човешко въздействие;
- Възможността да се използва информационния актив за генериране на доход - при разглеждане на заплахата от умишлено въздействие от човек;
- Технически възможности за реализиране на заплахи прилага се при умишлено въздействие от страна на човека;
- Степента на лекота, с която може да бъде използвана дадена уязвимост.

3.2.2.3. Сравнителна оценка на риска

Сравнителната оценка на риска се състои в сравняване на нивото на риска установено при извършването на одита с критериите за риск, установени в общината при определяне на обхвата на управлението на риска, за да се определи вида на риска и неговата значимост.

Одиторът следва да провери дали сравнителната оценка за риска използва информацията получена вследствие на неговия анализ.

Получените резултати от тази оценка следва да се използват при взимането на решения за предприемане на бъдещи действия по отношение управление на риска – необходимост и приоритети при обработка на риска; избор на способ за обработка на риска и др.. При взимането решенията от общините влияние оказват и финансови, юридически, етични и др. аспекти на ситуацията в тях.

Приетите решения и използваните за тази цел критерии следва да са съобразени с получените данни при идентификацията на опасностите и рисковете.

Критериите за приемане на риска често се влияят от политиките на общините за управление на риска, цели, технологии, средства, съответните закони и разпоредби и заинтересовани страни и в крайна сметка се определят от конкретно от всяка община. Следователно, одиторите е необходимо внимателно да проверят ефективността на критериите от гледна точка горните обекти, потвърждавайки също, че те са дефинирани и съществуват.

Одиторът трябва да оцени доказателствата за средносрочните и дългосрочните рискове свързани с провеждането на подходящ контрол и контрол на МИС за подобряване на устойчивостта на организацията срещу подобни загуби

Одиторът трябва да прегледа възможностите за третиране на риска на общината.Трябва да се провери дали за всички идентифицирани рискове е определено подходящо „третиране“ (т.е. намаляване на риска чрез прилагане на подходящи контроли и контроли, предотвратяване на риска, прехвърляне на риск към трети страни или съзнателно поемане на рискове, ако попаднат под апетита за управленски риск).

Одиторът трябва да търси несъответствия и други аномалии и да проверява. дали е имало скорошни промени (например нови ИТ системи или бизнес процеси) включени по подходящ начин в решенията за оценка на риска и лечение на риска.

Глава четвърта
ЗАКЛЮЧЕНИЕ

4.1 Одитен доклад

Официалният одитан доклад най-общо обичайно съдържа резюме на направените констатации, изводи и препоръки.

Водещият одитор (Ръководител на одитния екип) в процеса на изготвяне на доклада, трябва да установи – дали съдържащите се в доклада факти са с висока степен на достоверност; внимателно да прецени дали съдржащите се препоръки в него са подходящи и икономически възможни са прилагане; да анализира и предложи разумни срокове и дати за внедряване. Добра практика е водещият одитор .да проведе консултативен разговор с представителя на ръководството преди официалното представяне на одитния доклад. Целта е да бъдат изчистени евентулни неточности, непълно и неправилно оценени процеси и документи или съгласуване на датите за внедряване.. Представянето може да включва резюме за ръководството и презентация с направените констатации.

На срещата с представителя на ръководството се посочват установените както слаби така и силните страни относно състоянието на МИС в общините. Представят се критериите за категоризиране на откритията на несъответствия и зони за подобрения. Целта на срещата е да се съгласуват откритите несъответствия и ако е необходимо да се определят срокове за внедряване на коригиращи действия;

Официалният одитен доклад, изготвен в резултат на този вид одит, би могъл да съдържа следната структурирана информация:

- Степента на съответствие на състоянието на МИС в общината с разпоредбите на НМИМИС и на Закона за киберсигурност;
- Степен на съответствие със собствените вътрешни изисквания за МИС на общината;
- Брой и категории несъответствия и получени коментари;
- Препоръки за прилагане или модифициране на приложените мерки за МИС с цел привеждане състоянието на МИС в съответствие с разпоредбите на НМИМИС;
- Подробна препратка към основните документи на общината, включително политиката за сигурност, описания на процедурите за повишаване нивото на МИС,

допълнителни минимални и препоръчителни мерки за МИС приложими за съответната община.

Добра практика е Одитния доклад да бъде класифициран по смисъла на чл.6 от НМИМИС и Приложение 2 към него.

4.2. Заключителна среща

Приключването на одита е съпроводено от заключителна среща която се председателства от водещия одитор. На тази среща се представят резултатите от одита. Когато се представят резултатите, одиторът трябва точно, ясно и безпристрастно да ги обясни (а при необходимост) и да ги обсъди с одитираните. Представят се направените констатации, изводи и направете препоръки. Препоръките се правят на база на заключенията от извършения одит. На тази среща се съставя „Протокол от извършен одит", който се подписва от одиторския екип и от делегирани представители на одитираната община. Заключенията отразяват съответствието на състоянието на МИС в общината с разпоредбите на НМИМИС и на Закона за киберсигурност. Добра практика е също така при отразяването да намерят място и степента на ефективността на изпълнение и дали планираните цели, са подходящи за постигане на заложените цели. Те трябва да се основават на обективни доказателства. За всяко констатирано несъответствие и дадена от одитния екип препоръка, трябва да се предприемат коригиращи действия от одитираната община . Решенията за вида на тези действия се взимат от ръководството на одитираната община, а самите действия се извършват от определените от него отговорни служители.

Заключенията от одита показват необходимостта от коригиращи, превантивни или подобряващи действия, когато това е приложимо. Такива действия се предприемат от одитираната община, в рамките на определите от нея срокове за изпълнение на препоръките и се считат за част от одита.

Добра практика е също така управлението на внедряване на препоръките от одита да се осъществява на няколко етапа(например):

- Оценка на препоръките;
- Внедряване на ефективни и икономични финансово целесъобразни решения;
- Определяне на срокове и дати за изпълнение;
- Определяне на отговорници;
- Извършване на последващи действия за оценка на внедрените решения;
- Веднъж годишно да се извършва проследяване за изпълнението на дадените препоръки. За резултатите от извършените коригиращи действия по дадените препоръки да се изготвя доклад.

Документацията в едно одитно досие следва да съдържа, но не само:

- План (Програма) за провеждане на одита и неговия обхват;
- Описание на одитираната община и цели на одита;
- Извършен одит, дейности и събрани доказателства;
- Евентуално използване на услуги на други одитори / експерти;
- Одит - констатации, изводи и препоръки;
- Одитна документация за отстраняване на несъответствията с дефинирани дати и отговорници за отстраняването им.

Накрая следва да се има категорично предвид, че за успешното и ефективно провеждане на одита е необходимо активно участие ***<u>на ръководството на общините в процеса;</u>*** обективност и независимост на одиторите, тяхната компетентност и висок професионализъм; ясно структурирана процедура за проверки и активна реализация на препоръчаните мерки за отстраняване на констатираните несъответствия.

Глава пета

МЕТОДИЧЕСКИ НАПЪТСТВИЯ ЗА ПРИЛАГАНЕ НА МЕТОДИКАТА

5.1. Настоящата методика е примерна и е възможна за използване от общините за извършване на одит и оценка на риска по смисъла на чл.33, ал.1, т.1 от НМИМИС.

5.2. Методиката е насочена към изследване на степента на съответствие на МИС в общината с изискуемите от НМИМИС, минимални мерки.

5.4. За упоменатите в т.2.3.11, 2.3.15. 2.3.19, 2.3.20, 2.3.21 и 2.3.23 „Документи“ или „Документация“ следва да се приемат – заповеди, инструкции, одобрени от ръководител и списъци и други подобни.

5.5. В зависимост от броя на различните получени отговори, резултат в % може да се определя по формула:

$$(B/A) \times 100 = P\%$$

където: **P**- Резултат в проценти, **B** - брой на записите в т.2.3 и т.2.4, че съответния документ „отговаря изцяло на изискванията на НМИМИС“, **A** – сумата от броя на записите в т.2.3 и т.2.4, че съответния документ „отговаря на изискванията на НМИМИС“ и броя на записите „не отговаря на изискванията на НМИМИС“.

5.6. В съответствие със специфичните особености на отделните общини и в случай на необходимост в някои от дейностите по Раздел трети „Оценка на риска“, **може да**се използват клаузи от Приложение №3 на НМИМИС.

5.7. При използване на Приложението към настоящата Методика - Чек лист за резултатите от одита по т.2. и по т.2.4. , следва да се има предвид следното:

- Чек листа е подготвен на базата на разработения въпросник във връзка с изпълнение на дейност I „Мониторинг на ефективното прилагане на НМИМИС от малки, средни и големи общини“ по проект BG05SFOP001-2.025, „Повишаване общото ниво на мрежовата и информационната сигурност в общинската администрация“;

- В Чек листа, са включени въпроси относно всички разпоредби на НМИМИС релевантни на спецификите в общините;

- Въпросите свързани с разпоредби на НМИМИС по отношение на изискуеми документи (т.2.3 от Методиката) са включени в Част I на Чек листа;

- Въпросите включени в Част II на Чек листа, могат да се използват за събирането на информация по отношение на проведените интервюта и по отношение на резултатите от проверката на приложимите мерки по „извадков метод“ по т.2.4 от Методиката – Събиране на информация чрез интервюта и проверка по „извадков метод“, с оглед спецификите на всяка община;

При попълване на Чек листа е необходимо, да се използват единствено посочените по-долу възможни отговори, както следва:

- „да“, когато одитирания документ, резултатите от интервютата и проверката по т. 2.4, отговарят на изискването/изискванията на Наредбата;

- „не“, когато одитирания документ, резултатите от интервютата и проверката по т. 2.4, не отговарят на изискването/изискванията на Наредбета;

- „неприложимо“ (n/a), когато изискването/изискванията на НМИМИС по зададения въпрос не са релевантни за съответната община.

Въпроси на които не е отговорено и/или е отговорено с други думи освен горепосочените следва да се считат като отговори „не“.

В колона № 1 на Чек листа са показани две числа, разделени с наклонена черта. Първото число показва „№ по ред“на съответния въпрос, а второто число показва по кой член или по кое Приложение от НМИМИС е формулиран въпроса.

5.8. В рамките на II етап „Провеждане на одит, т.2. „ Събиране на информация“ при проучване, анализ и оценка за съответствие с изискванията за МИС и в случай на необходимаст за събиране на допълнителна и по пълна информация одитния екип би могъл да използва и следните уточняващи въпроси: :

Към т.2.3.1. Политика за информационна сигурност

- дали основните цели и принципи на Политиката са насочени към разкриване на значението на информационната сигурност като инструмент, който осигурява възможността за споделяне на информация;
- описани ли са управленските действия за постигане на целите на ИС;
- съдържа ли политиката за сигурност, принципите, правилата и изискванията, които са най-значими за общината;
- предвидени ли са мерки и действия при нарушаване на Политиката;
- съдържа ли Политиката общи дефиниции и функции на служителите в рамките на управлението на МИС;
- ими ли вписани изисквания за периодично преразглеждане на Политиката;
- съдържат ли функциите на ръководството по текстове по поддържане на въпросите за осигуряване на МИС

Към т.2.3.4.Управление на на риска

- избрана ли е подходяща методология за извършване на идентификация на риска и за оценка на риска;
- има ли описания на методите за определяне на стойността и критичността на информацията;
- има ли описание на процедурата за наблюдение, преглед и промяна на рисковете за МИС;
- има ли описание на методите и последователността за определяне на рисковете за информационната сигурност на обекта на атестиране;
- има ли описание на метода и последователността на оценка на идентифицираните рискове;
- има ли описание на метода за третиране на риска;
- има ли описания на метода и анализа на заплахите за МИС и източниците за тях;
- има ли описание на метода за определяне на вероятността от инцидент;
- има ли описание на процедурата за третиране на риска, като се вземат предвид коригирането, запазването, избягването, отделянето;
- има ли описание на изискванията за честотата на преглед и преоценка на рисковете;
- определяне и оценка на последствията при реализиране на риск;
- идентифициране на лица, отговорни за поддръжката и обработката на рисковете;
- описание на процедурата за съставяне на карта на риска;
- описание на процедурата за съставяне на план за третиране на риска въз основа на резултатите от оценката и анализа на риска

Към т.2.3.6. Опис на информационните активи

- при идентифициране на информационните активи взети ли са предвид тяхната стойност и важност;
- дали процедурата за идентифициране и класифициране на информационни активи, съответства на изисквания, отразени ли са тяхната поверителност, както и стойност и критичност;

- създаден ли е ред за съставяне и поддържане на регистъра на активите (с посочване на класа на актива, вида на актива, значението и собственика на актива);

- има ли процедура за етикетиране на активи в зависимост от техния установен клас, поверителност, стойност и критичност; .

- посочени ли са изисквания към формата на регистъра на активите, пълна ли е информацията.

- съществува ли процедура за издаване на паспорти (формуляр) на информационните активи ;

- има ли изисквания за честотата на инвентаризация на информационните активии;

- има ли изисквания за спиране от употреба на компютърен хардуер, телекомуникационно оборудване и софтуер, включително изхвърляне на устройства за съхранение на данни и гарантирано унищожаване на информация при повторна употреба на оборудването;

- има ли изисквания за назначаване на сужители на общината, отговорни за инвентаризацията и сертифицирането на ППО;

Към т.2.3.15. Документация относно всички операции, процеси и дейности извършени с администраторски права.

- съществуват ли изисквания към действията на администратора за основната стандартна работа;

- има ли изисквания към действията на администратора при инциденти, извънредни ситуации, природни климатични и техногенни въздействия;

- предвидена ли е за процедурата за инсталиране, актуализиране и премахване на софтуер на сървъри и работни станции;

- предвиденаи ли са процедури за управление на промените и анализ на софтуера в случай на промяна в системния софтуер.

Към т.2.3.24. и т.2.3.25. Вътрешни правила за управление на инциденти с МИС и План за справяне с инциденти

-има ли изисквания за съставяне на списък с възможни извънредни или кризисни ситуации, идентифициране на инциденти по МИС

- предвидено ли е своевременно уведомяване за нарушения на МИС, за да се осигури бърз, ефикасен и последователен отговор на инциденти, свързани с МИС;

- има ли възлагане на отговорност на длъжностни лица от общината за управление на инциденти в МИС ;

- планирани ли са мониторинг и регистриране на инциденти по МИС, процедури за докладване на инциденти по МИС;

- предвидено ли е събиране, съхранение и предоставяне на информация за инциденти с МИС, в случай че инцидентът може да доведе до съдебно производство - за разкриването и разследването на тежки престъпления и престъпления по чл. 319а – 319е от Наказателния кодекс в съответствие с чл. 14, ал. 4, т. 2 и чл. 15, ал. 3, т. 3 от Закона за киберсигурност; достъпът до тази информация трябва да е само за четене;

- предвидено ли е регистриране на събития, свързани със състоянието на МИС и откриване на нарушения чрез анализ на дневници на събития свързани с непрекъснатост на бизнеса

- има ли разработени процедури за възстановяване на обичайната дейност на общината след инцидент с МИС.

- има ли изисквания за наблюдение на изпълнението на превантивни действия за предотвратяване възникването на в МИСизвънредни или кризисни ситуации;

- има ли изисквания за разследване и анализ на регистриране инциденти в МИС на общината.

Към т.2.3.26. Вътрешни правила и/или инструкция за устойчивост

- определен ли е размера на резервното копие;
- има ли описания на изискванията за разполагане на резервно оборудване;
- има ли описания на изискванията за тестване на резервно оборудване;
- има ли описание на изискванията за разполагане на резервно сървърно оборудване и неговата физическа защита;
- има ли описания на процедурите за възстановяване на информация;
- има ли изисквания за документиране на процеса на архивиране по отношение на поддържането на регистър на главните копия, регистър на информационните ресурси, които трябва да бъдат архивирани, регистър на резервни записи, регистър на проверките за възстановяване на резервни копия, регистър на електронни архивни носители, регистър на въвеждане/премахване на електронен носител на резервна информация.

Към т.2.3.27. План за непрекъсваемост

- идентифицирани ли са събитията, които причиняват прекъсване на процесите на функциониране на обшината (планирането трябва да бъде придружено от оценка на риска);
- определяни ли са процесите за осигуряване на непрекъснатост на работата на активите, установени в регистъра на активите в случай на тяхната неизправност;
- разработен ли е план за осигуряване на непрекъснатост на работата на активите, свързани със средствата за обработка на информация и тяхното актуализиране;
- съществува ли процедура за тестване и актуализиране на планове за развитие на съществуващи процеси за непрекъснатост на експлоатацията на активите;
- назначени ли са отговорни лица за процесите на функциониране на общината;
- предвидени ли са начини за разполагане на оборудване, което да намалява риска от заплахи, опасности и възможности за нерегламентиран достъп;
- Предвидени ли са начини за защита на оборудването от повреди в системата за захранване и други смущения, причинени от смущения в работата на комуналните услуги;
- Има ли разписани изисквания за честотата на поддръжка на оборудването, за да се осигури непрекъснатост на работата, наличност и цялост.

Забележка: *Да се прави разлика между Управление на риска по чл. 7 и Приложение 3 от НМИМИС(извършва се комплексно за всички възможни обстоятелства които биха повлияли върху състоянието на МИС и преди разработване.то и/или актуализирането на документите изискуеми от НМИМИС) от една страна и Оенка на риска в рамките на Вътрешния одит от друга страна(оценката се извършва само за установените по време на одита несъответствия. Оценката се извършва от одитния екип).*

Приложение:

1.Чек лист за одита по т.2.3 и по т.2.4. - 3л.
2.Принципи за управление на риска – 2 л.

Приложение №1

ЧЕК ЛИСТ

за резултатите от провеждането на одит на МИС на общинско ниво .

№ по ред/чл. от НМИМИС	**Въпроси**	да	не	n/a
	ЧАСТ I Въпроси, релевантни на т.2.3 от Методиката			
1/4	Има ли община XXXX разработена и приета Политика за мрежова и информационна сигурност (МИС).?			
2/3	Извършван ли е преглед на Политиката за МИС в период от една година назад от датата на текущото оценяване ?			
3/3	Има ли определени служител или административно звено от общината, отговарящ/о за МИС с конкретна заповед?			
4/5	Има ли опис на информационните активи?			
5/5	Има ли Схема за физическата свързаност?			
6/5	Има ли логическата схема на информационните потоци?			
7/5	Има ли актуална документация на структурната кабелна система?			
8/5	Разполага ли община XXXXX с необходимата техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и компонентите им?			
9/5	Има ли инструкции и/вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер?			
10/5	Разработени ли са вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешни за общината системи, принтиране, факс, използване			

	на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.?			
11/5	Документацията идентифицирана ли е еднозначно (заглавие, версия, дата, автор, номер)?			
12/5	Документацията поддържали се в актуално състояние, чрез преразглеждане и обновяване при необходимост поне веднъж годишно?			
13/5	Документацията одобрена/утвърдена ли е от Административния Орган/Ръководителя?			
14/5	Документацията класифицирана ли е по смисъла на чл. 6 от НМИМИС?			
15/5	Регламентиран ли е достъпа до Документацията само до лицата, чиито задължения налагат това?			
16/5	Поддържа ли се в актуално състояние информация , доказваща по неоспорим начин изпълнението на НМИМИС?			
17/6	Има ли приети вътрешни правила за класификация на информацията, които регламентират как да се маркира, използва, обработва, обменя, съхранява и унищожава информацията с която разполага общината?			
18/6	Приложена ли е класификацията върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването на информацията?			
19/6	Различават ли се използваните от общината Нива на нкласификация спрямо тези предвидени в Закона за защита на класифицираната информация ?			
20/6	При обмена на информация използва ли се класификация TLP (traffic light protocol) съгласно приложение № 2 от Наредбата?			
21/7	Извършват ли се анализа и оценката на риска по одобрена/утвърдена от общината Методика?			
22/7	Има ли извършен анализ и оценка на риска за период от една година назад от датата на текущото оценяване ?			
23/7	Има ли план, който да включва подходящи и пропорционални мерки за смекчаване на неприемливите рискове, необходими ресурси за изпълнение на тези мерки, срок за прилагане на мерките и отговорни лица?			
24/8	Има ли приети вътрешни правила, регламентиращи процеса на управление на жизнения цикъл на информационните и комуникационните системи и техните компоненти?			
25/8	Определят ли еднозначно тези правила условията, начина и реда за придобиване, въвеждане в експлоатация, поддръжка,			

	преместване/изнасяне, извеждане от експлоатация и унищожаване на информационни и комуникационни системи и техните компоненти?			
26/8	Описът на информационните активи съдържа ли информация като: еднозначна идентификация (като инвентарен, сериен номер или др.); основни характеристики; услуги, процеси и дейности, в които участва; местоположение; година на производство, където е приложимо; дата на въвеждане в експлоатация, където е приложимо; версия, където е приложимо; местонахождение на свързаната с него документация (техническа, експлоатационна, потребителска и др.); отговорно лице?			
27/9	Има ли вътрешни правила и инструкции за служителите имащи отношение към процесите и дейностите в обхвата на наредбата, които да гарантират, че те имат подходящата квалификация, знания и умения за изпълнение на отговорностите си?ваната техника и технологии?			
28/9	Горепосочените вътрешни правила регламентират ли процеса за наемане на работа в съответствие с изискванията, свързани с дейността им?			
29/9	Горепосочените правила по предходния въпрос регламентират ли отговорностите и задълженията по отношение на сигурността на информацията при прекратяване или промяна на служебните/договорните отношения?			
30/9	Горепосочените правила по предходния въпрос регламентират ли дисциплинарен процес за лицата, в случаите когато са извършили нарушение по отношение на политиката и вътрешните правила за МИС?			
31/9	Документирани ли са отговорностите на служителите имащи отношение към процесите и дейностите в обхвата на НМИМИС с ясно определени функционални задължения?			
329	Проведено ли се периодично професионално обучение за повишаване на квалификацията на служителите в съответствие с използваните техника и технологии?			
33/9	Провежда ли се ежегодно инструктаж на служителите за повишаване на вниманието им по отношение на МИС, включително и за период от една година назад от датата на настоящото оценяване (от 01.01.2022 г., до 03.01.2023 г.)?			
34/10	В договорите с доставчици на стоки и услуги (трети страни) има ли предвидени изисквания за сигурност на информацията, свързани с достъпа на представители на трети страни до Ваши информация и активи?			

35/10	В договорите с трети страни има ли предвидени изисквания за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити?			
36/10	В договорите с трети страни има ли предвидени изисквания за прозрачност на веригата на доставките?			
37/10	В договорите с трети страни има ли предвидени изисквания за санкции при неспазване на изискванията за сигурност на информацията?			
38/10	В договорите с трети страни има ли предвидени изисквания за отговорност при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на МИС?			
39/10	В договорите с трети страни има ли предвидени изисквания за взаимодействие в случай на възникване на инцидент, който най-малко включва: контактни точки, начин за докладване, време за реакция, време за възстановяване на работата, условия за затваряне на инцидент?			
40/10	Има ли определен служител/служители, отговарящ/отговарящи за спазване на изискванията по договорите с трети страни и параметрите на нивото на обслужване?			
41/10	Има ли изготвен план за действие в случай на неспазване на уговорените дейности и клаузи свързани МИС с третата страна?			
42/11	Има ли приети вътрешни правила за управление на измененията във важните Ви, информационни активи?			
43/11	Прави ли се анализ и оценка на риска преди извършване на изменението?			
44/11	Планират ли се измененията?			
45/11	Измененията съгласуват ли се предварително с всички страни, имащи отговорности към процесите и дейностите в обхвата на НМИМИС?			
46/11	Извършването на измененията, одобрява ли се от Кмета/ представителя на ръководството?			
47/11	Оповестява ли се предварително за извършване на дадено изменение?			
49/11	Има ли план за връщане на системите в предишното им състояние, в случай на необходимост?			

50/14	Има ли разписани и одобрени правила за филтриране на трафика?			
51/15	Има ли политика относно използването на лични технически средства и преносими записващи устройства?			
52/16	Има ли политики и вътрешни правила за прилагане на криптографски механизми?			
53/17	Документират ли се всички операции, процеси и дейности в информационните и комуникационните системи и техните компоненти, извършени с администраторски права?			
54/19	Във вътрешните правила определени ли са правата на достъп до конкретни информационни активи на служителите според длъжността им?			
55/19	Във вътрешните правила определен ли е реда за заявяване, промяна и прекратяване на достъп?			
56/19	За периода от една година назад правен ли е преглед на достъпите?			
57/22	Има ли списък с одобрен софтуер, който се използва в информационните и комуникационните системи на общината?			
58 22	Има ли библиотека с дистрибутиви на използвания софтуер и фърмуер?			
59/22	Има ли вътрешни правила и инструкции за регламентиране на действията по управление на достъпа до нея?			
60/23	Има ли вътрешни правила и инструкции за регламентиране на действията по управление на уязвимости - проследяване за новооткрити уязвимости в сигурността на използваните в системите софтуери и фърмуер, техни актуализации (нови версии, ъпдейти и пачове), или мерки за смекчаването им, публикувани от производителите или доставчиците?			
61/23	Има ли вътрешни правила за придобиване и проверка на произхода и целостта на актуализацията преди идсталирането и?			
62/23	Има ли вътрешни правила и инструкции за регламентиране на действията по прилагането на актуализациите и препоръчаните мерки, които трябва да се извършват съобразно разпоредбите на чл. 11 НМИМИС?			
63/22	Извършва ли се проверка на конфигурационните файлове и/или описание на настройките?			
64/26	Извършва ли се наблюдение на информационните активи?			

65/28	Има ли документи (вътрешни правила и/или инструкции) регламентиращи действията за наблюдение и реакция на сигналите от система/системи за автоматично откриване на събития?			
66/29	Регистрират ли се автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, мрежово оборудване и работни места на администратори?			
67/29	В записите за всяко от тези събития отбелязано ли е астрономическото време, когато е настъпило събитието?			
68/29	Информацията за системните записи съхранява ли се за период не по-малко от 12 месеца?			
69/30	Във вътрешните правила по смисъла на чл. 5, ал. 1, т. 6 от НМИМИС, регламентирани ли са всички дейности при обработката на сигнали и реакция при инциденти?			
70/30	Във вътрешните правила регламентиран ли е реда за подаване на сигнали за настъпили или потенциални събития, оказващи негативно влияние върху МИС?			
7130	Във вътрешните правила съдържа ли се информация за лицата, отговорни за регистъра на инцидентите?			
7230	Във вътрешните правила съдържа ли се реда за регистриране на сигнала, проверката на неговата достоверност, класифицирането му, приоритизирането му и последващото уведомяване за това на подателя?			
73/30	Във вътрешните правила съдържа ли се реда за уведомяване за инцидента?			
74/30	Във вътрешните правила съдържа ли се реда за подаване на информация за начина за разрешаване на инцидента?			
75/30	Във вътрешните правила съдържа ли се реда за приключване на инцидента?			
76/30	Във вътрешните правила съдържа ли се процес за събиране, съхраняване и предаване на доказателства, когато инцидентът предполага извършването на процесуални действия срещу лице или организация, включително необходимите за това записи?			
77/30	Във вътрешните правила съдържат ли се правата на достъп до регистъра на инцидентите?			

78/30	Има ли планове за справяне с инцидентите, които да съдържат информация за отговорника за организацията при настъпване на инцидент; реда за информиране; мерките, които следва да се предприемат и отговорното за това лице; реда за консултиране; реда за следене на параметрите по време на инцидента и лицето, което ще събира и съхранява необходимата информация?			
7930	Има ли разработена стратегия за комуникация, която определя реда за споделяне на информацията за инцидента със служители, партньори, доставчици, клиенти, медии, държавни органи?			
80/32	Има ли вътрешни правила за резервиране и архивиране на информацията?			
81/32	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определена ли е информацията (бази данни, конфигурационни файлове, имиджи на системи и др.), която ще се резервира и/или архивира?			
82/32	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определен ли е типа на резервиране (частично, пълно и др.)?			
83/32	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определен ли е периода на извършване на архивирането и резервирането?			
84/32	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определен ли е броя на копията, които ще се правят?			
85/32	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определено времето за съхраняване на всяко копие съгласно изискванията на нормативните актове и оценката на риска?			
86/32	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определено ли е мястото за съхраняване на всяко копие?			
8732	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определен ли е начина на защита от неправомерен достъп (физическа и логическа);?			
88/32	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определени ли са записи за случаите на използване?			
89/32	В съдържанието на вътрешните правила за резервиране и архивиране на информацията определено ли е лицето, което дава разрешение за използването?			

9034	Има ли разработени планове за действия в случай на аварии, природни бедствия или други непредвидени обстоятелства, които биха причинили прекъсване на предоставяната услуга?			
91/34	Плановете съдържат ли обстоятелствата, за които се отнасят; праговете, при които се задействат; лицето, което дава разрешение за задействането им и реда за възстановяване на услугите и дейностите до определено ниво?			
92/34	Плановете проигравани ли са за период от една календарна година назад?			
93/34	Плановете актуализирани ли са за период от една календарна година назад?			
94/34	Плановете достъпни ли са само за лицата, които имат отговорности за тяхното изпълнение?			
95/34	Плановете съхраняват ли се най-малко на две места, едното от които е извън сградата, в която се намират системите, за които се отнасят?			
96/35	Организира ли се извършване на одити по смисъла на чл.35, ал.1, т.1 и 3 за доказване съответствието на предприетите мерки с горепосочените изисквания на НМИМИС?			

	ЧАСТ II въпроси релевантни на т.2.4 от Методиката			
1/11	Проверяват ли се измененията в тестова среда преди да се извършат?			
2/12	Въвеждат ли се в експлоатаия нови информационни и комуникационни системи само след успешно проведени и документирани тестове, доказващи защита на информациата от загуба на достъпност, интегритет и конфиденциалност?			
3/13	Разделени и изолирани ли са помежду им информационните и комуникационните системи, изпълняващи различни функции?			
4/14	Забранени ли са ненужните портове по протоколи Transmission control protocol (TCP) и User Datagram Protocol (UDP)?			
5/17	Актуализирани ли са идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационните активи?			

6/17	Създадени ли са администраторски профили само на служители, на които е функционално задължение?			
7/17	Ограничени ли са правата на всеки администраторски акаунт, само за административни цели?			
8/17	Специфични ли са данните за автентикация на администраторските акаунти за всяка система?			
9/17	Имат ли данните за автентикация с възможно най-висока степен на сложност?			
10/17	Данните за автентикация съхраняват ли се по подходящ начин и защитени ли са физически и логически?			
11/17	Има ли актуален списък на администраторските профили за информационните и комуникационните системи и техните компоненти?			
12/17	Правата на административните акаунти на администраторите спират ли се за съответния период при невъзможност на администратор да изпълнява пълноценно функциите си поради обективни причини?			
13/17	Паролите за автентикация на администраторските профили сменяни ли са за период от една година?			
14/17	Въвеждат и съхраняват ли се в документацията пароли на административен профил под формата на явен текст или хеш?			
15/18	Използва ли се отделна подходящо защитена среда за целите на администриране на информационните и комуникационните системи и техните компоненти?			
16/18	Ако не се използва отделна подходящо защитена среда за целите на администриране на информационните и комуникационните системи и техните компоненти, защитават ли се потоците информация чрез механизми за удостоверяване и криптиране?			
17/19	Прилагат ли се мерки за автентикация, оторизация и одит на компютърните мрежи и системи?			
18/19	Установена ли е практика минималната дължина на използваните пароли да бъде не по-малко от 8 символа за потребителските и 12 символа за администраторските профили ли е?			
19/19	Регламентирано ли е и сменят ли се регулярно паролите на потребителските акаунти на период не по-голям от шест месеца?			

20/19	Регламентирано ли е достъпът до споделени файлове и принтери да се извършва само от мрежата, контролирана от субекта			
21/20	При използване на достъп до информационни активи извън мрежата използва ли се двуфакторна автентикация?			
22/20	При използване на достъп до информационни активи извън мрежата използват ли се само канали с висока степен на защита?			
23/20	При използване на достъп до информационни активи извън мрежата забранено ли е използването на File Transfer Protocol (FTP) и Remote Desktop Connection?			
24/21	Климатико-механичните условия на хардуерните устройства съответстват ли на препоръчаните от производителя?			
25/21	Усъществява ли се наблюдение на параметрите климатико-механичните условия?			
26/21	Устройствата разположени ли са в зони, които са физически и логически защитени в съответствие с информацията, с която работят?			
27/22	Версиите на използваните в системите софтуер и фърмуер, поддържат ли се техните доставчици или производители и на общината актуални ли са от гледна точка на сигурността?			
28/22	Взимат ли са мерки за недопускане на инсталирането и използването на неодобрен софтуер и фърмуер?			
29/Пр.4	Забранени ли са macros в office пакетите?			
30/Пр.4	Забранени ли са pop-up в браузерите?			
31/Пр.4	Auto play функцията конфигурирана ли е винаги да иска потвърждение на потребителя?			
32/Пр.4	User Account Control конфигуриран ли е до на-високо ниво, така че винаги да издава предупреждения?			
33/Пр.4	При споделянето на файлове и принтери използва ли се настройка Everyone?			
34/Пр.4	Забранен ли е TRACE/TRACK методът?			
35/Пр.4	Забранена ли е anonymous authentication?			
36/Пр.4	Използва ли се Unicast Reverse-Path Forwarding (uRPF) и rate-limiting?			

37/Пр.4	Забранен ли е TLS renegotiation в системи, използващи TLS, или да се конфигурира rate-limiter за ограничаване на броя на предоговаряне на сесия?			
38/Пр.4	В съобщенията за грешки в системите скрита ли е излишната информация?			
39/Пр.5	Забранен ли е AutoComplete?			
40/Пр.4	Използват ли се приложения (add-ons) към браузърите за блокиране на рекламно съдържание?			
41/22	Съхранява ли се off-line копие от актуалните конфигурационни файлове и/или описание на настройките?			
42/22	Копията проверяват ли се регулярно относно качество и годност?			
43/23	Има ли инсталиран антивирусен софтуер?			
44/23	Антивирусният софтуер на всички устройства ли е инсталиран?			
45/23	Антивирусния софтуер актуализиран ли е?			
46/23	Инсталираният антивирусен софтуер позволява ли извършване на пълна проверка за наличие на зловреден софтуер поне веднъж в седмицата?			
47/23	Инсталираният антивирусен софтуер позволява ли проверка на електронната поща и файлове, свалени от интернет, както и на преносими записващи устройства, преди да бъдат отворени?			
48/24	Инсталиран ли е сертификат на уеб сървърите, издаден от доверена система за сертифициране (trusted certification authority system)?			
49/24	Сертификата издаден ли е за съответния уеб сайт или група сайтове?			
50/24	Сертификата уникален ли е?			
51/24	Сертификата използва ли алгоритъм за криптиране поне SHA2?			
52/24	Сертификата актуален ли е?			
53/24	Уебсайта достъпен ли е само по протокол Hypertext Transfer Protocol Secure (HTTPS)?			
54/24	В уеб сайта използват ли се само криптографски транспортни протоколи TLS (Transport Layer Security) версия 1.2, дефиниран в RFC 5246 на IETF (The Internet Engineering Task Force – Специализирана работна група за интернет инженеринг) през 2008 г., версия 1.3, дефиниран в RFC 8446 на IETF през 2018 г., или следващи по-нови версии на такива протоколи?			

55/24	Криптира ли се информацията, обменяна между уеб сървъра и потребителите му?			
56/24	Има ли Web Application Firewall (WAF), който наблюдава и филтрира трафика от и към съответното приложение?			
57/24	Забранено ли е вмъкване на данни от страна на потребителя, освен на определените за това места?			
58/24	Валидират ли се всички входни данни, постъпващи от клиента?			
59/24	Забранено ли е въвеждането на специални символи?			
60/24	Кодирани ли са всички данни, изпращани от клиента и показвани в уеб страница с HTML?			
61/24	Регламентирано ли е ограничение на заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по Url?			
62/24	Конфигуриран ли е типът и размерът на headers, които уеб сървърът ще приеме?			
63/24	Ограничени ли са времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка?			
64/24	За защита от brute force атаки има ли въведено ограничение на допустимия брой неуспешни опити за влизане в системата?			
65/24	Забранено ли е извеждането на списък на уеб директориите?			
66/24	Имат ли бисквитките (cookies) флаг за защита (security flag)?			
67/24	Имат ли бисквитките (cookies) флаг HTTP only?			
68/Пр. 5	Скрита/премахната ли е информацията за платформите и версиите на използвания софтуер в Headers на отговорите на заявките?			
69/Пр. 5	Headers на отговорите на заявките съдържат ли опция HTTP Strict Transport Security (HSTS)?			
70/Пр. 5	Headers на отговорите на заявките съдържат ли опция X-Content-Type-Options?			
71/Пр. 5	Headers на отговорите на заявките съдържат ли опция X-XSS-Protection?			
72/Пр. 6	Headers на отговорите на заявките съдържат ли опция X-Frame-Options?			
73/Пр. 5	Headers на отговорите на заявките съдържат ли опция Content-Security-Policy?			

74/Пр. 6	Headers на отговорите на заявките съдържат ли опция Referrer-Policy Header?			
75/Пр. 7	Headers на отговорите на заявките съдържат ли опция Feature-Policy Header?			
76/24	В главната директория на уеб сайта (website) има ли сложен файл robots.txt?			
77/24	Ако се използва Система за управление на съдържанието (CMS) променено ли е наименованието по подразбиране на папката за достъп до администраторския панел?			
78/25	Ако се използват повече от един DNS сървър, всеки от тях разположен ли е в различна мрежа/подмрежа?			
79/25	Прилага ли се DNSSEC (Domain Name System Security Extensions)			
80/25	Минимализирани ли са DNS заявките?			
81/25	Забранен ли се zone-transfers?			
82/25	В конфигурационния файл има ли сложен dmarc (Domain-based Message Authentication, Reporting and Conformance) запис			
83/25	В конфигурационния файл има ли сложен SPF (Sender Policy Framework) запис?			
84/26	Осигурена ли е защита на информационните активи от пожар, наводнение, химическа и физическа промяна на въздуха?			
85/26	Извършва ли се наблюдение на информационните активи?			
86/28	Използват ли се система/системи за автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността системи?			
87/29	Регистрират ли се автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, мрежово оборудване и работни места на администратори?			
88/29	В записите за всяко от тези събития отбелязано ли е астрономическото време, когато е настъпило събитието?			
89/29	Поддържат ли всички компоненти на системите единно време?			
90/32	Копията на информацията етикетирани ли са по начин, указващ еднозначно като минимум каква е информацията, за коя			

	система, какъв метод е използван за създаване на копието, дата и час?			
91/32	Копията на чувствителната информация в криптиран вид ли са и/или са защитени с парола?			
92/32	Копията на информацията съхраняват ли се на отделна машина?			
93/32	Съхранява ли се едно от копията на критичната за дейността информация off-line и по възможност в друга сграда или на отдалечено място?			
94/32	Правена ли е проверка на годността на резервните копия за период от една календарна година назад?			
95/33	Предприети ли са мерки по резервиране на системите и устройствата, балансиране на натоварването на критичните устройства или системи и резервиране на центрове за данни?			

Приложение №2

Принципи за управление на риска

Принципите за управление на риска може да се сведат до следните:

1.Управлението на риска подкрепя създаването и защитата на стойността. Целта на управлението на риска е да помага на общината да постигне целите си. Помощта се изразява в откриване и въздействие върху факторите, които пораждат неопределеност. По този начин, рискът не се управлява сам за себе си, а по начин, позволяващ целите да бъдат постигнати и резултатите подобрени.

2. Управлението на риска е неразделна част от всички процеси в общината. Дейностите, които извършва тя, както и решенията които взема водят до възникването на риск. Затова управлението на риска не се разглежда като отделна дейност, а представлява част от отговорностите на ръководството и е неразделна част от всички процеси в общината, включително стратегическо планиране, управление на проекти, управление на промяна.

3. Управлението на риска е част от вземането на решения. Управлението на риска дава възможност за информирано вземане на решения. Когато вземащите решения разполагат с необходимата информация те могат да направят информиран избор, чрез който да определят възможните решения, да определят приоритета и да правят разлика между различните алтернативи.

4. Управлението на риска изрично разглежда неопределеността. При управлението на риска се взема предвид същността на неопределеността, въздействието й върху целите и начините за нейното отстраняване. Рискът може да бъде успешно управляван или овладян, само ако се разбират естеството и източника на неопределеност. Важен момент е извършването на задълбочен анализ на неопределеността, за да не се допусне нейното подценяване или надценяване.

5. Управлението на риска е системно, структурирано и своевременно. Управлението на риска изисква въвеждането на организационни практики, които да отчитат рисковете, свързани с всички решения. От изключително важно значение е процесът на управление на риска да се прилага в точния момент на вземане на решения. В противен случай могат да бъдат загубени благоприятни възможности или да бъдат причинени значителни загуби.

6. Управлението на риска се основава на най-добрата налична информация. За правилното разбиране на рисковете от решаващо значение е качеството на наличната информация. Източници на информация могат да бъдат данни за минали периоди, опит, обратна връзка, наблюдение, анализи, експертна оценка. Понякога наличната информация може да бъде ограничена, което трябва да се отчита при вземането на решения, както и всякакъв друг вид неопределености, свързани с нея. Надеждността и верността на информацията трябва да се оценяват редовно за точност, приложимост и актуалност.

7. Управлението на риска е адаптивно. За да отговори на нуждите на всяка една община, управлението на риска трябва да се прилага в съответствие с външната и вътрешната среда и с характеристиките на конкретната община. Всяка общна е различна и има своя собствена култура, среда, стил на управление и няма единствен и правилен начин за разработване и прилагане на процеса за управление на риска. Необходима е гъвкавост и адаптивност, за да се постигне желания резултат.

8. Управлението на риска взема предвид човешки и културни фактори. Поведението на хората, техните способности и възприятия могат да улеснят или възпрепятстват постигането на целите на организацията, което само по себе си

представлява риск и трябва да се управлява. Ръководителите трябва да отчитат влиянието на човешките и културни фактори и да разбират и управляват тяхното въздействие, като:

-проявяват уважение и разбиране на индивидуалните различия;

-зачитат вижданията на хората;

-признават усилията на отделните хора;

-ценят знанията;

-проявяват обективност и др.

9. Управлението на риска е прозрачно и приобщаващо. Принципът предполага подходящо и навременно участие на всички участници в процеса и най-вече на тези, които вземат решенията. Участието на заинтересованите страни в процеса им позволява ясно да представят своите виждания, които да бъдат взети под внимание при управлението на риска. Ключът към прилагането на този принцип е създаването на доверие. Доверието е едно крехко и особено чувствително състояние, което лесно може да бъде разрушено. За да се избегне това е необходимо съответните заинтересовани страни да бъдат включени на всеки етап от процеса на управление на риска. Във тази връзка особено актуални стават въпросите относно осигуряването на поверителност, сигурност и защита на предоставената и използваната в процеса информация.

10. Управлението на риска е динамично, повтарящо се и реагиращо на промени. Всяка промяна във външната и/или вътрешната среда или пък в целите на общината, неизбежно води до промяна на рисковете. Успешното управление на риска предполага, че процесът е проектират по начин, който отразява динамиката на промените, в общината. Защото всяка промяна води до възникването на нови рискове, изчезване или промяна на съществуващите.

11. Управлението на риска улеснява непрекъснатото подобряване на общината . Подобряването стои в основата на всичко. Непрекъснато подобряване трябва да има както на процеса на управление на риска, така и на всеки друг аспект от общината. Разбира се не бива да се прекалява с излишно усложняване на процеса, защото по този начин ще се ограничи възможността за търсене на благоприятни възможности и ще се намали гъвкавостта на реагиране на общината.