Европейски съюз

ОПАК. Експерти в действие

Европейски социален фонд
Инвестиции в хората

Проект „**Подобряване на административното обслужване на потребителите чрез надграждане на централните системи на електронното правителство”**” с рег. № К11-32-1/ 20.9.2011 г., осъществяван с финансовата подкрепа на Оперативна програма „Административен капацитет”

Проектът се финансира от Европейския социален фонд и от държавния бюджет на Република България

СЪЗДАВАНЕ НА УНИФИЦИРАНИ ИЗИСКВАНИЯ КЪМ ЦЕНТРОВЕТЕ ЗА ОСОБЕНО ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ В СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ

МЕТОДИКА ЗА ПРИЛОЖЕНИЕ НА ЕДИННИТЕ ДЪРЖАВНИ ИЗИСКВАНИЯ ЗА ИЗГРАЖДАНЕ, СЕРТИФИЦИРАНЕ И ПОДДЪРЖАНЕ НА НИВОТО НА СИГУРНОСТ НА ЦЕНТРОВЕ ЗА СЪХРАНЕНИЕ НА ОСОБЕНО ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ ЗА НУЖДИТЕ НА ЦЕНТРАЛНА ДЪРЖАВНА АДМИНИСТРАЦИЯ В СЪОТВЕТСТВИЕ СЪС СИСТЕМА ОТ УНИФИЦИРАНИ ДЪРЖАВНИ ИЗИСКВАНИЯ И ИЗИСКВАНИЯТА НА БДС ISO/IEC 27001:2005.

Съдържание

СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ

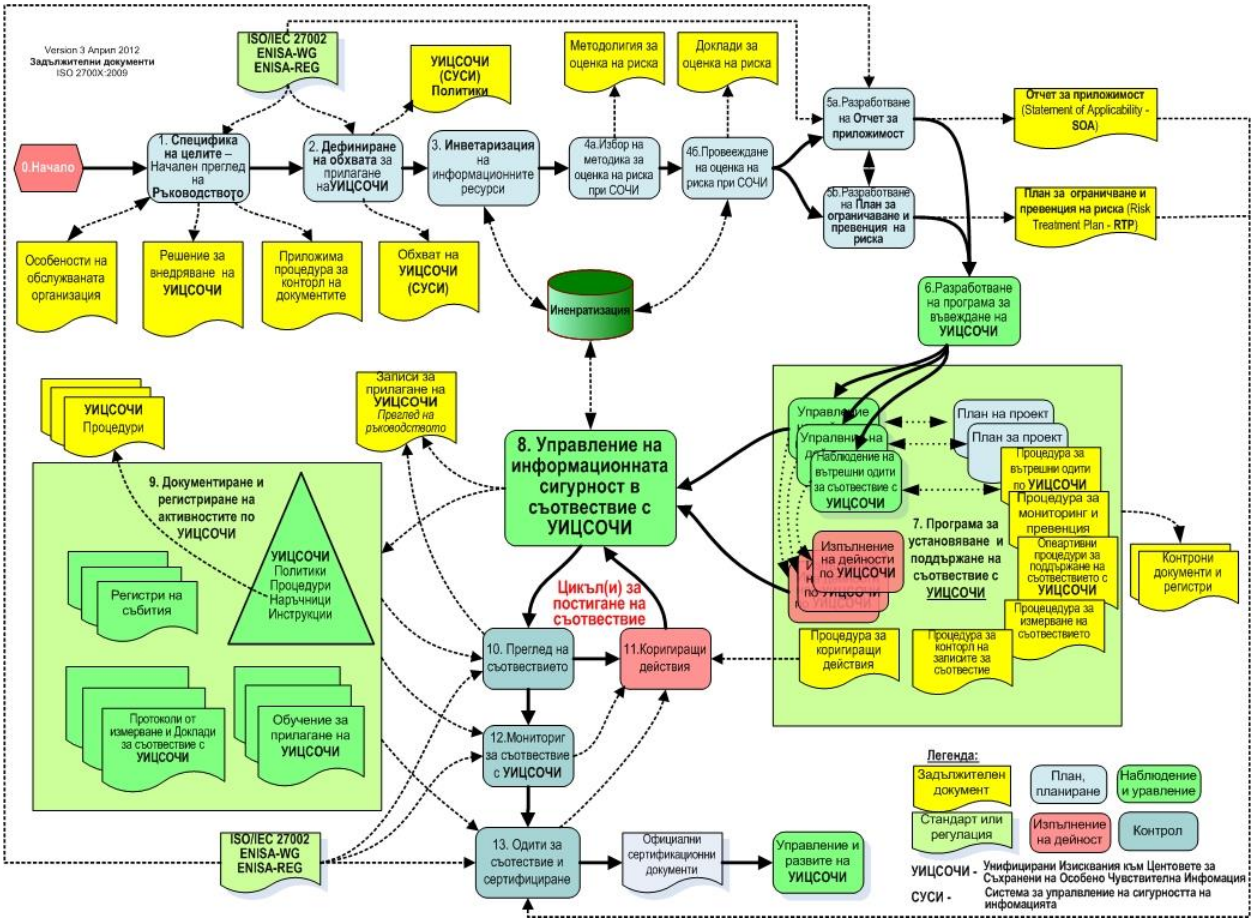
ЕУИЦСОЧИ	**Единни унифицирани изисквания за Центровете за съхранение на особено чувствителна информация**
МДВП	**Максимално време на прекъсване**
ПИПД	**Планиране-изпълнение-проверка-действие**
ЦСОЧИ	**Център за съхранение на особено чувствителна информация**
ISO	**International Standard Organization**

1. Цел

Целта на настоящата методика е да регламентира реда и начините за изграждане и сертифициране на обекти във връзка с ЕУИЦСОЧИ.

2. Структура на методиката за приложение на ЕУИЦСОЧИ

Структурата на методиката за приложение на **ЕУИЦСОЧИ** е представена на Фиг.1.



Фиг.1. Методика за изграждане и сертифициране на обекти във връзка с ЕУИЦСОЧИ

3. Оценка на текущото състояние на защита на информацията и оперативната съвместимост от гледна точка на специфичната система от рискове за осигурявания процес на информационно обслужване в обекта за приложение – център за съхранение на чувствителна информация.

3.1. Идентификация и категоризация на активите.

3.1.1. Активите в обхвата на ЦСОЧИ се идентифицират поединично в съответствие с предварително определена класификационна структура.

3.1.2. За идентифициране на активите на приемливо ниво на детайлност, за всеки един актив задължително се определят:

а) Наименование;

б) Тип и подтип;

в) Идентификатор (напр. инвентарен номер, персонален номер и т.н.);

г) Местоположение;

д) Категория (съобразно стойността на актива за ЦСОЧИ);

е) Класификация за сигурност;

ж) Изисквания за съответствие (съгласно приложимото законодателство и стандартите на ЦСОЧИ);

з) Собственик[1];

и) Допълнителна информация, съответстваща на типа/подтипа на актива.

3.1.3. Идентифицираните активи се вписват в специализиран регистър на активите.

3.2. Оценка на общите и специфичните рискове за процеса на информационно обслужване в обекта за приложение.

3.2.1. Идентифициране на заплахите за активите.

Заплахите се идентифицират по произход и по тип в зависимост от типовете и подтиповете активи, върху които биха могли да въздействат и наличието на съответстващи на характера им уязвимости.

3.2.2. Идентифициране на уязвимости.

Уязвимостите се идентифицират в съответствие със свойствата и характеристиките на обкръжаващата среда, типовете и подтиповете активи, с които се асоциират, както и със заплахите, които биха могли да ги използват.

3.2.3. Преценяване на въздействието върху идентифицирани активи.

Въздействието върху идентифицираните активи се преценява на базата на критерий за максимално време на прекъсване (МДВП) и на базата на критерий за оценяване на възможните последствия в резултат на загуба на поверителност, цялостност на данни, представляващи особено чувствителна информация.

[1] Терминът "собственик" означава физическо лице или обект, одобрено от Ръководителя на Центъра за съхранение на особено чувствителна информация да носи отговорността за контрол на производството, разработването, поддържането, използването и сигурността на активите.
Терминът "собственик" не означава, че лицето има действителни права на собственост на актива

3.2.4. Преценяване на вероятността за реализиране на заплахи.
Вероятността за реализиране на дадена заплаха се преценява като се взема предвид колко често се реализира заплахата и колко лесно уязвимостта, съответстваща на разглеждания актив може да бъде използвана.

3.2.5. Преценяване нивото на въздействие на механизмите за контрол.
Въздействието на механизмите за контрол по отношение на идентифицираните рискове се преценява на базата на обобщени данни от проведени измервания и отчитайки техните характеристики.

3.2.6. Остойностяване на риска.
Стойността на рисковете за всеки актив се определя разделно с/без отчитане на нивото на въздействие на механизмите за контрол чрез функция за изчисление на стойността на риска.

3.2.7. Определяне нивата на риска.
Нивата на риска се определят в разделно в съответствие със стойностите на риска с/без отчитане на нивото на въздействие на механизмите за контрол.

3.2.8. Третиране на риска.
Възможностите за третиране на риска се избират на база резултата от оценяването на риска, очакваните разходи за внедряването им и очакваните ползи от тях, като те могат да бъдат:

1) Намаляване на риска - нивото на риска се намалява чрез избиране на механизми за контрол в съответствие с ЕУИЦСОЧИ, така че остатъчният риск да може да бъде оценен като приемлив при повторно оценяване;
2) Избягване на риска - когато идентифицираните рискове са отчетени като много големи или разходите за внедряване на други възможности за третиране на риска превишават ползите, може да се вземе решение за цялостно избягване на риска чрез изваждане на планирана или съществуваща дейност или набор от дейности или промяна на условията, при които се извършва дейността;
3) Трансфер на риска - при наличие на достатъчно основания и в зависимост от остойностяването на риска, може да се вземе решение, че рискът трябва да бъде прехвърлен към друга страна, която може много по-ефикасно да управлява конкретния риск;
4) Приемане на риска - когато нивото на риска отговаря на предварително определени критерии за приемливост на риска, се приема, че не е необходимо внедряване на допълнителни механизми за контрол и рискът може да бъде поддържан.

3.3. Анализ на специфичната необходимост от постигане на съответствие с ЕУИЦСОЧИ.

На базата на изходните данни от процеса на идентифициране и преценяване на риска за ЦСОЧИ и решенията, касаещи въздействието върху риска, се анализира специфичната необходимост от постигане на съответствие с ЕУИЦСОЧИ, отчитайки:

- Подлежащите на внедряване ЕУИЦСОЧИ и механизми за контрол от BDS ISO/IEC 27001:2006;
- Степента на параметризация на някои от ЕУИЦСОЧИ;
- Внедрените в момента ЕУИЦСОЧИ и механизми за контрол и
- Изключването на някои от ЕУИЦСОЧИ механизмите за контрол.

За определяне нивото на съответствие с ЕУИЦСОЧИ се провежда вътрешен диагностичен одит.

3.3.1. Разработване на декларация за приложимост.

В съответствие с резултатите от анализа на специфичната необходимост от постигане на съответствие с ЕУИЦСОЧИ се разработва Декларация за приложимост, излагаща подробно всички релевантни за обекта на приложение механизми за контрол от ЕУИЦСОЧИ, както и кратко изложение на причините, поради които някои от механизмите за контрол са отхвърлени.

3.4. Дефиниране на специфичния обхват на проекта за постигане на критериите и поддържане на съответствие с Единната система от държавни изисквания и изискванията на БДС ISO/IEC 27001:2006.

3.4.1. Подход за определяне на специфичните цели, обхват на дейностите и определяне на обектно ориентирани индикатори за оценка на степента на изпълнение на целите.

Специфичните цели, обхвата на дейностите и индикаторите за изпълнение на целите се определят в съответствие с характеристиките на релевантните за обекта на приложение ЕУИЦСОЧИ, критериите за тяхното прилагане и целите по контрола и механизмите за контрол описани в Приложение А на BDS ISO/IEC 27001:2006 и включени в Декларацията за приложимост.

Специфичните цели и обхвата на дейностите по оценката за степента на изпълнение се определят на базата на избраната структура за представяне на ЕУИЦСОЧИ , съгласно ПРИЛОЖЕНИЕ 1. ЕУИЦСОЧИ - Минимални изисквания за съответствие дефинираното множество критерии от Единни държавни изисквания към изграждането и сертифицирането на центрове за съхранение на особено чувствителна информация за нуждите на централна държавна администрация в съответствие с изискванията на БДС ISO/IEC 27001:2005, За всеки един от 8-те раздела в ЕУИЦСОЧИ са дефинирани дейности, ориентирани към съответния раздел. За всяка дейност в ПРИЛОЖЕНИЕ 1 е

определен механизъм за установяване на съответствие , като са приложение следните типове индикатори за оценка на степента на изпълнение:

-количествени индикатори за дейностите, които за обусловени по силата на стандарт или добра практика, която осигурява възможност за определения на количествен измерител за изпълнение и/или постигане на съответствие. За всеки количествен индикатор е поставено в съответствие – основание за формиране и прилагане. Количествените индикатори за обективно измерими и за тях се съставят регистрационни форми, съгласно Приложение 1, в които се отразяват текущата стойност, измерена за съответния индикатор, както и на базата на стойностите и/или доверителните интервали, определени в колона „Критерий/Метрика“ от Приложение 1

-качествени индикатори – тези индикатори са свързани с постигане на съответствие с определен тип функционалност по дейност от Приложение 1. За този тип индикатори за изпълнение на дейностите в колона „Критерий/Метрика“ от Приложение 1 са определени като система от неотменни и измерими свойства, като : технология на изпълнение, като поддържани критични функции, като приложни свойства на обектите, относими към конкретната дейност. Измерването на качествените индикатори се предвижда да бъде реализирано на базата на „Листове за проверка на функционалното съответствие“ със специфична цел, описание на извикванията/ критериите към ЦСОЧИ (колона „Описание на извикванията/ критериите към ЦСОЧИ от Приложение 1). От гледна точка на постигане на обективност при оценката е необходимо „Листове за проверка на функционалното съответствие“ да бъдат попълнение от най-малко двама експерта, независимо един от друг и при различия в оценките да се проведе съвместно оценяване до достигане на единно становище, което да се отрази във финалната версия на „Листове за проверка на функционалното съответствие“

-процедурни индикатори – те са характерни за специфичните цели и изисквания в Раздел VII и раздел VIII. Тези раздели третират организационната структура и системата за управление на сигурността на информацията (СУСИ), които са взаимно свързани, тъй като на базата на ролевия подход при дефиниране на организационната структура и свързаната с него матрица на компететностите се осигуряват условията за фактическото прилагане и ефективността на СУСИ. За този тип индикатори се прилага двуфазна оценка:

--документална фаза, в която се проверяват длъжностни характеристики (за Раздел VII) и степента на разработка на СУСИ;

--процедурна фаза , в която се проверяват записите по прилагане на СУСИ от момента на внедряването до момента на измерването.

Предлаганият подход за оценка „индикатор-измерване-съотвествие“ води до две състояния за изпълнение , съгласно Приложение 1. За всяко едно от изискванията се формира оценка от тип: „съответства“ или „ не съответства“ като не се допускат междинни състояния, а единствената възможност е да се определи допълнителен период за постигне на изискваната в Приложение 1 степен на изпълнение. В края не периода се определя частичен контрол за съответствие, само за критериите, които не са изпълнени.

-

3.4.2. Структура, особености и методически аспекти при разработването и управлението на проекти за въвеждане и поддържане на устойчива съвместимост със системата от Единни държавни изисквания.

След изготвяне на Анализ на специфичната необходимост от постигане на съответствие и адаптиране на изискванията на ЕУИЦСОЧИ и BDS ISO/IEC 27001:2006 за конкретния ЦСОЧИ се изготвя проект за реализирането на техническите и организационни мерки за постигане на поддържане на устойчива съвместимост със системата от ЕУИЦСОЧИ. Структурата на проекта задължително трябва да включва:

1) Обхват на проекта;
2) Описание на проекта;
3) Цел на проекта;
4) Очаквани резултати;
5) Основни задачи;
6) Организация на проекта;
7) Основни рискове за проекта;
8) Доставчици;
9) Необходими финансови ресурси;
10) Необходими организационни ресурси;
11) Подробен план за реализация на проекта, включващ мерките за ограничаване и превенция на риска, определени в Декларацията за приложимост.

От методическа гледна точка управлението на проекта се реализира на базата на процесния модел като от приложна точка могат да се дефинират следното минимално множество от процеси за реализирането на Проект за установяване и поддържане на съответствие с ЕУИЦСОЧИ (респективно и BDS ISO/IEC 27001:2):

Базови процеси:

- *Процес 1*:Оценка на възникващата необходимост за постигане на съответствие с ЕУИЦСОЧИ;
- *Процес 2:*Дефиниране на проекта, съгласно определената структура от 11 елемента и спецификата на възникващата необходимост;
- *Процес 3:*Установяване на съответствие и постигане на индикаторите, съгласно Приложение 1 от ЕУИЦСОЧИ;
- *Процес 4:* Оценка на съответствие и определяне на коригиращи действия
- *Процес 5*.Поддържане на съответствието.

Базовите процеси осигуряват т.е. „верига на добавената стойност“ на проекта като преминаването през тях гарантира необходимия минимум от активности за промяна на състоянието на обекта (Център за данни) от несъответстващ към съответстващ по

отношение на ЕУИЦСОЧИ. За всеки от процесите от веригата е определена на входно-изходната свързаност. Оценката на възникващата необходимост (Процес 1) е задължителната настройка на обхвата на проекта към спецификата на конкретния Център за данни. Практическия изходен резултат дава база за провеждането на Процес 2 – какъв обхват, какви цели, какви дейности за пристигане, с какви доставчици, при каква организация и в каква рискова среда ще се проведе Процес 3, т.е. фактическото установяване на първичното съответствие . Процес 4 се идентифицира до голяма степен със сертификационния одит, а Процес 5 е т.н. „operation" процес , който протича перманентно, като през планиран период от време (циклично се изпълнява Процес 4).

При управлението на проекта е важно да се осигури целева функция , свързана с Декларацията за приложимост, на базата на която се определя и ключовите индикатори за ефективността на управлението :

- Постигане на съответствие с ЕУИЦСОЧИ за минимално време при зададен доверителен интервал на бюджета (бюджетна рамка)
- Постигане на съответствие с ЕУИЦСОЧИ при минимизиран бюджет за време не по-голямо от наложените регламентни или други ограничаващи срокове
- Постигане на съответствие при минимални рискове в периода на трансформацията на състоянието на обекта (центъра за данни) до постигане на съответствие с ЕУИЦСОЧИ.

както и приоритетната роля на един от трите базови индикатора., тъй като всеки един от тях влияе по различен начин на инструментите за управление на проекта за установяване на съответствие с ЕУИЦСОЧИ

Спомагателни процеси:

- Управление на промените
- Управление на ескалациите
- Управление на рисковете

Спомагателните процеси за характери за управлението на всеки проект, т.е. те са проектно независими. В конкретния случай спомагателните процеси преди всичко са свързани с осигуряването на устойчиво качество на управлението на процеса на трансформиране на центъра от състояние преди установяването и състоянието на постигане на устойчиво съответствие с ЕУИЦСОЧИ.

3.4.3. Техническо и организационно проектиране на специфичната система от мерки за постигане и поддържане на устойчива съвместимост със системата от ЕУИЦСОЧИ.

1) За изпълнение на дейностите по проектиране и прилагане на специфичната система от мерки за изпълнение и прилагане на ЕУИЦСОЧИ към конкретния ЦСОЧИ се определя специализирана комисия при спазване на принципа на пропорционалното представителство на организационните структури в ЦСОЧИ;

2) Специфичната система от технически мерки за изпълнение и прилагане на ЕУИЦСОЧИ се проектира в съответствие с технологичните особености и спецификация на релевантните за обекта на приложение ЕУИЦСОЧИ и указанията на БДС ISO/IEC 27002:2008.

3) Специфичната система от технически мерки за изпълнение и прилагане на ЕУИЦСОЧИ е необходимо да бъде документира като инвестиционен проект, разработена като структура и обособени части съгласно изискванията на Наредба 4 за обхвата и съдържанието на Инвестиционните проекти. Този аспект на техническото проектиране е задължителен, тъй като в резултата от прилагането на ЕУИЦСОЧИ се предполага, че ще бъдат направени съществени конструктивни изменения и попада в разпоредбите за В Наредба 5 за техническите паспорти от 28.06.2006 г. за сгради трета и по-висока категория, по определението на чл. 137, ал. 1, т. 3 от Закона за устройство.

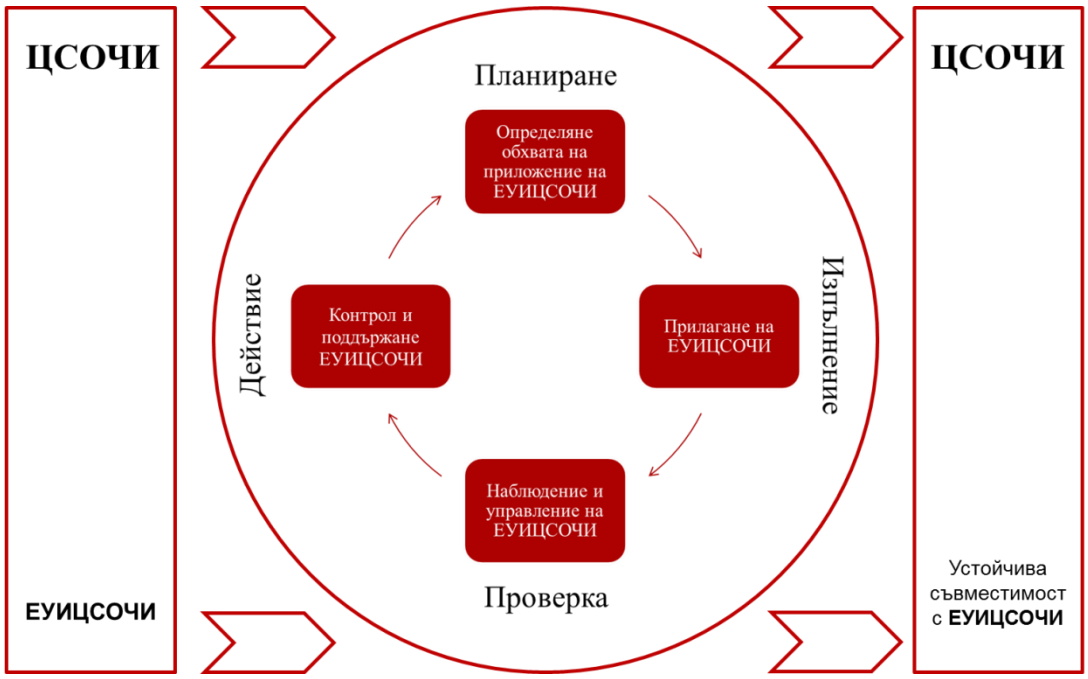
4) Организационното проектиране на системата от мерки предполага управлението на проекта да се развие в контекста на частта от изисквания по Раздел VII и Раздел VIII от Приложение 1 (ЕУИЦСОЧИ) с цел структурата за управление на проекта да се трансформира в рамките на Процес 5 (т.3.4.2) в ролевото множество (съгласно Раздел VII), което да осигурява устойчивото поддръжане на съответствието с ЕУИЦСОЧИ, от гледна точна на внедряването на действаща СУСИ (съгласно Раздел VIII)

3.5. Процесен подход и управление на проекти за въвеждане и поддържане на устойчива съвместимост със системата от Единни държавни изисквания.

Настоящата методика възприема използването на процесния подход при изграждането, сертифицирането и поддържането на нивото на сигурност на центрове за съхранение на особено чувствителна информация.

За прилагането и управлението на системата от процеси в обхвата на настоящата методика се прилага модела "планиране-изпълнение-проверка-действие, ПИПД" (Plan-Do-Check-Act, PDCA).

Прилагането на ПИПД модела по отношение на методиката за изграждане и сертифициране на обекти във връзка с ЕУИЦСОЧИ е представена на Фиг.2.



Фиг.2. Прилагане на ПИПД модел

Определяне обхвата на приложение на ЕУИЦСОЧИ	Оценка на текущото състояние на защита на информацията, определяне на специфичния обхват на проекта, планиране и проектиране на специфичната система от мерки за въвеждане на системата от Единни държавни изисквания.
Прилагане на ЕУИЦСОЧИ	Въвеждане и поддържане на системата от Единни държавни изисквания.
Наблюдение и управление на ЕУИЦСОЧИ	Мониторинг на индикаторите за съответствие с Единните държавни изисквания и изискванията на БДС ISO/IEC 27001:2006.
Контрол и поддържане на ЕУИЦСОЧИ	Управление на промените и инцидентите, одитиране и коригиращи мерки при установяване на несъответствия със специфичния обхват и метрика на индикаторите за изпълнение на ЕУИЦСОЧИ.

3.6. Механизми за мониторинг на индикаторите за изпълнение и осигуряване на устойчиво във времето съответствие с Единните държавни изисквания и изискванията на БДС ISO/IEC 27001:2006.

Мониторингът на индикаторите за съответствие се осъществява на базата на предварително определен модел за измерване ефективността на релевантните за обекта на приложение ЕУИЦСОЧИ и механизми за контрол, определени в Декларацията за приложимост.

Структурата на модела за измерване задължително трябва да включва данни за:

- Идентификацията на структурата за измерване;
- Целта на измерването;
- Обекта на измерването;
- Цел на механизма за контрол;
- Индикатор;
- Формула/Критерии за измерване;
- Аналитичен модел за оценка нивото на ефективност;
- Честотата на измерването;
- Лицето, извършващо измерването;
- Източника на данни за измерването.

Метриката за провеждане на фактическия мониторинг се определя в ПРИЛОЖЕНИЕ 1. ЕУИЦСОЧИ - Минимални изисквания за съответствие дефинираното множество критерии от Единни държавни изисквания към изграждането и сертифицирането на центрове за съхранение на особено чувствителна информация за нуждите на централна държавна администрация в съответствие с изискванията на БДС ISO/IEC 27001:2005. Методическите аспекти за установяване на съответствието са представени в т.3.4.1, като за всяка от трите групи измерители се прилага диференциран подход.

Периодичността на мониторинга се определя в зависимост от началната оценка за съответствие и периода, необходим за провеждане на коригиращите действия, но не по-късно от 6 (шест) месеца след сертификационния одит и за период не по-дълъг от 1 (една година) при продължаване на сертификацията за съответствие (ресертифициране). Тъй като обхвата на съответствието по отношение на ЕУИЦСОЧИ е по-широк от обхвата на БДС ISO/IEC 27001:2006 е необходимо да се институционализира областта на компетентност на сертифицирания одитор по БДС ISO/IEC 27001:2006, като към нея се добавят специфични разширени профили, във връзка с обхвата на ЕУИЦСОЧИ. Същите изисквания следва да се приложат и към вътрешните одитори с оглед на тяхната сфера на копететност и обхват на задачите като функционална роля, съгласно раздел VII от Приложение 1.

3.7. Управление на промените и инцидентите при поддържане на устойчива съвместимост със системата от единни държавни изисквания.

3.7.1. Управление на промените.

1) Промените в обекта на приложение на ЕУЦСОЧИ се инициират на базата на информацията от мониторинга на параметрите, извършван от системата за мониторинг и ранно предупреждение и прогнозира или открива тенденции в повишаване на рисковия потенциал в резултат на несъответствие по отношение

на ЕУИЦСОЧИ на един или повече основни или спомагателни елементи от инфраструктура на Центъра за данни;

2) Промените в обекта на приложение на ЕУЦСОЧИ се инициират чрез подаване на заявка за промяна;

3) Заявката за промяна задължително трябва да включва данни за:

- Лицето иницииращо промяната;
- Цел на промяната;
- Характера на исканата промяна;
- Основанията за исканата промяна;
- Приоритета на промяната;
- Обхват на исканата промяна;
- Услугите, които ще бъдат засегнати от промяната;
- Активите, които ще бъдат засегнати от промяната;
- Ползите от исканата промяна (технически и финансови);
- Рисковете, свързани с прилагането на промяната.

4) Всяка заявена промяна се оценява от специализирана комисия в структурата на ЦСОЧИ;

5) Комисията отхвърля или утвърждава предложената промяна, отчитайки потенциалните ползи и рисковия потенциал на предлаганата промяна.

6) За всяка утвърдена промяна комисията определя критерии за приемане и се разработва план за нейното прилагане.

7) Прилагането на промените се извършва задължително след провеждане на тестове и анализ на постигнатото съответствие с предварително определените критерии за приемане и при спазване на изискванията на ПРИЛОЖЕНИЕ 1. ЕУИЦСОЧИ - Минимални изисквания за съответствие дефинираното множество критерии от Единни държавни изисквания към изграждането и сертифицирането на центрове за съхранение на особено чувствителна информация за нуждите на централна държавна администрация.

8) Управление на промените се допустимо да се реализира и на етапа на изпълнение на Процес 1 (т.3.4.2.),ако в резултат на оценка на възникващата необходимост се установи съществена причина за промяна на метрика и/или разширяване на обхвата на системата от изисквания, съгласно Приложение 1. Причините са отразяват в Декларацията за приложимост и се съставя редактирана версия на Минималните изисквания (Приложение 1), като се отчитат особеностите на обекта, установени по време на Процес 1.

9) Заявката за промяна не се изпълнява,ако тя е в противоречие с базовата версия на Минималните изисквания (Приложение 1) или предполага трайно несъответствие с един или повече критерии, независимо, към кой от 8-те раздела са съотносими.

3.7.2. Управление на инцидентите.

1) При получаване на информация относно инцидент в сигурността на информацията и/или трайно отпадане на устойчивостта на съответствието с ЕУИЦСОЧИ се анализира фактическата обстановка и определя типа на инцидента в съответствие с неговите характеристики и рисков потенцила.

2) За всеки инцидент в сигурността на информацията и/или несъответствие към адаптираната версия на ЕУИЦСОЧИ се оценяван степента на въздействие на инцидента по отношение на прилежащите на ЦСОЧИ активи и се определя неговия приоритет.

3) За всяко събитие на докладван в следствие на автоматичен или физически мониторинг потенциален пробив в сигурността на информацията и/или несъответствие по отношение на ЕУИЦСОЧИ се определя инкубационен период, в който събитието се наблюдава и се трансформира при устойчива честота на повторение като инцидент. Размера на инкуабационния период се определя в оперативна инструкция, част от процедурата за управление на инциденти, която се разработва индивидуално за всеки отделен обект.

4) На базата на определения приоритет на инцидента и след изтичане на инкубационния период (трансформиране на събитието в инцидент) се изпълнява следната последователност от:

- Незабавно се предприемат мерки за ограничаване въздействието на инцидента;
- Уведомяват се отговорните лица;
- При необходимост се сформира работна група за отработване и справяне с последствията от инцидента;
- В случаите, когато инцидента съставлява нарушение на законови и нормативни изисквания уведомява съответните компетентни органи;
- Извършват се действия за отработване и приключване на инцидента.

5) След овладяването на инцидента:

- Установяват се причините за възникване на инцидента;
- Идентифицират се несъответствия с ЕУЦСОЧИ и механизмите за контрол, които не са изпълнили целите на контрола;
- Определят се необходимите превантивни действия за отстраняване на причините за възникване на инцидента и недопускане повторната му поява;
- Събират се и се осигуряват контролни записи и доказателства, в случаите, когато инцидента съставлява нарушение на законови и нормативни изисквания, в съответствие с разпорежданията на компетентните органи;
- Изготвя се доклад за отработен инцидент в сигурността на информацията.

- Документира се процедурата за ефективна реакция за локализиране овладяването на инцидента и минимизиране на потенциалните щети, загуби и друг тип негативни въздействия.

3.8. Одитиране и прилагане на коригиращи мерки при установяване на несъответствие със специфичния обхват и индикаторите за изпълнение на единните държавни изисквания за обекта на приложение.

3.8.1. Провеждане на вътрешни одити.

1) Провеждането на вътрешни одити се извършва от квалифицирани одитори на базата на изготвен и утвърден годишен график за провеждане на вътрешни и външни одити;

2) За всеки конкретен одит се разработва индивидуален план, с който се определят:

- Обхвата и целите на одита;
- Продължителността на одита;
- Вида на одита;
- Одиторския екип;
- Методите на провеждане на одита;
- Планирани дейности по часове.

3) Определените цели на одита се постигат чрез преглед на документите и записи, преки наблюдения и провеждане на интервюта с отговорните лица за спазване на съответствието с ЕУИЦСОЧИ и стандарта BDS ISO/IEC 27001:2006, като резултатите, констатациите и препоръките от одита се обобщават в специален доклад.

4) При установяване на несъответствие с ЕУИЦСОЧИ и стандарта BDS ISO/IEC 27001:2006 същото се класифицира в съответствие с неговия характер и обхват се определят подходящи коригиращи мерки за неговото отстраняване.

5) За прилагането на коригиращи мерки се разработва план, в който се определят действията за прилагане на коригиращите мерки, сроковете и отговорните лица за тяхното изпълнение.

3.8.2. Провеждане на външни одити.

1) Външни одити на ЦСОЧИ се провеждат от:

- Сертифициращата организация;
- Структури на държавната администрация, упълномощени по силата на приложимото законодателство.

2) Одитите от страна на сертифициращата организация се провеждат съгласно изискванията на стандарта БДС ISO/EN 19011:2011 по предварително съгласуван с ЦСОЧИ график;
3) Одити от страна на упълномощени структури на държавната администрация се извършват по реда и критериите, определени изрично за тези случаи.