Специфики на процесите по планиране, проектиране и внедряване на ISMS (СУСИ)

Доклад на организиран от БИС семинар-дискусия по темата
"Криза, киберзаплахи и информационна сигурност"
инж. Бончо Антонов, старши консултант, Алфа Куолити
2011-05-19, гр. София

В това изложение няма да доказваме, че сигурността на информацията е критично важна за бизнеса и обществото. Това е вярна теза, говорена е многократно и, надяваме се, в днешно време няма кой да я подлага на съмнение или да я оспорва.

Няма и да се убеждаваме взаимно, че системите за управление на сигурността на информацията, построени на стандартите от серията ISO/IEC 270XX, създават пълни гаранции за постигната сигурност – това не е вярно. Да, системите само повишават значително равнището на сигурност и създават условия и подходи това равнище да се удържа и да се развива в посока на подобрения – разбира се, само ако се прилагат адекватно и правилно изискванията на ISO/IEC 27001. Идеята за "относителна" и "достатъчна за практическите нужди" сигурност в стандарта я има и тя е заложена, както ще видим след малко, и на концептуално равнище.

Налагаме си тези две ограничения, за да фокусираме вниманието си към нуждите на хората, на които им предстои да проектират и внедряват СУСИ и по-точно към онези специфики, които ако са познати и реализирани, засилват ефикасността на СУСИ и така организациите генерират доверие и, нека вместо "сигурност" кажем "спокойствие", за своя бизнес, за партньорите си и за клиентите, за обществото като цяло и, разбира се, и за успех в един сертификационен процес.

Налага се обаче да се кажат няколко предварителни думи ...

За кои организации се отнася СУСИ? Или, да го кажем метафорично, "За кого бие камбаната?"

Нека да започнем с това, че приложението на ISO/IEC 27001 би трябвало да засяга много повече организации, отколкото в момента познава българската практика. Едва ли има "бизнес", който да не работи с информация за клиентите и да не генерира собствена чувствителна информация, необходима да бъде добре опазвана, за да продължи да съществува бизнесът и за да е успешен.

В този смисъл не са единствено организациите, които Законът за електронното управление задължи да въведат и поддържат СУСИ. Тук може да започнем изброяване на фирми, за които СУСИ е безусловна необходимост, но които май не са се усетили, защото пазарът им е приспан и, както изглежда, още ще продължи да спи, докато не бъде сепнат от болезнено голяма "издънка":

- фирми, занимаващи се (по един или друг начин) с клинични изпитвания;
- фирми, изпълняващи "инсталационни" услуги от всякакъв вид;
- архитекти и строителни проектанти на бизнес обекти;
- фирми за счетоводно обслужване на фирми;
- охранителни фирми, детективски агенции;
- телекомуникационни оператори;
- туроператори и хотелиери;
- адвокатски фирми;
- застрахователи;
- банкери;
- *и... други.*

Спираме нарочно изброяването като недовършено – нямаме нито амбиции, нито възможности да правим изчерпателен списък, а надали има и смисъл. По-скоро би трябвало всяка организация да

си постави въпрос за значението на сигурността за бизнеса си и да стигне до обоснован извод. По подобен начин би трябвало и всички ние, като клиенти на различни видове бизнеси, също да си зададем въпрос и да намерим отговор дали ще сме спокойни, когато се доверяваме на фирми.

Каква информация трябва да защитава СУСИ?

Нататък ще продължим с напомнянето, че сигурността на информацията засяга всички видове и форми на представяне, разпространение и ползване на информация. Добре замислената и добре приложена СУСИ закриля различните по вид и форма информации и свързаните с тях средства. В този смисъл често пъти СУСИ има доста по-широк обхват от защитата на IT инфраструктурата и само на свързаната с нея информация. Може да се случи СУСИ да е необходима за организация, в която няма нито един компютър (надали има такава, но на теория това е вярно), но е достатъчно да се водят важни разговори под заплахата да бъдат подлушани или пък да има досиета или проекти, заплашени от унищожаване, разкомплектоване, загубване или преднамерена кражба.

Без какво не може в началото? Опознаване на фамилията стандарти и логиката на метода PDCA

Преди да се захванем с прилагане на стандарта, ще е нужно да обърнем внимание поне на две неща – първо, трябва да опознаем съдържателно основното ядро от фамилията стандарти. Това ще осигури правилното разбиране на ISO/IEC 27001 и прилагането му без лутане и грешки. Второ, ако сме пропуснали да научим философията на метода PDCA, ще се наложи да навакваме или да си я припомним. Изискванията на стандарта са групирани в раздели, които се водят точно по линията на PDCA. Нещо любопитно – един от разделите, четвърти, сам по себе си е изграден по логиката на PDCA цикъла и с това се акцентува вниманието точно на този раздел, защото той представя задълбочено най-съществената част от жизнения цикъл на СУСИ – планирането.

Но да се върнем на първото, което е необходимостта да опознаем най-общо фамилията стандарти:

- БДС ISO/IEC 27000 – тук намираме значението на термините, ползвани в ISO/IEC 27001;
- БДС ISO/IEC 27002 – това са добри практики по прилагане на ISO/IEC 27001/Annex A;
- ISO/IEC 27003 – твърде полезен стандарт! Той е ръководството за внедряване на СУСИ;
- ISO/IEC 27004 – дава насоки за планиране на измерители на ефикасността на СУСИ;
- БДС ISO/IEC 27005 – съдържа насоки за практиките на управление на риска;
- БДС ISO/IEC 27006 – изисквания за органите, извършващи одит и сертификация.

Одитите на СУСИ, включително и вътрешните, в основни линии се определят от познатия ни БДС EN ISO 19011, но заради спецификата на СУСИ се подготвят два твърде важни, от гл. т. на практиките на вътрешното и външно одитиране, стандарти:

- ISO/IEC 27007 – сега е *ISO/IEC FCD 27007*, етап 40.60 (DIS – приключено съгласуване). Стандартът ще даде налагащите се уточнения и допълнения към ISO 19011;
- ISO/IEC 27008 – сега е *ISO/IEC DTR 27008* (Draft Technical Report). Стандартът ще даде насоки за одиторите при проверките на механизми за контрол (защита) в СУСИ.

Нататък фамилията продължава в секторни и браншови стандарти. Те не ни интересуват пряко, освен ако сме в някой от тези сектори или браншове и се налага да добавим и някой от тях ...

Да си припомним съвсем накратко какво съдържа стандартът БДС ISO/IEC 27001 …

Раздел 3 "Термини и определения" – всякакви действия по проучване на стандарта или, по-лошо, по започване на проектиране на СУСИ, губят смисъл и опорна точка, ако не се изучат много внимателно термините. Полезно е да се правят справки и с чуждоезичните версии на стандарта.

Раздел 4 "Система за управление на сигурността на информацията" (P) – този раздел представя изискванията за създаване и управление на СУСИ, разпределени в четири групи, които по същество представят вътрешно заложен в Раздел 4 цикъл PDCA, а именно:

- **(P)**/създаването на СУСИ обхваща група ключови изисквания за –
  - обхват, граници, политика на СУСИ и критерии за оценяване на риска,
  - избор и прилагане на метод за оценяване на риска,
  - определяне на възможности за въздействие върху рисковете,
  - избор на цели и механизми за контрол (мерки за защита),
  - одобрение за въвеждане на СУСИ и описването ѝ чрез декларация;
- **(D)**/внедряването и функционирането на СУСИ включва изискванията за –
  - планиране и прилагане на въздействия спрямо рисковете,
  - измерване на ефикасността на механизмите за контрол,
  - обучения, управление на ресурси и "хватки" за бързо засичане на пробиви;
- **(C)**/наблюдението и прегледът на СУСИ съдържа изискванията за –
  - наблюдения на индикатори и прегледи за разкриване на опити за пробиви,
  - прегледи на ефикасността на СУСИ по вътрешни данни и информация отвън,
  - актуализация на обхвата на СУСИ, оценките на рисковете и плановете;
- **(A)**/поддържането и подобряване на СУСИ е с изисквания, отнасящи се за –
  - планиране и провеждане на подобрения, на коригиращи и превантивни мерки.

Раздел 4 приключва с изисквания за състав и управление на документите и записите в СУСИ.

Раздел 5 "Отговорност на ръководството" (D) – този раздел обхваща изискванията за:

- ангажиментите на ръководството по повод на СУСИ;
- осигуряването на ресурси за СУСИ;
- дейностите по обучения, осъзнаване и компетентност.

Раздел 6 "Вътрешни одити на СУСИ" (C) – този раздел изисква:

- да има и да се прилага документирана процедура за вътрешни одити на СУСИ;
- одитите да са планирани чрез Програма, отчитаща ссъстояние и важност на процесите.

Раздел 7 "Преглед от ръководството на СУСИ" (C) – в този раздел намираме изисквания за:

- насочеността на прегледите на СУСИ и входните данни, които подготвят един преглед;
- изходните елементи от (резултатите, с които завършва) преглед на СУСИ.

Раздел 8 "Подобрения на СУСИ" (A) включва:

- изисквания за непрекъснато подобряване;
- и изискванията за планиране и провеждане на коригиращи и превантивни действия, като последните подлежат на приоритизиране в зависимост от значимостта на рисковете.

и накрая ...

Приложение А "Цели по контрола и механизми за контрол" – Приложението има особено значение при планиране и проектиране на СУСИ, тъй като дава (неизчепателен!) структуриран в 11 части списък на възможни за прилагане цели по контрола и механизми за контрол.

Този кратък преглед показва ясно, че ISO/IEC 27001 има твърде близко подобие с ISO 9001, а и с останалите стандарти за системи за управление – предимство, което силно облекчава работите по интегриране на СУСИ към съществуваща система за управление. Заедно с това става ясно и,

че ако говорим за специфики в подходите при СУСИ, ще ги намерим най-вече в Раздел 4, където е представена основната част от материята по управление на рисковете.

Специфики на процесите по планиране, проектиране и внедряване

Обхватът

Изисква се обхватът на СУСИ да бъде описан конкретно чрез:

- вида на организацията;
- характеристиките на дейността – т.е. чрез обявяване на включените бизнес процеси;
- точно посочено местоположение на всяка обхваната площадка;
- активи и технологии, които ще бъдат защитавани с прилагане на СУСИ;
- изрично посочени изключвания, за които СУСИ не се прилага.

“Опитът”, който може да имаме от проектиране на системи за управление на качеството, може да ни подведе, поради формалния подход за обявяване на обхват на СУК в най-общи категории.

Непълното определяне на обхвата, спрямо посоченото по-горе, дава цялостно негативно отражение върху всяка последваща работа по планиране и проектиране на СУСИ, включително на етапа на оценяване на рисковете. Прегледът на съдържателната част на дефинирания обхват на СУСИ е важен момент при оценяване на съответствието на системата.

Политиката

По подобен начин стои въпросът и с дефиниране на политиката, свързана със СУСИ, и на това трябва да се обърне специално внимание поради вече допуснати масово разпространени дефекти при “определяне” на политики по СУСИ в българската практика. Основната особеност се състои в това, че и за политиката стандартът изисква тя да се определи въз основа на същите елементи, както и обхватът. Това прави формулировката на политиката да е строго индивидуална за всяка отделна организация. Освен това тя трябва да ориентира към целите, да посочва принципите, на които стъпва цялостната постройка на СУСИ и, най-важното, да послужи за конкретизиране на критериите, използвани при преценката на рисковете в процеса на оценяване.

Получава се така, че политиката по СУСИ, като структура на изложение и като съдържание, може да бъде особено значим индикатор за адекватен, коректен и смислен подход при изпълнение на изискванията за определена политика и за съдържанието ѝ. Споменатите по-горе “разпространени дефекти” в българската практика са, за голямо съжаление, сред най-неприятните:

- виждаме десетки публикувани в Интернет политики на най-различни организации, които са като близнаци, даже има буквално еднакви (само със сменено име на организацията);
- виждаме неправилно цитирано означение на стандарта, например “EN ISO 27001”;
- накрая, виждаме и съчинено от общи кухи фрази и излъчващо формализъм съдържание.

Ако политиката, свързана със СУСИ, не насочва към определяне на целите, ако не декларира принципите на сигурността, които ще определят акцентите в проектирането и функционирането на СУСИ, и ако не може да послужи за изработване на критериите, използвани при оценката на рисковете, такава политика лишава системата от важни опорни точки и, ако бъде публикувана в този вид, вместо да създава, тя руши авторитета на организацията и на тези, които са ѝ “помагали”.

“Съставни” (или сателитни) политики

Тези политики операционализират на работно равнище политиката по СУСИ в три от частите на Приложение А. Грижливото планиране и прилагането на съставните политики има голямо значение за поддържане на сигурността в ежедневната практика, особено ако основното ядро, обхванато от СУСИ, се състои предимно от IT средства за обработка и за обмен на информация.

Такива съставни политики са политиките за:

- резервиране на информация;
- обмен на информация;
- работа на взаимосвързани системи;
- контрол на достъпа;
- планиране и употреба на пароли;
- "чисто бюро" и "чист екран";
- ползване на мрежовите услуги;
- работата с мобилни компютри и комуникации;
- работата от разстояние;
- ползване на криптография.

Може да се случи това, че в една организация, тези или подобни политики да са установени и действащи по силата на приети добри практики. Една от задачите на началната диагностика е да се разбере какви съставни политики съществуват и дали са ефикасни или са "само на хартия".

Ясно е, че ако се наложи (пре)дефиниране на съставните политики, те трябва да кореспондират с основната политика и, освен това, да са съобразени с подходящите за всяка от тях принципи. Но най-важно при тези политики е те да са достъпно формулирани, добре обяснени и усвоени.

<u>За диагностиката и за някои организационни и проектантски решения ...</u>

Може да се погледне на ISO/IEC 27001 не само като "списък от изисквания", но и като "план за действие" понеже редът на излагане на изискванията следва последователността PDCA. С други думи може в по-голяма степен "сляпо" да следваме заложения в стандарта ред и да планираме и проектираме цялата система без да допуснем сериозно отклонение.

1. Практиката допълва този подход и с други решения, които често пъти може да са уместни:
   - възможно е да се работи направо по определяне на обхват и политика почти веднага след като има съответното "стратегическо решение" за въвеждане на СУСИ. В този момент имаме цялата необходима информация, което позволява да ги дефинираме;
   - полезно е, за да бъдат адекватни всяко от следващите решения, да направим първоначална диагностика във вид "GAP анализ" за установяване на разликите между настоящо и желано (определено от стандарта) състояние. Има смисъл диагностиката да мине по реда, който е даден в Приложение А, за да разкрием наличие и вид на съществуващите мерки за защита. Казано кратко – първото, което правим е *диагностика* на съществуващото положение;
   - много е вероятно диагностиката да изяви очевидни слаби места и пропуски, които от гл. т. на сигурността са "уязвимости" и даже, още на този предварителен етап, ако се знаят някои "дежурни" заплахи, може да се стигне и до представа за съответни рискове. Какво следва по-нататък? За предварително установените рискове се налага да се състави предварителен план – така както би следвало да се реагира с план за въздействия след като приключи "официалното" оценяване на рисковете. Планът, който съставяме преди самото оценяване на рисковете, е предварителен, спешно необходим и може да се нарече "*План-старт*";
   - подходящо е нататък, след приключило оценяване на рисковете, планът-старт се допълни с дейности и задачи, налагащи се от резултатите от оценяването, и да добие съдържанието на плана за въздействие върху рисковете – такъв, какъвто се изисква от стандарта.

2. Голяма част от изискванията на стандарта се обявяват чрез “Организацията трябва да ...”, а на места има и “Ръководството трябва да ...”. Чисто практически въпрос във всяка организация е да се разбере кого или кои имаме предвид, когато се казва “организацията” или “ръководството”. Това налага при разработване на СУСИ отговорностите да се насочват към конкретни лица или групи. В някои случаи може да възникне решение за образуване на “Съвет по сигурността”, който да влезе в ролята на нейерархичен консултативен орган, подпомагащ ръководството в решения, отнасящи се до СУСИ, в частност, при разпределяне на отговорности.

3. В повечето примери за методи за оценка на рисковете се стига до определяне/задаване на числова стойност като критерий за установяване на приемливостта на всеки от рисковете. В най-общия случай тази стойност е една от скалата с нивата, пресметната във функция от заплахата като вероятност и като последствия, ако настъпи. Накратко, критерият е практично обоснована прагова стойност в множеството от стойности, представящи нивата на пресметнатите рискове.

Има по-отговорни случаи, в които тази “еднодименсионна” схема може да бъде допълнена с въвеждане и на втори критерий, свързан вече не с нивата на рисковете, а с друг параметър или аспект на управлението на рисковете. В частност, вторият критерий може да бъде обвързан със стойности на някоя от основните характеристики на сигурността – поверителност, цялостност или наличност. Така оценяването на рисковете става още по-реалистично и с акцент, предвид на това, че винаги тези три характеристики нямат еднаква значимост за всяка дадена организация.

4. Документирането на СУСИ е важна част от работите по проектиране и внедряване.
Минимумът от документи и записи, представящи доказателства за съответствие, е определен от стандарта в т. 4.3 (“Изисквания към документацията”), като при процедурите, тези от тях, за които е задължително да са документирани, това е указано изрично. Не е грешка да се смята, че за всички други процедури, споменати в стандарта, може и да няма писани процедури, като с това се разчита на стабилно и еднозначно установени добри практики. Реализмът изисква да си признаем, че в много малко организации може да станем свидетели на такива неписани добри практики, и следователно, добре е в СУСИ да се планират документи и за такива процедури. Тук стигаме до нежеланата опасност системата да стане хипердокументирана, което, естествено, става източник на съпротива, като тази съпротива не е единствената беда. Една от заплахите за сигурността на информацията са многословно описаните и в голямо количество документи норми. Персоналът, дори и да иска, му е трудно да спазва изискванията и допуска неволни грешки.

Има много да се обсъжда по въпроса за достатъчно необходимата и добре скроена документация. Някъде по средата, която балансирано удовлетворява всички интереси, може да се приеме подход за документиране, при който в тялото само на една “макропроцедура” са вградени по няколко “съставни процедури”, в текстовете на които се залага само най-необходимото за организацията нормативно съдържание. С този подход е достатъчно да се разработят само две макропроцедури, като едната покрива всички процедури от стандарта, отделно тези, за които се изисква да са документирани, а с другата – всички процедури, споменати в текстовете на Приложение А.

<u>В заключение</u>

Посочените до тук специфики, свързани с прилагане на ISO/IEC 27001 не са единствените, а може би не са и най-важните. Преценката за важност зависи най-вече от нуждите на практиците. Практиката ще налага да се търсят ефикасни и оригинални решения и по други въпроси, като:

- реалистично и оптимално анонсиране на видовете активи в обхвата на СУСИ;
- степен на детайлизация при включване на активите в схеми за оценка на рисковете;
- условия за групиране и варианти за групиране на еднородни активи;
- степен на детайлизация при разкриване на заплахите и при проучване на уязвимостите;

- избор на подходяща готова или съставяне на своя методика за оценяване на рисковете;
- възможности и ограничения за ползване на IT средства при разработване на СУСИ;
- обективизиране на избора на варианти за въздействие върху рисковете и в избора на мерки за защита от Приложение А;
- разработване на индикатори за установяване на ефикасността на прилаганите мерки;
- удобно формализиране при разработка на Декларацията за приложимост (SOA);
- … и ред други въпроси, които не могат да бъдат обхванати в обема на това изложение.

Става ясно, че усвояването на БДС ISO/IEC 27001 има ред специфични подходи и решения, твърде различни от досега познатите ни стандарти за системи за управление. Това прави проектите за въвеждане на СУСИ едно истинско предизвикателство за тези, които търсят свои решения и не понасят калъпите на чуждата конфекция. Ползвайки умело стандартите с насоки и указания (последният новоиздаден е ISO/IEC 27031:2011 (за бизнес устойчивост)) имаме шанс да генерираме адекватни, оригинални и работоспособни решения за прилагане на ISO/IEC 27001

Приложение – полезни източници на информация

International Organization for Standardization
www.iso.ch

Най-новото в стандартите за сигурност на информацията
http://www.iso.org/iso/specific-applications_it-security

Български институт за стандартизация
www.bds-bg.org

Европейска агенция за сигурност на информацията
http://www.enisa.europa.eu/

Изпълнителна агенция "Електронни съобщителни мрежи и информационни системи"
http://www.esmis.government.bg

ISMS International User Group
www.iso27001usergroup.co.uk

Форум и информационен сайт за стандартите от серията ISO/IEC 27000
http://www.iso27001security.com/

International Register of ISMS Certificates
http://www.iso27001certificates.com/

Визитка

Алфа Куолити ООД – гр. София

02 8687531

office@alphaquality.org

www.alphaquality.org

инж. Бончо Антонов Поптодоров
старши консултант,
продуктов мениджър ISMS

boncho@alphaquality.org

0888 973292