Някои решения за облекчено документиране на системи за управление на сигурността на информацията

инж. Бончо Антонов, Алфа Куолити България

Трябва да си признаем, че все по-често срещаме клиенти, които искат и имат необходимост да въвеждат системи за управление, но пристъпват към това с нежелание или даже се отказват поради страх от "голяма и ненужна бумащина". Друга тема е, ако речем да критикуваме такава една позиция, защото тя няма сериозни основания. Сега искаме да погледнем от различна гледна точка, която приема, че наистина зле документираната система за управление може да тежи и да спъва процесите във фирмата или пък, че бягството от "бумащина" може да се окаже здрава спирачка пред намеренията да се въведе такава система.

Да разгледаме случай с въвеждане на Системи за Управление на Сигурността на Информацията (СУСИ), съгласно ISO/IEC 27001 и по-точно, ако става дума за малка или средна по числен състав фирма, още повече, ако тя не е с ICT профил, а просто ползва ICT активи в дейността си.

Нататък ще продължим с "рецепти" за документиране, но след изричното предупреждение, че те не бива да се приемат за непременно подходящи за всеки един случай. Винаги трябва да се действа така, че документалната част на системата да бъде точно скроена за тялото на организацията.

Решенията за облекчено документиране се основават на ЗАБЕЛЕЖКА 1 в текста на т. 4.2.1 "Общи положения" на стандарта ISO 9001:2008, а именно, че *"... Един документ може да съдържа изисквания, свързани с една или повече процедури. ..."*

Прилагането на даденото в забележката указание, отнесено към документите на СУСИ, може да даде някои от следните резултати.

1) Обща процедура за управление на документите и управление на записите. Това не е ново и се прави и за други системи за управление, но тук е удобно да се добави и "съответния набор от процедури", необходим за означаване и работа с информацията, съгласно възприета схема на класифициране (A.7.2.2 на Приложение А).

2) Обща процедура за коригиращи и превантивни действия. Това също се прави за други видове системи, но тук е възможно да се включат споменатите процедури за "засичане и бърза реакция при пробиви и инциденти" и тези за "наблюдение, преглед и други механизми за контрол" – виж 4.2.2 h) и 4.2.3 a).

С тези две общи процедури плюс документираната процедура за вътрешни одити (т.е., общо три) се изчерпват изискваните от стандарта документирани процедури. Записите, които стандартът изисква като задължителни също не са много.

Става ясно, че проблеми при документиране на СУСИ възникват от това, че стандартът изисква:

- редица други документи, които не са процедури;
- други процедури, за които не се казва, че трябва да са "документирани";
- политики, за някои от които също не се казва, че трябва да са документирани.

Чисто формално, може изобщо да не се документира всичко, за което няма изрично изискване, но тук възникват поне два, ако не и повече, критични моменти:

- трудно е в една действаща СУСИ да се осигури точно спазване на политики или процедури, които не са документирани. Това би заплашило ефикасността на СУСИ;
- дори и да бъде постигнато горното, то трудно и продължително се налага да се разяснява в ситуация на външен одит как именно се осигурява спазването на политики и изисквания, които ги няма в документален вид. Стига се до извод, че ще е значително по-практично да се документират и тези процедури и политики.

3) В практиката се оказва, че в голяма степен Политиката по сигурността на информацията се реализира чрез действието на подкрепящите я частни политики, които стандартът посочва за някои дейности по СУСИ. Оттук естествено следва, че е възможно обединяване на всичките политики в общ документ.

Резултатът, който се получава, е Политика по сигурността на информацията и към нея (в нея):

- политика за резервиране на информация A.10.5.1
- политики (и процедури) за обмен на информация A.10.8.1
- политика (и процедури) за защита при взаимосвързани системи A.10.8.5
- политика по контрол на достъпа A.11.1.1
- политика за планиране и употреба на пароли A.11.2.3
- политика за чисто бюро и чист екран A.11.3.3
- политика за използване на мрежовите услуги A.11.4.1
- политика за работата с мобилни компютри и комуникации A.11.7.1
- политика за работата от разстояние A.11.7.2
- политика по използване на криптографски механизми за контрол A.12.3.1

4) Подобно на политиките е и положението с процедурите. Освен вече споменатите в т. 1) и в т. 2), за СУСИ се изискват още осемнадесет "обикновени, т.е. недокументирани" процедури:

- процедури и механизми за контрол с цел поддържане на СУСИ 4.3.1 c);
- документирани процедури за работа A.10.1.1
- процедури за осведомяване на потребителите за злонамерен софтуер A.10.4.1
- процедури за управлението на сменяеми информационни носители A.10.7.1
- официални процедури за унищожаване на ненужни носители A.10.7.2
- процедури за работа и съхраняване на информацията A.10.7.3
- (политики) и процедури за защита на обмена на информация A.10.8.1
- (политика) и процедури за защита при взаимосвързани системи A.10.8.5
- процедури за наблюдение на средствата за обработка на информация A.10.10.2
- официална процедура за регистрация и дерегистрация на потребители A.11.2.1
- официални процедури за преглед на правата за достъп на потребители A.11.2.4
- процедури за сигурно влизане в системата A.11.5.1
- оперативни планове и процедури за работа от разстояние A.11.7.2
- процедури за контрол на инсталиране на софтуер в операционни системи A.12.4.1
- официални процедури за контрол на измененията A.12.5.1
- процедури за бърза системна реакция на инциденти A.13.2.1
- процедури за осигуряване на съответствие с изисквания на нормативни актове и договорни изисквания A.15.1.2

Веднага става ясно, че не е практично да се тръгне с разработване и прилагане на осемнадесет процедури и така съвсем лесно се стига до решението те да се обединят в едно общо тяло. Но това решение ще се окаже тромаво и непрактично, освен ако преди това не се направи "ревизия" на понятието за процедура или по-скоро за обема и състава на такъв документ. При такава ревизия не трябва да се прави компромис единствено с идеята да се получат кратки и ясни за изпълнение изисквания. За всичко, което остава, са допустими големи "отстъпки" в посока на съкращаване или дори на отказ от станали вече традиционни в "писането на процедури" съвсем непрактични и тромави похвати и "Copy - Paste" щампи.

Ако "ревизираме" в този стил една процедура, възможният резултат може да изглежда така ... (пример)

Процедура	(наименование, означение)
Цели	(посочват се)
Изисквания	(за всяко от тях – какво, кой, как)
Ползвани документи и записи	(посочват се)

Такава "mini"-процедура може да се напише само на 4 – 5 реда и с това се разкрива възможност всички процедури, включени в състава на механизмите за контрол от Приложение А да бъдат групирани в само една компактна "A-master"-процедура, която събира на едно място всички полезни практики за защита на активите и информацията в конкретната организация.

5) Дълбоки размисли би могъл да причини стандартът в онази своя част, където става дума за изискванията към документацията, по-конкретно в следващия му текст ...

"Документацията на СУСИ трябва да включва следното:
a) ...b) … c) … d) … e) … f) …, след които следва
g) документирани процедури, необходими на организацията да осигури ефективното планиране, действие и контрол на процесите, свързани с информационната сигурност, и описание как да се измерва ефективността на механизмите за контрол (виж точка 4.2.3c));"

Може да е трудно да се намери бързо отговор на въпроса "Кои точно са необходимите документирани процедури ... ?", още повече, че те, според стандарта, като че ли са в четири области – планиране, действие, контрол на процеси и измерване на ефикасността на механизми за контрол.

И тук може да се окаже полезен за практиката и лесен за изпълнение подходът за разработване на компактна "ISMS-master"-процедура, включваща всички основни клаузи на стандарта. Полезно е при това в тази процедура да се правят позовавания към всички останали разработени документи на СУСИ. Така тази процедура ще играе роля и на своеобразен справочник на СУСИ.

Двете "мастер"-процедури – "ISMS-master" и "A-master" – взети заедно, всъщност ще дават добра представа за цялостния облик на конкретната СУСИ.

6) Има и други решения, които дават "дребни" предимства и улеснения:

- например, ако се документират целите по сигурността като текущо поддържан запис, който включва и отчетна част, това спестява съставянето на отделни отчети за изпълнение, както би било, ако целите са записани в документ;
- стремим се по-голямата част документация на СУСИ, ако ли не цялата документация, да се създаде, поддържа и съхранява в удобно достъпен за ползване електронен формат;

- за да създадем вътрешна класификационна схема на документацията може да ползваме поле "Properties" на някои документални файлове, в което има различни опции за достъп и ползване.

7) Има документи на СУСИ, за които може да се каже, че е по-добре да си останат отделни – без да се комбинират с други и без да се разделят, защото са с ключово значение:
- декларация за политиката по сигурността на информацията;
- обхват на СУСИ;
- план за въздействие върху риска;
- декларация за приложимост.

8) Записите, които изисква стандартът, също съдържат някакви, макар и не толкова гъвкави и оригинални, решения за удобно и просто документиране.

Някои записи е удобно да се поддържат текущо като регистри, най-добре в електронен формат:
- действия, които могат да окажат влияние върху СУСИ 4.2.3 h)
- записи за всички случаи на инциденти по сигурността 4.3.3
- свързани с решения на ръководството 4.3.1
- записи за резултати от прегледите на СУСИ 7.1
- записи за резултати от коригиращи действия (КД) 8.2
- записи за резултати от превантивни действия (ПД) 8.3

Има възможност, но трябва внимателно да се прецени, горните записи да се комбинират "по двойки":
- действия с влияние върху СУСИ и инциденти;
- за решения на ръководството и резултати от прегледи на ръководството;
- за резултати от КД и ПД.

и така да се образуват нещо като "комби"-регистри.

Комбинирането на серия еднотипни записи в общ регистър води до натрупване на данни, които, ако е използвана подходяща платформа и начин на представяне, биха могли лесно да се обработват за анализи и насочване на подобренията.

9) Изискваните в т. 5.2.2 d) записи за образование, обучения, умения, опит и квалификация всъщност представляват персонални досиета (в частта образование, умения, опит, квалификация), към които може да се прикрепят последователно записи за всяко проведено обучение или може да се поддържа отново персонален или общ регистър със записи за всички обучения.

10) Изискваните в т. 4.3.3 записи "За процеса, описан в т. 4.2", освен тези от тях, които вече са посочени в т.4.3.1, остава да бъдат определени от нас самите в хода на проектирането, но би се очаквало те да са свързани с процеса на оценяване на рисковете и с действията по установяване на ефикасността на приложените механизми за контрол.

В заключение
Идеята да се търсят и прилагат решения за пестеливо документиране има за момента само една цел – да стане стандартът ISO/IEC 27001 по-достъпен, защото нуждата от него е голяма и актуална

2012.05.03