Интервю с участието на инж. Бончо Антонов Поптодоров
Computerworld.bg: Опазването на информацията – мисия на съвременните организации
08.11.2010, http://computerworld.bg

ОПАЗВАНЕТО НА ИНФОРМАЦИЯТА – МИСИЯ НА СЪВРЕМЕННИТЕ ОРГАНИЗАЦИИ

Сертифицирането по стандарти за информационна сигурност и управление на ИТ услуги ще става все по-търсено в България

Константа Григорова

По данни на международния регистър на акдеритираните сертификати по управление на системите за информационна сигурност към 4 ноември по стандарта ISO/IEC 27001:2005 в световен мащаб има общо 6942 сертификата, от които 10 – в България. По данни на Сдружение "Клуб 9000" – единственият, макар и неофициален източник на статистическа информация в тази област, към момента в страната фигурират общо 69 сертифицирани български фирми с валидни към момента сертификати с различен обхват на дейност по стандарта ISO/IEC 27001:2005. Сред тях са технологични компании като Абати, Ай Би Ес (IBS), АСИ Кумпани, Борика Банксервиз, Грамма Нет Ис, Давид Холдинг, Информационно обслужване, Контракс, петте дружества на Лирекс, Мултипроцесорни Системи, Немечек, S&T, CNSYS, Сименс Ентърпрайз Комюникейшънс, Софика Груп, Стоун Компютърс, Теза, Телеком Бизнес Солюшънс, Телепойнт, Транс Телеком и др. Допитването на в. Computerworld България до специализирани организации в сферата на сертификацията показа, че официална статистика или национална база данни за сертифицирането по стандартите ISO (и в частност за ISO/IEC 27001:2005 и ISO/IEC 20000-1:2005) няма.

Сертификация по ISO 27000 и ISO 20000 не съществува.

Стандартите, спрямо които се извършва сертификация, са ISO/IEC 27001:2005 и ISO/IEC 20000-1:2005, изтъкнаха експертите в тази област от Lloyd's Register Quality Assurance (LRQA) и SGS България. ISO/IEC 27001 е процесно–ориентиран стандарт за информационна сигурност, фокусиран върху въвеждането и непрекъснатото усъвършенстване на система за управление на информационната сигурност. Стандартът ISO/IEC 20000, предназначен за сертифициране на системи за управление на ИТ услуги, е базиран на модела за дефиниране на процесите ITIL (IT Infrastructure Library), обясни Георги Шарков, управител на Центъра на Европейския софтуерен институт за Източна Европа (ЕСИ Център България). ITIL е модел от специализирани методологически принципи и синтез от най-добрите практики, разработен с цел да се оптимизират процесите при предоставяне на ИТ услуги. ISO/IEC 20000 е съвместим с и допълващ процесния подход, дефиниран в рамките на ITIL от Департамента за търговия на британското правителство. За разлика от ISO/IEC 20000 ITIL не предполага оценка и сертификация на ниво организация, а е персонална сертификация на ниво отделен професионалист. Друг модел, който допълва ITIL, е CMMI - SVC (Capability Maturity Model Integration for Services). CMMI – SVC предоставя интегриран подход за въвеждане на добри практики за управление на услуги и сертификация на организационно равнище, както и обща процесно ориентирана инфраструктура за непрекъснато подобряване на процесите при разработване на софтуер и предоставяне на услуги, допълни Шарков.

"Стандартите от фамилията 27XXX наистина са много, но организациите и фирмите ги интересува само ISO/IEC 27001, защото той единствено съдържа изисквания, предвиждащи процес на независима сертификация. Голяма част от останалите стандарти във фамилията са стандарти с указания и насоки, по които не се извършва сертификация. Тук се крие и една заблуда, че това кара фирмите много силно да се фокусират върху ISO/IEC 27001 и да пренебрегват други членове на фамилията като ISO/IEC 27002 (определящ добри практики), ISO/IEC 27003 (с указания за проектиране и внедряване), ISO/IEC 27005 (с указания за оценка на риска). Други членове на фамилията са бранщово профилирани и дават указания за

въвеждане на Системи за управление на сигурността на информацията (СУСИ) в организациите от даден бранш – например ISO/IEC 27011 е за телекомуникациите", разказа инж. Бончо Поптодоров, продуктов мениджър ISO/IEC 27001 в Алфа Куолити Интернешънъл.

"Свидетели сме на все по-бързо развиващи се технологии и комуникации и бизнесът става все по зависим от ИТ, но заедно с това съответно растат и рисковете, които застрашават бизнеса, обясни Иван Савов – управител на Муди Интернешънъл България и председател на Европейската федерация на асоциациите на сертифициращите органи в Брюксел - ISO/IEC 20000 е първият международен стандарт, специално насочен към ИТ услугите. Той описва интегриран набор от процеси за управление на ефективно и качествено доставяне на услуги към бизнеса и клиентите на оптимизирана цена". Според Савов, ISO/IEC 20000 става все по-популярен, защото използването на ИТ услуги е критично за успеха на бизнеса, а ИТ услугите са в основата на почти всички важни бизнес процеси. "Бизнесите ползват ИТ услуги от вътрешни и външни доставчици, те изнасят (аутсорсват) бизнес процеси и ИТ услуги и по този начин информационните технологии стават все по-сложни. Нараства необходимостта от по-високо гарантирано ниво на качеството на услугите и гаранции, че доставчиците на ИТ услуги следват добрите практики. Всичко това мотивира организациите да внедряват добри практики за управлението на ИТ и да се сертифицират по управленския стандарт ISO/IEC 20000", допълни Савов. Друг тясно свързан с ИТ стандарт е BS 25999 Business Continuity Management - първият британски стандарт за управление на непрекъснатостта на бизнеса, посочи Савов.

Процесът по сертифициране по ISO 27001:2005 или ISO 20000-1:2005.
За да се сертифицира по стандарта ISO/IEC 27001, една фирма трябва първо да избере консултантска фирма, която да я подготви за сертификация, или ако разполага с достатъчно квалифициран персонал по темата се подготвя сама, каза Даниел Неделчев, водещ одитор по ISO/IEC 20 000 и ISO/IEC 27 001 в Lloyd's Register Quality Assurance (LRQA). Или накратко:
Фаза 1 – подготовка на фирмата за съответствие с изискванията на стандарта ISO 27001:2005 или ISO 20000-1:2005.
Фаза 2 – Избор на сертифицираща организация;
Фаза 3 – Сертификация, която обикновено се извършва на 2 етапа – Етап 1 – преглед на документацията за съответствие с изискванията на съответния стандарт и
Етап 2 – преглед на конкретното прилагане на изискванията на стандарта и създадената документация. За 27001 – да, включително и физически достъп до всички помещения, където се извършват дейностите, особено там, където са привилегированите потребители. За 20000 – не всички компании подлежат на сертификация, трябва основната дейност на фирмата или отдела да е свързана с предоставяне на информационни услуги/технологии. От тази гледна точка част от дейностите (ако е вътрешен отдел) могат и да не бъдат сертифицирани.

"Интересът към стандартите от сериите ISO20000 и ISO27000 в България непрекъснато нараства, твърди Стоян Жеков – водещ одитор по СУСИ към SGS България. - Сертификация е възможна съгласно изискванията на един от стандартите от тези серии, а именно ISO27001:2005 и ISO20000-1:2005. ISO27001:2005 е стандарт, който е приложим за всички видове организации, независимо от типа и вида на дейността им. При ISO20000-1:2005 нещата стоят по-различно – сертификация съгласно изискванията на този стандарт е възможна само за организации, които предлагат ИТ услуги и желаят да управляват качеството на тези услуги съобразно изискванията на стандарта". Според Жеков, фазите и процедурите, през които една организация трябва да премине, за да разработи, внедри и управлява ефективно система за управление съгласно един от двата или двата стандарта едновременно, могат да се опишат най-общо като: определяне на обхват на системите, разработване на документация, определяща правилата на работа, критериите за измерване и подобряване, внедряване на разработената в организация документация и извършване на задължителните вътрешни одити и преглед от ръководството.

След успешното приключване на всички тези етапи е възможно да се проведе и одит за сертификация. Организациите трябва да са определили обхвата на сертификация – възможно е той да обхваща или част, или всички процеси (дейности), които се развиват в компаниите, заключи Жеков. “За да бъде сертифицирана една организация, е необходимо тя да има разработена и ефективно внедрена система за управление на информационната сигурност, да отправи запитване към сертифицираща организация и да избере такава на база компетентност, квалификация и капацитет и предложена цена, условия и срокове. Извършва се одит, при който поради спецификата на стандарта се изисква одит на всички дейности, обвързани със системата за информационна сигурност, като това може да включва в някои случаи дейности, за които се искат специални разрешителни за достъп до информация. Етапите на сертификация условно могат да бъдат определени като 3: планиране и подготовка на одит, извършване и последващи действия. Тези 3 етапа са задължителни за регистрацията на всяка организация по ISO/IEC 27001”, категоричен бе Иван Савов.

“Сертификацията по стандарта БДС ISO/IEC 27001 (като процес) и сертификатът (като документ, декларищ съответствие със стандарта) се свързват с въведена, прилагана, поддържана и подобрявана система за управление на сигурността на информацията. Фазите, свързани с усвояването на СУСИ, са “планиране-изпълнение-проверка-действие”, по-популярни като фази на модела PDCA (Plan-Do-Check-Act), уточни инж. Бончо Поптодоров. - Но всичко трябва да започне от там, че трябва да бъде взето стратегическо решение за въвеждане на СУСИ и това решение да отчита конкретните потребности, цели и изисквания по сигурността, заедно с други специфики като брой и сложност на включените процеси, големина и структура на организацията и всичко да бъде поставено на реалистична основа – както се посочва в текста на самия стандарт - “елементарен проблем да изисква елементарно решение”.

Кой има право да сертифицира (обучение не е = сертифициране)

“Право да извършват сертификация имат само организации, които са акредитирани като сертификационен орган, посочи Стоян Жеков – водещ одитор по СУСИ към SGS България. Акредитиращият орган управлява постоянен контрол над сертификационния орган, за да се гарантира спазването на изискванията на международните стандарти при издаването на сертификати. Получаването на акредитиран сертификат е гаранция за качество и международно признание на извършената сертификация на системите за управление. По отношение на стандарта ISO27001:2005 SGS извършва сертификация под акредитация UKAS и/или БСА, а по отношение на ISO20000-1:2005 се извършва сертификация с itSMF акредитация – единствената в света акредитираща организация за този стандарт.” “Обучението и сертификацията са две отделни дейности, категоричен е и Даниел Неделчев, водещ одитор по ISO/IEC 20 000 и ISO/IEC 27 001 към LRQA. Възможно е сертифициращата организация да предлага обучения по определени стандарти, в случая по ISO 27001:2005 или ISO 20000.” За да бъде сертификатът признат, трябва да бъде издаден от сертификационна организация, която е акредитирана от Национален акредитационен орган, увери Неделчев. Съответният НАО трябва да е член на IAF MLA. По този начин се контролира процесът на сертификация, осигуряващ ниво, приемливо/признато в цял свят. Първият в света Национален акредитационен орган е United Kingdom Accreditation Service (UKAS), под чиято акредитация се издават повечето сертификати по тези стандарти в България. ISO/IEC 20000-1:2005 е разработен и контролиран от IT Service Management Forum (itSMF). Тези контроли се отразяват и с полагането на съответния акредитационен знак на самият сертификат, издаден от акредитираната сертификационна организация, разкри Неделчев. Детелин Александров – директор “Консултантски услуги” в Стоун Компютърс, също изтъкна, че не е задължително условие организацията, предлагаща различни курсове и обучения по международните стандарти да е сертификационна компания. “За да извършваш обучения и издаваш сертификати за водещи одитори (в конкретния случай за стандартите ISO 27001:2005 и ISO 20000-1:2005), следва да имаш акредитация за това - за

методологията, материалите и преподавателите за съответните курсове. Нашите курсове са акредитирани от IRCA за ISO 27001:2005 и от itSMF за ISO 20000-1:2005", посочи Александров. От юли т. г. Стоун Компютърс предлага акредитирани курсове за одитори по международно признатите стандарти ISO/IEC 20000 и ISO/IEC 27001. "От стартирането на предлаганите курсове се наблюдава висок интерес от страна на технологичните компании в България, предоставящи ИТ решения и решения за сигурност както за свои нужди, така и за клиенти. В по-голяма степен интересът е към курсовете за международния стандарт ISO/IEC 27001:2005. Това е обясним факт поради по-голямата комуникация на стандарта в средите на държавната администрация и бизнеса. На този етап все още няма достатъчна вътрешно-корпоративна култура и разбиране за прилагането на стандарта ISO/IEC 20000-1:2005. Факт е, че към ИТ компаниите при участие в обществени поръчки има изискване за сертификат по ISO 9001:2008, а не към релевантния за специфичната им дейност стандарт ISO/IEC 20000-1:2005, заяви Детелин Александров от Стоун Компютърс. - Налагането на ISO 27001:2005 и интереса към него е продиктуван и от изискванията на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност към Закона за електронното управление. Проявява се интерес и към стандарта ISO 20000-1:2005 от ИТ компаниите, предоставящи услуги както и от банките, прилагащи добрите практики на ITIL. Международният стандарт ISO 20000 е изключително близък с добрите практики на ITIL". Според Александров, интересът към курсовете по двата международни стандарта ще расте предвид действащата схема за предоставяне на базвъзмездна помощ „Покриване на международно признати стандарти" по Оперативна програма „Развитие на конкурентоспособността на Българската икономика" 2007-2013. Съгласно приетите международни правила и стандарти, процесите на подготовка по даден стандарт (консултации и обучения) трябва да са разделени от самата сертификация, изтъкна и Юлиан Узунов от Top Management Advisors. "Обикновено подготовката по стандарт като ISO/IEC 27001 - за разлика от други стандарти - предполага задълбочени обучения по някои от методиките за реализация на стандарта, защото част от дейността не може да се изпълни от външен консултант. Консултантът е най-полезен като „фасилитатор" – експерт, който обучава и насърчава служителите на фирмата да прилагат модерно управленско ноу-хау, а не като писач на процедури, които да се оценяват от вътрешни одитори", уточни Узунов.

Според инж. Бончо Поптодоров от Алфа Куолити Интернешънъл, не трябва да се търси задължаваща връзка между услугите за предлагане на обучение и тези за сертификация. Обучения предлагат както фирми с консултантски профил, така и органи за сертификация.

"В редки случаи организациите имат възможността да предложат на клиентите си двете услуги - сертификацията и обучението, с наличието на международните акредитации. Това дава възможност на клиентите да се възползват от цялостно и завършено обслужване, като се запазва проследимостта и прозрачността в процеса на запознаване и работа с международните стандарти", обясни Иван Савов от Муди Интернешънъл България.

КАРЕ 1

Ползите от сертифициране по ISO/IEC 27001:2005 според Даниел Неделчев, водещ одитор по ISO/IEC 20 000 и ISO/IEC 27 001 към LRQA: Наличие на система, гарантираща че фирмена или клиентска информация няма да попадне в неподходящи ръце. Създаване на фирмени правила и политики, осигуряващи опазване на информацията. Контролирано назначаване и освобождаване на персонал. Наличие на система, която постоянно се усъвършенства чрез мониторинг, анализ и проверки. Увереност в контрагентите относно сигурността на техните данни. Съвместимост със световно признат стандарт в областта на информационната сигурност. Намаляване на риска от загуба на информация и система за възстановяване при възникване на аварии от всякакъв характер. Участие в обществени поръчки и предимство в сделките, свързани с институциите, където опазването на информацията е от първостепенна важност, напр. МВР, МО, болници, банки, както и всякакъв тип организации, опериращи с лични данни. Повишаване

на доверието в извършваните от фирмата услуги, характерно е и за двата стандарта - ISO/IEC 27001:2005 и ISO/IEC 20000-1:2005. В българската нормативна база съществува и Наредба за общите изисквания за оперативна съвместимост и информационна сигурност, Приета с ПМС № 279 от 17.11.2008 г., обн., ДВ, бр. 101 от 25.11.2008 г., в сила от 25.11.2008 г. КАРЕ 2 Тенденцията за ИТ компаниите по отношение на вътрешна потребност и полезност е внедряването на стандарта ISO 20000-1:2005 на мястото на ISO 9001:2008, твърди Детелин Александров – директор "Консултантски услуги" в Стоун Компютърс. Според него, ползите от внедряването и функционирането на двете системи са следните: - управление на капацитета и непрекъсваемост на предоставяните услуги; - точност в отчитане на нивото на предоставяните услуги; - управлението на пускането на услугите в реална среда; - правилно управление на отношенията с клиентите и доставчиците; - сигурност по отношение на персонала работещ в организацията; - сигурност при работа при посещение на външни лица; - сигурност на техническите средства за обработка на информацията; - сигурност по отношение на физическите зони и зони за достъп; - сигурност в съхранението на документите и достъпа до тях; - сигурност в преносната среда необходима на техническите средства; - осигуряване на резервираност на информацията и информационните системи; - осигуряване непрекъсваемост на бизнес дейността; - предпазване от непланирани извънредни финансови разходи; - осигуряване непрекъсваемост на дейността и предоставяните ИТ услуги; - изграждане на необходимия корпоративен имидж и сигурност със заинтересовани страни.

Ползите от сертифициране по ISO/IEC 27001:2005

Ползите от сертифицирането на системите за управление са международно признаване на дейността на организациите в тази посока, намаляване на преките разходи за дейността чрез ефективно управление, повишаване на доверието между партниращи си организации, създаване на добра корпоративна култура и много други, посочи Стоян Жеков от SGS България. Според Иван Савов от Муди Интернешънъл България, сертификацията на система за управление на сигурността на информацията доказва, че организацията-притежател на сертификата гарантира в максимална степен сигурността както на собствената си информация, така и на тази на своите клиенти. Внедрената и сертифицирана СУСИ гарантира осигуряването на непрекъсваемостта на бизнеса в случаи на извънредни ситуации и кризи. Покриването на изискванията на всеки от международните управленски стандарти често се разглежда като технически въпрос, за който се търсят конкретни формални решения. По тази причина има огромна девалвация на управленските стандарти, тъй като за повечето служители това е излишна бумащина (и обикновено са прави), изтъкна Юлиан Узунов от Top Management Advisors. По думите на специалиста, истинска полза има, ако внедряването на стандарта е свързано с решаването на реални управленски проблеми и води до повишаване на управленската култура и оптимизация на управленските процеси. "Нерядко сертификацията по даден стандарт се явява задължително условие за участие в обществени поръчки. Не виждам нищо лошо в това, че някои фирми директно си признават, че „Тапията ми трябва само за участие в конкурси!". Твърде често в тръжната документация се поставят условия за покриване на стандарти, без това да допринася за реална оценка на възможностите на дадена фирма. Това прави процеса формален и от двете страни, но явна полза е, че фирмата не може да бъде отстранена от даден конкурс заради липса на сертификация", посочи Узунов.

Пряката полза от сертифицирането на СУСИ се изразява чрез притежаването на издаден сертификат за съответствие с БДС ISO/IEC 27001, обясни инж. Бончо Поптодоров от Алфа Куолити Интернешънъл. Сертификатът е официално и общовалидно признание за действаща и ефикасна система. Но това е само формалната страна на нещата. Ползите трябва да се търсят и в по-голяма дълбочина, не непременно свързани със самия сертификат. Най-общо казано фирмата, внедрила и поддържаща СУСИ, е по-спокойна за своя бизнес, а нейните клиенти също са спокойни и уверени, че няма да имат проблеми със сигурността, категоричен е Поптодоров. "Фирмите, внедрили и поддържащи СУСИ, се сдобиват с похвати и механизми,

които им позволяват да си държат сетивата отворени за възможни заплахи и да действат превантивно, за да не допускат рискове. И тъй като абсолютната сигурност не може да бъде достигната, тези фирми, спазвайки изискванията на стандарта, се учат да реагират правилно на събития и инциденти по сигурността, като при всеки един случай те се "измъкват" с въвеждане на нови подходи и подобрени защити. Иначе казано – колкото повече е заплашвана една такава фирма, толкова тя става по-резистентна и сигурна", поясни Поптодоров.

Положителни прогнози

И двата стандарта - ISO/IEC 27001:2005 и ISO/IEC 20000-1:2005, са сравнително нови за България и е нормално интересът към тях да расте. Привлекателни са с тяхната значително по-тясна насоченост към определени браншове и видове организации, смята Даниел Неделчев от LRQA. Голяма част от фирмите поради естествената по-ниска натовареност на персонала в кризата видяха добра перспектива и време за сертификация и обучение на персонала, посочи Неделчев. От LRQA виждат перспективите за развитие на пазара в създаването на интегрирани системи по приложимите за фирмата стандарти, което оптимизира документацията на фирмата, снижава разходите за сертификация и подобрява връзките между изисквания на нормативната база, фирмената практика и постоянно нарастващите изисквания на клиентите и обществото. Определено може да се каже, че търсенето на такъв тип сертификации (ISO 27001:2005 и ISO 20000-1:2005) расте – само за година и половина броят на сертифицираните компании в България се е увеличил двойно, посочи и Стоян Жеков от SGS България. Иван Савов от Муди Интернешънъл България обясни, че кризата се отразява на пазара на обучения и сертификация, но въпреки това бизнесът все повече осъзнава важността на СУСИ и ценността на информацията. Загубата или неправилното и неоторизирано използване могат да причинят щети за милиони във всяка организация и в някои случаи дори да доведат компанията до фалит, допълни Савов. Търсенето на сертификати по управленски стандарти расте най-вече под натиска на изискванията в тръжната документация по обществени поръчки, убеден е Юлиан Узунов от Top Management Advisors. Според него ISO/IEC 27001 има отлично бъдеще, особено ако по стандарта се работи професионално. За съжаление, повечето управленски стандарти са компрометирани от некомпетентни консултанти, от комерсиализирани сертифициращи органи и от злоупотребите със стандартите при обществените поръчки, смята Узунов.

Перспективите пред сектора на обучения и сертификация са много добри, заключи и инж. Бончо Поптодоров от Алфа Куолити Интернешънъл. Прогнозите му са базирани и по общото развитие на тези услуги в световен мащаб. "Търсенето у нас расте, макар и не толкова бързо", посочи той.