ЕВРОПЕЙСКИ СЪЮЗ
Европейски фонд
за регионално развитие
Инвестираме във вашето бъдеще

НАЦИОНАЛНА
СТРАТЕГИЧЕСКА
РЕФЕРЕНТНА РАМКА
2007 – 2013

ОПЕРАТИВНА ПРОГРАМА
„Развитие на конкурентоспособността
на българската икономика“ 2007-2013
www.opcompetitiveness.bg

СТАНДАРТИ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

БЪЛГАРСКИ
ИНСТИТУТ ЗА
СТАНДАРТИЗАЦИЯ

ПРОЕКТ: № BG 161PO003-4.3.01-0003-C0001

„УСЪВЪРШЕНСТВАНЕ НА СИСТЕМАТА ЗА СТАНДАРТИЗАЦИЯ В БЪЛГАРИЯ“

СЪДЪРЖАНИЕ

Този документ е създаден с финансовата подкрепа на Оперативна програма „Развитие на конкурентоспособността на българската икономика“ 2007–2013, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие. Цялата отговорност за съдържанието на документа се носи от Българския институт за стандартизация и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз или Министерство на икономиката, енергетиката и туризма.

Брошурата е издадена през януари 2013 г.

УНИВЕРСАЛНИЯТ ЕЗИК НА СТАНДАРТИТЕ

Стандартите са универсалният език, на който говорим всички. Език, необходим на производители, потребители, учени, доставчици, държавни власти и неправителствени организации навсякъде по света.
Почти няма област, в която стандартите са безмълвни, защото те способстват за нашата сигурност, безопасност и бъдеще.

Новите информационни технологии доведоха до бързи промени в начина на живот. Информацията е изключително ценна, а нуждата от управление на огромно количество данни и тяхната защита е очевадна. И тук на помощ идват стандартите, тъй като универсалният им език:

- улеснява общуването между икономическите партньори – производителите, потребителите и официалните власти;
- подпомага законодателството при създаването и изпълнението на нормативни актове;
- служи за основа при оценяване на съответствието;
- служи при договаряне по отношение на технически изисквания и предписания;
- насърчава иновациите и инвестициите;
- предлага решения за по-ефикасно използване на ресурсите;
- поддържа минимално ниво на качество;
- осигурява съвместимост и намалява многообразието.

Новите технологии, както и стандартите, на практика заличават географските, икономическите и културните граници на планетата.

Думата „стандарт“ се използва за всичко – от храната в чинията до информационните технологии. Наистина, стандартите са навсякъде, но те не са кухи думи. Това са документи, които определят правила, указания и характеристики за обща и многократна употреба.
Мнозина бъркат стандарт и нормативен акт. Нормативният акт се разработва и одобрява от държавен орган, докато стандартът е дело на всички – производители, доставчици, учени, потребители.
Прилагането на стандарта е доброволно, а на нормативния акт – задължително. Но когато стандартът е позован в нормативен акт или договор, става задължителен.

Езикът на стандартите е универсален, защото е и независим. Заповедният тон, с който се налагаха както стандарти, така и информация, вече е немислим. Новите реалности изключват командно-административния подход в стандартизацията. Стандартите не са механизъм за държавен контрол, а важен елемент на пазарната икономика.

Доказателство за универсалния език на стандартите е Обединена Европа. Европейските стандарти се изработват с консенсус и отразяват икономическите и социалните интереси на всички държави членки. Свободното движение на стоки и услуги е една от основните свободи на Европейския съюз. Един европейски стандарт заменя 33 различни национални стандарти и създава достъп до пазара на над 600 милиона потребители.

КАК СЕ УПРАВЛЯВАТ УСЛУГИТЕ ПРИ ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ

Организацията трябва да идентифицира и управлява множество свързани една с друга дейности, за да може да функционира ефикасно. **БДС ISO/IEC 20000-1 Информационни технологии. Управление на услуги. Част 1: Изисквания относно системата за управление на услуги** помага за възприемане на интегриран процесен подход за ефикасно предоставяне на управлявани услуги в отговор на изискванията на бизнеса и потребителите.
Стандартът посочва, че е необходим план, който включва:

- определяне на фондове и бюджети;
- разпределяне на роли и отговорности;
- документиране и поддържане на политики, планове, процедури и дефиниции за всеки процес или набор от процеси;
- определяне и управление на рисковете за услугата;
- управление на екипите, например наемане и обучение на подходящ персонал и управление приемствеността между служителите;
- управление на средствата и бюджета;
- управление на екипите, включително тези за поддържане и експлоатация;
- докладване на изпълнението на плановете и
- координиране на процесите, свързани с управление на услугата.

Необходима е политика за подобряване на услугата и всяко несъответствие със стандарта или с плановете трябва да бъде коригирано. Изискванията за непрекъснатост и наличност на услугата се определят на основата на бизнес планове, споразумения за ниво на услугата и оценки на риска. Необходими са политика за информационна сигурност и документирани механизми за контрол.

Трябва да има приети процедури за управление на въздействието от инциденти. Те определят начина на записване, задаване на приоритет, класифициране, обновяване, предвижване по йерархията, окончателно решение и официално приключване на всички дейности за разрешаване на инциденти. Клиентът трябва да бъде информиран за напредъка на докладвания от него инцидент или заявка за услуга, и предупреден предварително, ако нивото на услугата не може да бъде постигнато и да бъдат договорени някакви действие. Трябва да се записват и всички индентифицирани проблеми.

Необходим е интегриран подход при планиране на управлението на промени и конфигурации. Трябва да има политика за това, какво е определено като елемент на конфигурация и съставящите го компоненти.
Управлението на конфигурациите осигурява механизми за определяне, контрол и проследяване на версиите на набелязаните компоненти на услугата и инфраструктурата. Необходимо е да се гарантира, че степента на контрол е достатъчна, за да отговори на потребностите на бизнеса, риска от провал и критичността на услугата.
Промени в елементите на конфигурация трябва, където е уместно, да бъдат проследими и да може да бъдат одитирани, например при промени и преместване на софтуер и хардуер.
Процедурите за контрол на конфигурациите трябва да гарантират запазване целостта на системите, услугите и техните компоненти. Преди пускане в експлоатация се прави описание на първоначалното състояние на подходящите елементи на конфигурацията.
Оригиналните копия на елементите за цифрово конфигуриране трябва да са контролирани, в защитени физически или електронни библиотеки, и свързани със записите за конфигуриране, например софтуер, проддукти за изпитване, поддържащи документи.
Всички елементи на конфигурация са уникално идентифицирани и записани в база данни, до която достъпът е стриктно контролиран. Състоянието на елементите на конфигурация, техните версии, местоположение, свързаните с тях промени и проблеми, както и съответната документация трябва да бъдат видими за тези, които я изискват.
Процедурите за одитиране на конфигурациите включват записване на недостатъци, предизвикване на коригиращи действия и докладване на резултатите.

Промените в услуги и инфраструктура трябва да имат ясно определен и документиран обхват. Всички заявки за промени се записват и класифицират, например като спешни, извънредни, основни и второстепенни. При искания за промени трябва да се извърши оценяване на риска, въздействието и ползата за конкретната организация. Промените трябва да бъдат одобрени, проверени и въведени по контролиран начин.

Процесът на управление на пускането в действие трябва да бъде интегриран в процесите за управление на промените и конфигурациите. Политиката за пускане в действие, в която се заявяват честотата и видът на пусканите в действие нови версии, трябва да бъде документирана и договорена.
Пускането в действие и разпространението трябва да бъдат разработени и внедрени, така че целостта на хардуера и софтуера да се запази по време на инсталирането, обработката, пакетирането и доставката.
Успехът и неуспехът на новите версии се измерват и е необходим анализ, който включва оценка на въздействието върху бизнеса, работата на IT и ресурсите на персонала.

СТАНДАРТЪТ, КОЙТО ПОКАЗВА ДОБРА ПРАКТИКА

При увеличаващата се зависимост от поддържащи услуги и при разнообразния обхват от достъпни технологии, доставчиците на услуги трябва да положат усилия, за да поддържат високо ниво на обслужване на клиентите. Ако само реагират, те изразходват твърде малко време за планиране, обучение, преглеждане, изследване и работа с клиентите.
БДС ISO/IEC 20000-2 Информационни технологии. Управление на услуги. Кодекс за добра практика показва как се предоставят качествени IT услуги. Разработен е под формата на ръководство, съдържа препоръки и трябва да се използва заедно с БДС ISO/IEC 20000-1.

Стандартът посочва как трябва да се извършват планирането и внедряването на управлението на услугите. Определени са обхватът, подходите при планиране, както и какво да включва планът за управление на услугата. Посочени са събитията, които трябва да се вземат под внимание, например промени в нормативни актове, регулаторни промени, обединяване и сливане и др.

Каталогът на услугата определя всички услуги. Той се поддържа и актуализира, тъй като е основен документ, в който са отразени очакванията на клиента.
Услугата официално се документира в споразумение за ниво на услугата, което е одобрено от висши представители на клиента и на доставчика. Определящи за съдържанието, структурата и целите на споразумението са специфичните потребности на клиента и неговият бюджет. Минималното съдържание включва кратко описание на услугата, период на валидност, детайли за одобрение, кратко описание на комуникирането, включително отчитане; също и данни за контакт на лица, упълномощени да действат в спешни случаи, да участват при разрешаване на възникнали конфликтни ситуации и проблеми, възстановяване или вземане на временни решения. Включва се работно време, планирани и договорени прекъсвания, отговорностите на клиента и доставчика и други.

Процесът за управление на нивото на услугата трябва да бъде гъвкав, за да се отразят в него промени като нарастване, реорганизиране и сливания, промяната в изискванията на клиента. Удовлетвореността на клиента е важна част от управлението на нивото на услугата, но това трябва да се оцени като субективен фактор, докато целите трябва да имат обективно измерими критерии.

Стандартът посочва как се отчита услугата. Когато има много доставчици, главни доставчици и подизпълнители, докладите отразяват взаимоотношенията между тях. Посочени са видовете доклади и как се съставят.

Изискванията за непрекъснатост и наличност на услугата се установяват на основата на бизнес приоритетите на клиентите, споразумението за ниво на услугата и оценените рискове. Доставчикът планира повишаването или понижаването на обемите данни и потребители, очакваните пикове и спадове в работното натоварване и всякакви други бъдещи промени. Стратегията за непрекъснатост се преразглежда най-малко веднъж годишно.

Стандартът посочва как трябва да се формират и отчитат разходите, свързани с предоставянето на IT услуги.
Доставчикът поддържа опис на информационните активи, като всеки се класифицира според неговата значимост и нивото на защита, от което той се нуждае. Определя се собственик, който отговаря за осигуряване на тази защита. Посочено е как да се оценяват рисковете, свързани с информационните активи, и на какво да се обърне внимание. Определени са и механизмите за контрол, а също какви да бъдат документите и записите, тъй като системата за управление на сигурността на информацията трябва да бъде надеждно документирана.

Доставчикът и клиентът извършват преглед на услугата най-малко веднъж годишно, както преди и след основни промени. Стандартът посочва какво трябва да съдържа процеса за управление на договорите, как се разрешават споровете, как се поставят приоритети и определя график за разрешаването на инциденти и проблеми.

В стандарта е определено как се управлява конфигурация. Всички основни активи и конфигурации се вземат под внимание и имат определен отговорник, който осигурява поддържането на подходяща защита и контрол.
Всички елементи на конфигурацията трябва да бъдат еднозначно идентифицирани и определени чрез атрибути, които описват техните функционални и физични характеристики. Информацията трябва да бъде актуална и подлежаща на одит.
Контролът трябва да осигури, че само оторизирани и идентифицируеми елементи на конфигурацията са приети и записани от приемането им до ликвидирането им.
Поддържат се текущи и точни записи на конфигурацията, които отразяват промените в статута, местоположението и версията ѝ.
В стандарта е посочено какво включва верификация на конфигурацията и одит. Публикации на информационни системи и софтуер от вътрешни екипи, от изграждащи системи, системни интегратори или от други организации трябва да се верифицират при получаване.

Процесите на разгръщане, разпространение и инсталиране трябва да гарантират, че:
- всички места за съхранение на софтуер и хардуер са сигурни;
- има налични подходящи процедури за съхранение, изпращане, приемане и унищожаване на продуктите;
- планирани са и са извършени проверки на инсталацията, околната среда, електрически проверки и проверки на съоръженията;
- персоналът на организацията и на доставчика на услуги е уведомен за нови пускания;

След разпространяване на софтуер през мрежа е необходимо да се провери дали пускането е цялостно и работоспособно, когато достигне местоназначението си.
След успешно инсталиране записите за активите и за управлението на конфигурацията трябва да бъдат обновени чрез местоположението и собственика на хардуера и софтуера.
Може да бъде използван въпросник за приемане и за удовлетвореност на клиентите, за да се отбележи успехът или неуспехът. Резултатите от всяко проучване на клиентите трябва да се използват при управлението на бизнес взаимоотношенията.

СТАНДАРТИТЕ И СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Новите информационни технологии доведоха до бързи промени в начина на живот. Информацията е изключително ценна, а необходимостта от управление на огромно количество данни и тяхната защита е очевидна.

Информацията и свързаните с нея процеси, системи и мрежи представляват критични бизнес активи. Организациите и техните информационни системи и мрежи са изправени пред многобройни заплахи за сигурността, включително измами, шпионаж, саботаж, вандализъм, пожари и наводнения. Компютърните пробиви и атаки стават по-чести, по-смели и по-сложни. И тук на помощ идват стандартите от серията за системи за управление на сигурността на информацията.

Терминът „сигурност на информацията“ се отнася главно за информация, определена като актив, който има стойност, и изисква съответстваща защита – например от загуба на наличност или по отношение на конфиденциалност и интегритет (цялостност).

Системата за управление на сигурността на информацията (СУСИ) предоставя модел за създаване, внедряване, функциониране, наблюдение, преглед, поддържане и подобряване на защитата на информационни активи.

Принципи

- осъзнаване на необходимостта от сигурност на информацията;
- определяне на отговорностите по отношение на сигурността на информацията;
- ангажимент на ръководството и интерес у заинтересованите страни;
- повишаване на обществената значимост;
- оценяване на риска и установяване на подходящи механизми за контрол за постигане на приемливи нива;
- сигурност, включена като основен елемент на информационни мрежи и системи;
- активна превенция и разкриване на инциденти, свързани със сигурността на информацията;
- осигуряване на всестранен подход за управление на сигурността на информацията;
- непрекъснато повторно оценяване на сигурността на информацията и реализиране на изменения, ако е уместно.

Процесният подход, представен в стандартите от серията за СУСИ, се основава на принципа, възприет от стандартите за системи за управление на ISO, известен като планиране – изпълнение – проверка – действие – ПИПД (Plan – Do –Check – Act).

- Планиране – определяне на целите и разработване на планове (анализиране на ситуацията в организацията, установяване на общите цели и желаните резултати и разработване на планове).
- Изпълнение – осъществяване на плановете (извършване на планираните действия).
- Проверка – измерване на резултатите (измерване/наблюдение на степента, до която постиженията отговарят на планираните цели).
- Действие – действия за коригиране и подобряване (поуки от грешките за подобряване на дейностите с цел постигане на по-добри резултати).

ЗАЩО Е ВАЖНА СИСТЕМАТА ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Разработването и внедряването на система за управление на сигурността на информацията зависи от потребностите и целите на организацията, изискванията за сигурност, използваните за дейността процеси, големината и структурата на самата организация. Разработването и функционирането на системата трябва да отговарят на интересите и изискванията за сигурност на информацията на всички заинтересовани страни, включително клиенти, доставчици, бизнес партньори, акционери и други свързани страни.

Системата за управление на сигурността на информацията е важна както за бизнеса, така и за обществения сектор.

Сигурността на информацията невинаги се взема предвид при проектирането и разработването на информационните системи и често се схваща като техническо решение. Интегрирането на сигурност в дадена информационна система постфактум може да бъде трудно и скъпо.

При създаване, наблюдение, поддържане и подобряване на системата всяка организация трябва да следва дадените по-долу етапи:

- идентифициране на информационните активи и свързаните с тях изисквания,
- оценяване на рисковете по отношение сигурността на информацията,
- избор и внедряване на приложими механизми за контрол за неприемливите рискове,
- наблюдение, поддържане и подобряване на ефикасността на механизмите за контрол на сигурността, свързани с информационните активи на организацията.

Тези етапи трябва да бъдат непрекъснато повтаряни, за да се идентифицират промени в рисковете, в стратегията или целите на организацията.

Ползи

- подпомага процеса на определяне, внедряване, функциониране и поддържане на всеобхватна и разходо-ефективна интегрирана и съгласувана система, която отговаря на потребностите на организацията по отношение на различните дейности и местоположения;
- подпомага ръководството при структуриране на неговия подход, свързан с управлението на сигурността на информацията;
- популяризира общопризнати добри практики, давайки на организациите свобода на действие за възприемане и подобряване на приложимите механизми за контрол, които съответстват на техните специфични условия,
- осигурява общ език и концептуална основа за сигурността на информацията, чрез което се улеснява създаването на пълно доверие у бизнес партньорите в съответната система, и най-вече ако партньорите изискват сертификация за съответствие с ISO/IEC 27001 от акредитиран орган за сертификация.

Стандартите от серията за системи за управление на сигурността на информацията са под общото наименование **Информационни технологии. Методи за сигурност** и са изброени по-долу

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

БДС ISO/IEC 27001 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания

БДС ISO/IEC 27002 Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията

БДС ISO/IEC 27003 Информационни технологии. Методи за сигурност. Указания за внедряване на система за управление на сигурността на информацията

БДС ISO/IEC 27004 Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Измерване

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

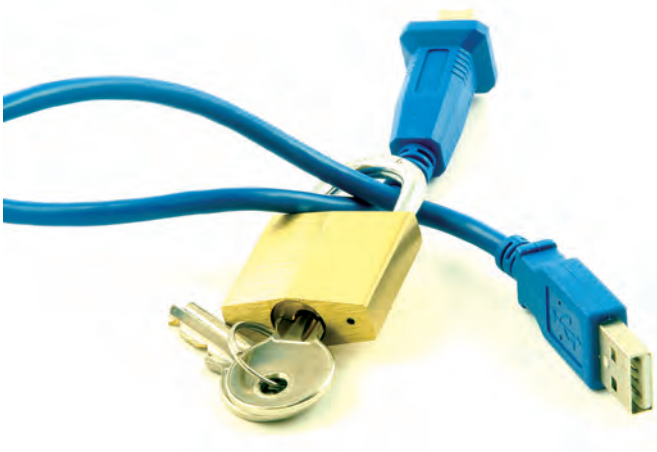
БДС ISO/IEC 27006 Информационни технологии. Методи за сигурност. Изисквания за органите, извършващи одит и сертификация на системи за управление на сигурността на информацията

ISO/IEC 27007 Информационни технологии. Методи за сигурност. Указания за одит на системите за управление на сигурността на информацията

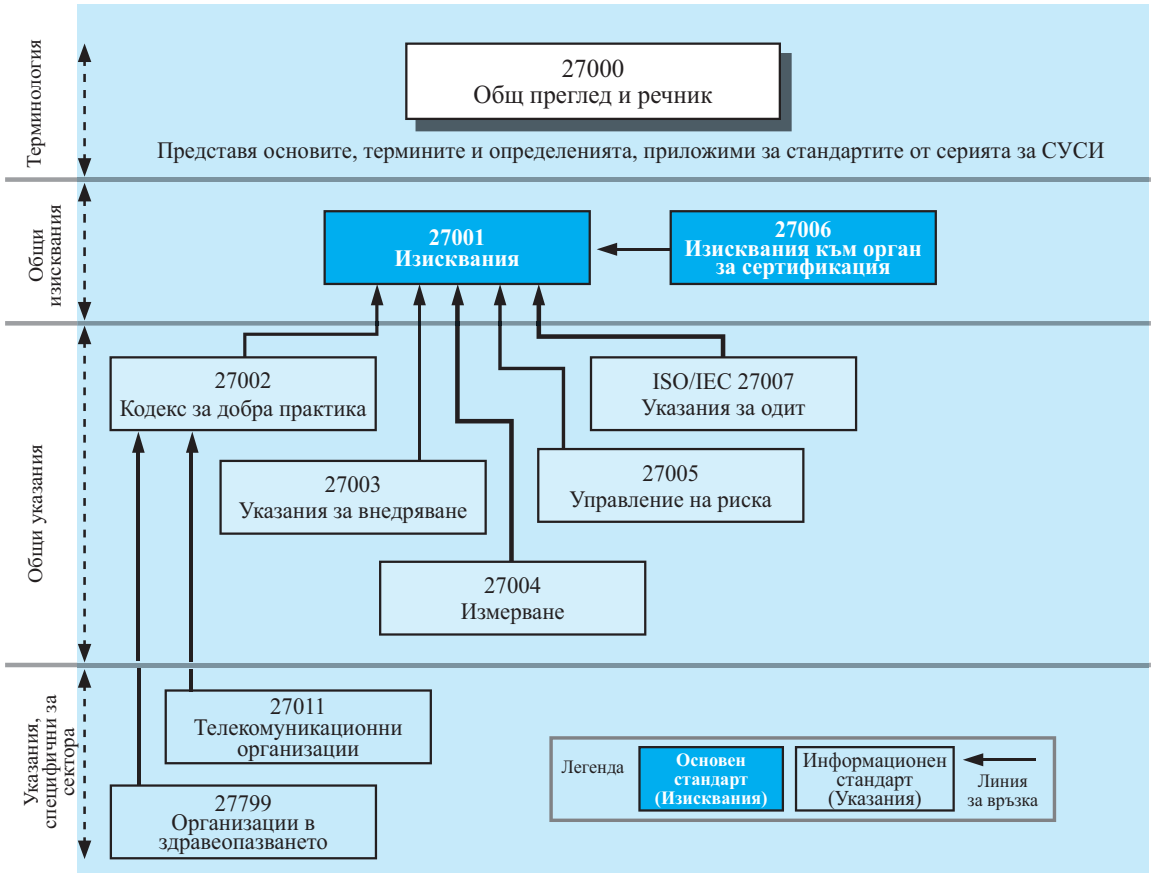
ISO/IEC TR 27008 Информационни технологии. Методи за сигурност. Указания за одитори, свързани с механизмите за контрол на сигурността на информацията

БДС ISO/IEC 27011 Информационни технологии. Методи за сигурност. Указания за управление на сигурността на информацията за телекомуникационни организации, базирани на ISO/IEC 27002

БДС ISO/IEC 27799 Информатика в здравеопазването. Управление на сигурността на информацията в здравеопазването на основата на ISO/IEC 27002



Взаимовръзката между стандартите от серията за СУСИ е показана на следната фигура.



Стандартите от серията за СУСИ са в тясна връзка с много други стандарти на ISO и ISO/IEC.

СТАНДАРТИ ОТ СЕРИЯТА ЗА СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Речник: БДС ISO/IEC 27000

БДС ISO/IEC 27000 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник описва основните принципи на системите за управление на сигурността на информацията и дефинира свързаните с тях термини.

Под „сигурност на информацията" се разбира опазване на поверителността, интегритета (целостта) и наличността на информацията. Могат също да се включат и други свойства, като автентичност, отчетност, неотхвърляемост и надеждност.
За да се отговори на променящия се статут на стандартите от серията за СУСИ, се очаква този стандарт да бъде непрекъснато осъвременяван – много по-често, отколкото е обичайната практика за останалите стандарти на ISO/IEC.

Изисквания: БДС ISO/IEC 27001

БДС ISO/IEC 27001 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания съдържа основни изисквания, които могат да бъдат прилагани във всички организации без значение от вида, големината и дейността им.
Той може да бъде използван за оценяване на съответствието от вътрешни и външни заинтересовани страни. Съобразен е с ISO 9001:2000 и ISO 14001:2004, за да се поддържа съвместимо и интегрирано внедряване и действие със системите за управление на качеството и по отношение на околната среда.

Кодекс за добра практика: БДС ISO/IEC 27002

БДС ISO/IEC 27002 Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията дава указания и общи принципи за внедряване, поддържане и подобряване на управлението на сигурността на информацията в дадена организация.
Стандартът съдържа списък с общоприети цели по контрола и най-добри практики за механизмите за контрол, които да бъдат използвани. Включва 11 точки, отнасящи се за контрол на риска и съдържащи общо 39 основни категории за сигурност.

Указания за внедряване: БДС ISO/IEC 27003

БДС ISO/IEC 27003 Информационни технологии. Методи за сигурност. Указания за внедряване на системи за управление на сигурността на информацията предоставя практически указания за разработване на план за внедряване на системата за управление на сигурността на информацията (СУСИ) в съответствие с ISO/IEC 27001:2005.
Той е приложим за всички видове организации независимо от тяхната големина и дейност.

Измерване: БДС ISO/IEC 27004

БДС ISO/IEC 27004 Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Измерване дава насоки и съвети за разработване и използване на измерители за оценяване на ефикасността на дадена СУСИ, целите по контрола и механизмите за контрол, използвани за внедряване и управление на сигурността на информацията, както е описано в ISO/IEC 27001.

Управление на риска: БДС ISO/IEC 27005

БДС ISO/IEC 27005 Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията предоставя указания за управление на риска за сигурността на информацията в дадена организация в подкрепа на изискванията за системата за управление на сигурността на информацията (СУСИ) съобразно ISO/IEC 27001. От организацията зависи как ще определи своя подход към управлението на риска съобразно обхвата на СУСИ, контекста на управлението на риска или сектора на индустрията.

Процесът може да бъде приложен към организацията като цяло, към нейна отделна част (например отдел, местоположение, дейност), към всяка информационна система или към специфични аспекти на контрол.

Изисквания за органите, извършващи одит и сертификация: БДС ISO/IEC 27006

БДС ISO/IEC 27006 Информационни технологии. Методи за сигурност. Изисквания за органите, извършващи одит и сертификация на системи за управление на сигурността на информацията определя изискванията и предоставя указания на органите за сертификация, извършващи одит и сертификация на системи за управление на сигурността на информацията (СУСИ), в допълнение на изискванията, съдържащи се в ISO/IEC 17021 и ISO/IEC 27001. Неговото основно предназначение е да подпомага акредитацията на органите за сертификация, извършващи сертификация на СУСИ.
Необходимо е всеки орган за сертификация да докаже компетентност и надеждност по отношение на изискванията, съдържащи се в този стандарт.

ДРУГИ СТАНДАРТИ

ISO/IEC 27007 ***Информационнитехнологии.Методизасигурност.Указаниязаодит на системите за управление на сигурността на информацията.*** Стандартът дава практически указания за извършването на одит на документирана система за управление на сигурността на информацията в контекста на основните рискове за дейността на организацията и внедрените стандарти от серията ISO/IEC 27000.

БДС ISO/IEC 27011 ***Информационни технологии. Указания за управление на сигурността на информацията за телекомуникационни организации, базирана на ISO/IEC 27002*** установява общите принципи за създаване, внедряване, експлоатация и усъвършенстване на управлението на сигурността на информацията в телекомуникационния сектор на основата на ISO/IEC 27002. В резултат от внедряването му организациите ще бъдат в състояние да осигурят конфиденциалност, интегритет и наличност на телекомуникационните съоръжения и услуги и ще възприемат защитни процеси и механизми за контрол, гарантиращи намаляване на рисковете при доставка на телекомуникационни услуги.

ISO/IEC 27799 ***Информатика в здравеопазването. Управление на сигурността на информацията в здравеопазването на основата на ISO/IEC 27002*** дава указания, съдействащи за внедряването на управлението на сигурността на информацията в здравните организации.

В резултат на въвеждането на стандартите от серията ISO/IEC 27000 организации от всякакъв вид и големина, навсякъде по света, ще гарантират на своите партньори и клиенти, че работят със защитени системи и се стремят да сведат до минимум риска, а оттам и разходите за възстановяване на работоспособността на системите и/или целостта на данните.

Повече информация може да бъде открита на http://www.iso.org/iso/iso_catalogue/ и на http://www.bds-bg.org

Къде да намерим необходимата информация за стандарти и специализирани издания на Българския институт за стандартизация?

Българският институт за стандартизация разполага с информационен център и библиотека с читалня.

Работно време: **понеделник – петък**

9.00–12.30
13.30–16.30
Тел. 02/ 81 74 582 – Библиотека
Тел. 02/ 81 74 523 – Информационен център

В Българския институт за стандартизация ще намерите информация за:

1. **Продажба на стандарти и специализирани издания**

За поръчка и закупуване на стандарти и специализирани издания на БИС можете да използвате един от следните начини:

- В Информационния център на БИС на адрес: гр. София, кв. „Изгрев“, ул. „Лъчезар Станчев“ № 13, библиотека стандарти
- По електронната поща: info@bds-bg.org,
- По факс: 02/873-55-97,
- Онлайн на нашата интернет страница на адрес: www.bds-bg.org
  Плащане – в касата на БИС, по банков път или чрез www.epay.bg

За получаване на поръчаните стандарти можете да изберете или доставка чрез куриер, получаване на място в БИС или он-лайн през интернет страницата на БИС.

2. **Подробни и допълнителни справки за стандарти – в информационния център на БИС:**

- библиографска справка,
- тематична справка в определена област,
- справка за актуалност за национални, европейски, международни и чуждестранни стандарти.

Тел: 02/ 81 74 523
E-mail: info@bds-bg.org

ДЕСЕТ ПРИЧИНИ ДА ИЗПОЛЗВАТЕ СТАНДАРТИТЕ

1. За да подобрите качеството на вашия продукт или услуга

Високото качество винаги е много силен аргумент при продажбата на даден продукт. Прилагането на стандарти подобрява качеството и увеличава продажбите на предлаганите продукти и услуги, а това е един от най-добрите начини да се задържат постоянните клиенти.

2. За да привлечете нови клиенти

Стандартите са най-ефективният начин да убедите потребителите, че вашият продукт отговаря на най-високите и разпространени изисквания за качество, безопасност и сигурност.

3. За да повишите конкурентоспособността си

Прилагането на стандарти затвърждава репутацията, че вашият бизнес преследва отлично качество. Това може да ви даде голямо предимство пред конкурентите, които не прилагат стандарти и дори може да привлечете техни клиенти.

4. За да затвърдите доверието във вашия бизнес

С въвеждането на стандарти ще увеличите доверието на клиентите към вашия продукт. Прилагането на определени стандарти, например свързани с опазването на околната среда, може да способства за доброто ви име в обществото.

5. За да намалите вероятността от грешки

Стандартите предоставят на бизнеса сигурна отправна точка, която намалява риска от грешки и недоразумения. Така няма да губите време и пари за разработване на продукти, които не отговарят на нужното качество и съответните изисквания. Освен загуба на пари грешките вредят и на вашата репутация.

6. За да намалите разходите

Прилагането на технически стандарт ще намали разходите за проучване и разработка и нуждата от създаване на вече съществуващи продукти. С въвеждане на стандарт за система за управление ще подобрите организацията на работа и ще направите бизнеса си много по-доходоносен.

7. За да бъдат вашите продукти конкурентни

Прилагането на технически стандарти гарантира, че вашите стоки и услуги са конкурентоспособни. Това е най-ефективният начин да се увеличи максимално вашият потенциален пазар и със сигурност е предимство при износа на продукти.

8. За съответствие със задължителните изисквания

Стандартите са доброволни и законово не сте задължени да ги прилагате. Това, че вашите продукти отговарят на определените изисквания, помага в случаите, когато те трябва да съответстват и на задължителни нормативни разпоредби, свързани с безопасността на продуктите и опазването на околната среда. Вашата продукция няма да може да се продава на някои пазари, ако тя не отговаря на определени критерии за качество и безопасност. Прилагането на стандарти спестява време, усилия, разходи и дава увереност, че спазвате задълженията си.

9. За да улесните износа на вашите продукти

Много стоки трябва да отговарят на спецификациите, определени от Директивите на ЕС, за да могат да се продават на Общия европейски пазар. Такива продукти обикновено трябва да носят маркировка CE. Ако постигнете това, ще можете да продавате стоките си в държави – членки на ЕС.

10. За да увеличите шансовете си за успех

Включването на стандартите като част от вашата маркетингова стратегия ще даде много по-голям шанс за успех на вашия продукт. Прилагането на стандарти увеличава шансовете ви за успех на пазари, където те се изискват.