Април 2014

БЪЛГАРСКИ ИНСТИТУТ ЗА СТАНДАРТИЗАЦИЯ	**БЪЛГАРСКИ СТАНДАРТ**	**БДС**
	ИНФОРМАЦИОННИ ТЕХНОЛОГИИ **МЕТОДИ ЗА СИГУРНОСТ** **СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА** **ИЗИСКВАНИЯ**	**ISO/IEC 27001**

ICS 35.040

Заменя БДС ISO/IEC 27001:2006

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Този стандарт е официално издание на български език на международния стандарт ISO/IEC 27001:2013.

Преводът е направен от Българския институт за стандартизация.

БДС ISO/IEC 27001:2014 е идентичен на английската версия на международния стандарт ISO/IEC 27001:2013.

Този български стандарт е одобрен от изпълнителния директор на Българския институт за стандартизация на 2014-04-30.

Национални стр. 2
и 28 стр. на ISO/IEC

Национален № за позоваване БДС ISO/IEC 27001:2014

НАЦИОНАЛЕН ПРЕДГОВОР

Този стандарт е подготвен с участието на БИС/ТК 57 "Информационни и комуникационни технологии".

Този стандарт заменя и отменя БДС ISO/IEC 27001:2006.

В стандарта е направено позоваване на международни/европейски стандарти и документи, на които съответстват следните български стандарти:

- на ISO/IEC 27000	- БДС ISO/IEC 27000

Следват 28 страници на ISO/IEC 27001:2013 в превод на български език.

СЪДЪРЖАНИЕ

ПРЕДГОВОР

ISO (Международната организация за стандартизация) и IEC (Международната електротехническа комисия) представляват специализирана система за световна стандартизация. Националните органи, които са членове на ISO или IEC, участват в разработването на международни стандарти чрез технически комитети, създадени от съответната организация за отделни области на техническата дейност. Техническите комитети на ISO и IEC си сътрудничат в области от взаимен интерес. В работата участват също така и други международни организации, правителствени и неправителствени, свързани с ISO и IEC. В областта на информационните технологии ISO и IEC създадоха обединен технически комитет ISO/IEC JTC 1.

Международните стандарти се разработват в съответствие с правилата, дадени в директивите на ISO/IEC, част 2.

Основна задача на обединения технически комитет е да разработва международни стандарти. Проектите на международни стандарти, приети от обединения технически комитет, се разпращат до националните органи за гласуване. Публикуването на международен стандарт изисква одобрението най-малко на 75 % от участвалите в гласуването национални органи.

Обръща се внимание на възможността някои от елементите на този документ да бъдат обект на права на интелектуална собственост или подобни права. ISO и IEC не носят отговорност при идентифицирането на някои или всички подобни права.

ISO/IEC 27000 подготвен от обединения технически комитет ISO/IEC JTC 1 *Information technology [Информационни технологии],* подкомитет SC 27 *IT Security techniques [Методи за сигурност на информационните технологии].*

Това второ издание отменя и заменя първото издание (ISO/IEC 27001:2005), което е технически преработено.

0 Въведение

0.1 Общи положения

Този международен стандарт е разработен, за да осигури изисквания за създаване, осъществяване, поддържане и непрекъснато подобряване на система за управление на сигурността на информацията. Възприемането на система за управление на сигурността на информацията е стратегическо решение за една организация. Създаването и внедряването на система за управление на сигурността на информацията на една организация зависят от нейните потребности и цели, от изискванията по отношение на сигурността, от използваните организационни процеси и от големината и структурата на организацията. Очаква се всички тези влияещи фактори да се променят с течение на времето.

Системата за управление на сигурността на информацията запазва поверителността, цялостността и наличността на информацията чрез прилагане на процес за управление на риска и дава увереност на заинтересуваните страни, че рисковете се управляват по подходящ начин.

Важно е системата за управление на сигурността на информацията да бъде част и да е интегрирана с процесите и цялостната управленска структура на организацията и сигурността на информацията да се взема под внимание при разработването на процесите, информационните системи и механизмите за контрол. Очаква се, че реализацията на система за управление на сигурността на информацията ще бъде в размера, който е в съответствие с нуждите на организацията.

Този международен стандарт може да бъде използван от вътрешни и външни страни за оценяване на способността на организацията да отговори на своите собствени изисквания към сигурността на информацията.

Редът, по който са представени изискванията в този международен стандарт, не отразява тяхната важност или не определя реда, в който те трябва да бъдат реализирани. Точките в списъците са номерирани само с цел позоваване.

ISO/IEC 27000 представя общ преглед и терминологията на системите за управление на сигурността на информацията, като се позовава на поредицата от стандарти за системи за управление на сигурността на информацията (включително ISO/IEC 27003 [2], ISO/IEC 27004 [3] и ISO/IEC 27005 [4]), заедно с имащите отношение термини и определения.

0.2 Съвместимост с други стандарти за системи за управление

Този международен стандарт прилага структура от високо ниво, идентични заглавия на подточките, идентичен текст, общи термини и основни определения, определени в приложение SL на Директиви на ISO/IEC, част 1, обединено допълнение на ISO (Annex SL of ISO/IEC Directives, Part 1, Consolidated ISO Supplement) и следователно е съвместим с други стандарти за системи за управление, които са възприели приложението SL.

Този общ подход, определен в приложение SL, е полезен за организациите, избрали да прилагат една единствена система за управление, която отговаря на изискванията на два или повече стандарта за системи за управление.

ИНФОРМАЦИОННИ ТЕХНОЛОГИИ
МЕТОДИ ЗА СИГУРНОСТ
СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА
ИЗИСКВАНИЯ

1 Обект и област на приложение

Този международен стандарт определя изискванията за създаване, внедряване, поддържане и непрекъснато подобряване на системата за управление на сигурността на информацията в контекста на организацията. Този международен стандарт включва също изисквания за оценяване и въздействие върху рисковете за сигурността на информацията, съобразени с потребностите на организацията. Поставените в този международен стандарт изисквания са общи и са предназначени за прилагане от всички организации, независимо от вида, размера или естеството им. Изключването на което и да е изискване, посочено в точки от 4 до 10, е неприемливо, когато организацията декларира съответствие с този международен стандарт.

2 Позоваване

Следните документи, изцяло или частично, са нормативно позовани в този документ и са необходими за неговото прилагане. За датираните позовавания е приложимо само цитираното издание. За недатирани позовавания се прилага последното издание на посочения документ (включително и измененията).

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

3 Термини и определения

За целите на този документ се прилагат термините и определенията, дадени в ISO/IEC 27000.

4 Контекст на организацията

4.1 Разбиране на организацията и нейния контекст

Организацията трябва да определи външните и вътрешните въпроси, които са свързани с нейната цел и които влияят на нейната способност да постигне желания(те) резултат(и) от системата за управление на сигурността на информацията.

ЗАБЕЛЕЖКА: Определянето на тези въпроси се отнася за установяване на външния и вътрешния контекст на организацията, разгледани в 5.3 на ISO 31000:2009 [5].

4.2 Разбиране на нуждите и очакванията на заинтересуваните страни

Организацията трябва да определи:

a) заинтересуваните страни, които имат отношение към системата за управление на сигурността на информацията, и

b) изискванията на тези заинтересувани страни по отношение на сигурността на информацията.

ЗАБЕЛЕЖКА: Изискванията на заинтересуваните страни може да включват законови и нормативни изисквания и договорни задължения.

4.3 Определяне на обхвата на системата за управление на сигурността на информацията

За да установи нейния обхват, организацията трябва да определи границите и приложимостта на системата за управление на сигурността на информацията.

При определяне на този обхват организацията трябва да вземе под внимание:

a) външните и вътрешните въпроси, посочени в 4.1;

b) изискванията, посочени в 4.2, и

c) интерфейсите и зависимостите между дейностите, изпълнявани от организацията и тези, които се изпълняват от други организации.

Обхватът трябва да бъде на разположение като документирана информация.

4.4 Система за управление на сигурността на информацията

Организацията трябва да създаде, внедри, поддържа и непрекъснато да подобрява система за управление на сигурността на информацията в съответствие с изискванията на този международен стандарт.

5.Лидерство

5.1 Лидерство и ангажираност

Висшето ръководство трябва да демонстрира лидерство и ангажираност по отношение на системата за управление на сигурността на информацията чрез:

a) гарантиране, че политиката за сигурност на информацията и целите за сигурност на информацията са установени и са съвместими със стратегическата насока на организацията;

b) гарантиране, че изискванията на системата за управление на сигурността на информацията са интегрирани в процесите на организацията;

c) гарантиране, че необходимите ресурси за системата за управление на сигурността на информацията са налични;

d) разгласяване на важността от ефикасно управление на сигурността на информацията и от съобразяване с изискванията на системата за управление на сигурността на информацията;

e) гарантиране, че системата за управление на сигурността на информацията постига своя(ите) предвиден(и) резултат(и);

f) насочване и подкрепа на служителите да допринасят за ефикасността на системата за управление на сигурността на информацията;

g) съдействие за непрекъснато подобряване и

h) подкрепяне на други свързани управленски роли за демонстриране на тяхното лидерство, доколкото то е приложимо в техните области на отговорност.

5.2 Политика

Висшето ръководство трябва да създаде политика по сигурност на информацията, която:

a) е подходяща за целта на организацията;

b) включва цели за сигурност на информацията (виж 6.2) или осигурява рамката за поставяне на цели за сигурност на информацията;

c) включва ангажираност за изпълняване на приложимите изисквания, свързани със сигурността на информацията; и

d) включва ангажираност за непрекъснато подобряване на системата за управление на сигурността на информацията.

Политиката по сигурността на информацията трябва:

e) да бъде на разположение като документирана информация;

f) да бъде разгласена в рамките на организацията и

g) да бъде на разположение за заинтересуваните страни, когато е подходящо.

5.3 Организационни роли, отговорности и пълномощия

Висшето ръководство трябва да гарантира, че са разпределени и оповестени отговорностите и пълномощията на ролите, свързани със сигурността на информацията.

Висшето ръководство трябва да разпредели отговорността и пълномощията за:

a) гарантиране, че системата за управление на сигурността на информацията съответства на изискванията на този международен стандарт;и

b) докладване относно действието на системата за управление на сигурността на информацията пред висшето ръководство.

ЗАБЕЛЕЖКА: Висшето ръководство може също да разпредели отговорности и пълномощия за докладване относно действието на системата за управление на сигурността на информацията в рамките на организацията.

6 Планиране

6.1 Действия за справяне с рискове и възможности

6.1.1 Общи положения

Когато планира системата за управление на сигурността на информацията, организацията трябва да вземе под внимание въпросите, посочени в 4.1, и изискванията, посочени в 4.2, и да определи рисковете и възможностите, които трябва да бъдат отчетени, за да се:

a) гарантира, че системата за управление на сигурността на информацията може да постигне желаните резултати;

b) предотвратят или намалят нежеланите ефекти и

c) постигне непрекъснато подобряване.

Организацията трябва да планира:

d) действия за отчитане на тези рискове и възможности и

e) как да

1) интегрира и реализира действията в процесите на своята система за управление на сигурността на информацията и

2) оцени ефикасността на тези действия.

6.1.2 Оценяване на риска за сигурността на информацията

Организацията трябва да определи и приложи процес за оценяване на риска за сигурността на информацията, който:

a) установява и поддържа критерии за риска за сигурността на информацията, които включват:

1) критерии за приемане на риска; и

2) критерии за оценяване на риска за сигурността на информацията;

b) гарантира, че повторните оценявания на риска за сигурността на информацията дават последователни, действителни и сравними резултати;

c) идентифицира рисковете за сигурността на информацията:

1) прилага процеса за оценяване на риска за сигурността на информацията, за да идентифицира рискове, свързани със загуба на поверителност, цялостност и наличност за информация в обхвата на системата за управление на сигурността на информацията, и

2) идентифицира собствениците на риск;

d) анализира рисковете за сигурността на информацията:

1) оценява потенциалните последствия, които произтичат от осъществяване на рисковете, идентифицирани в 6.1.2 c);

2) оценява реалната възможност рисковете, идентифицирани в 6.1.2 c) 1), да се случат и

3) определя нивата на риск;

e) оценява рисковете за сигурността на информацията:

1) сравнява резултатите от анализа на риска с критериите за риск, установени в 6.1.2 a), и

2) определя приоритети за анализираните рискове с оглед въздействие върху риска.

Организацията трябва да съхранява документирана информация относно процеса за оценяване на риска за сигурността на информацията.

6.1.3 Въздействие върху риска за сигурността на информацията

Организацията трябва да определи и прилага процес за въздействие върху риска за сигурността на информацията, за да:

a) избере подходящи опции за въздействие върху риска за сигурността на информацията, като се вземат под внимание резултатите от оценяването на риска;
b) определи всички механизми за контрол, които са необходими за реализиране на избраната(ите) опция(и) за въздействие върху риска за сигурността на информацията;

ЗАБЕЛЕЖКА: Организациите може да разработят изискваните механизми за контрол или да ги идентифицират от произволен източник.

c) сравни механизмите за контрол, определени в 6.1.3 b) по-горе, с тези от приложение A и да провери, че не е пропуснат никой от необходимите механизми за контрол;

ЗАБЕЛЕЖКА 1: Приложение А съдържа изчерпателен списък на цели на контрола и механизми за контрол. Тези, които използват този международен стандарт, се насочват към приложение А, за да се гарантира, че не са пропуснали необходими механизми за контрол.

ЗАБЕЛЕЖКА 2: Целите на контрола са косвено включени в избраните механизми за контрол. Целите на контрола и механизмите за контрол, изброени в приложение А, не са изчерпателни и е възможно да са необходими допълнителни цели на контрола и механизми за контрол.

d) изработи „Декларация за приложимост", която съдържа необходимите механизми за контрол (виж 6.1.3 b) и c)), обосновка за включването им, дали те са реализирани или не и обосновка за изключване на механизми за контрол от приложение А;

e) формулира план за въздействие върху риска за сигурността на информацията и

f) получи от собствениците на риск одобрение на плана за въздействие върху риска за сигурността на информацията, както и приемане на остатъчните рискове за сигурността на информацията.

Организацията трябва да съхранява документирана информация относно процеса за въздействие върху риска за сигурността на информацията.

ЗАБЕЛЕЖКА: Процесът за оценяване и въздействие върху риска за сигурността на информацията в този международен стандарт е в съответствие с принципите и общите насоки, представени в ISO 31000[5].

6.2 Цели на сигурността на информацията и планиране за постигането им

Организацията трябва да установи своите цели за сигурността на информацията на подходящи функции и нива.

Целите за сигурността на информацията трябва:

a) да са в съответствие с политиката за сигурност на информацията;

b) да са измерими (ако е осъществимо);

c) да вземат предвид приложимите изисквания към сигурността на информацията, както и резултатите от оценяването на риска и въздействието върху риска;

d) да са оповестени и

e) да са подходящо осъвременени.

Организацията трябва да съхранява документирана информация за целите на сигурността на информацията.

Когато планира как да постигне своите цели за сигурността на информацията, организацията трябва да определи:

f) какво трябва да се направи;

g) какви ресурси са необходими;

h) кой ще бъде отговорен;

i) кога това ще бъде завършено и

j) как ще бъдат оценени резултатите.

7 Поддържане

7.1 Ресурси

Организацията трябва да определи и осигури необходимите ресурси за създаването, внедряването, поддържането и непрекъснатото подобряване на системата за управление на сигурността на информацията.

7.2 Компетентност

Организацията трябва:

a) да определи необходимата компетентност на лицето(ата), което(ито) извършва(т) работа под неин контрол, засягаща действието на сигурността на нейната информация;

b) да гарантира, че тези лица са компетентни въз основа на подходящо образование, обучение или опит;

c) когато е приложимо, да предприеме действия за придобиване на необходимата компетентност и да оцени ефикасността от предприетите действия и

d) да съхранява подходяща документирана информация като доказателство за компетентност.

ЗАБЕЛЕЖКА: Приложимите действия може да включват например: осигуряване на обучение, наставничество или преназначаване на сегашни служители; или наемане, или договаряне с компетентни лица.

7.3 Осъзнаване

Лицата, извършващи работа под контрола на организацията, трябва да имат ясна представа за:

a) политиката за сигурност на информацията;

b) своя принос към ефикасността на системата за управление на сигурността на информацията, включително и ползите от подобрено действие на сигурността на информацията; и

c) последствията от несъответствие с изискванията на системата за управление на сигурността на информацията.

7.4 Обмен на информация

Организацията трябва да определи необходимостта от вътрешен и външен обмен на информация, съответстващ на системата за управление на сигурността на информацията, който включва:

a) каква информация да се обменя;

b) кога да се обменя информация;

c) с кого да се обменя информация;

d) кой трябва да обменя информация и

e) процесите, чрез които трябва да бъде осъществен обменът на информация.

7.5 Документирана информация

7.5.1 Общи положения

Системата за управление на сигурността на информацията трябва да включва:

a) изискваната от този международен стандарт документирана информация и

b) документирана информация, определена от организацията като необходима за ефикасността на системата за управление на сигурността на информацията.

ЗАБЕЛЕЖКА: Размерът на документираната информация за система за управление на сигурността на информацията на една организация може да се различава от тази на друга поради:

1) размера на организацията и вида на нейните дейности, процеси, продукти и услуги;

2) сложността на процесите и техните взаимодействия и

3) компетентността на лицата.

7.5.2 Създаване и актуализиране

Когато създава или актуализира документирана информация, организацията трябва да осигури подходящи:

a) идентифициране и описание (например заглавие, дата, автор или номер за справка);

b) формат (например език, версия на софтуера, графика) и информационен носител (например хартия, електронен) и

c) преглед и одобряване за съответствие и достатъчност.

7.5.3 Контрол на документираната информация

Изискваната от системата за управление на сигурността на информацията и от този международен стандарт документирана информация трябва да бъде контролирана, за да се гарантира, че:

a) тя е достъпна и подходяща за използване, където и когато това е необходимо, и

b) тя е съответно защитена (например от загуба на поверителност, неправилно използване или загуба на цялостност).

За контрол на документираната информация организацията трябва да разгледа следните дейности, доколкото е приложимо:

c) разпространяване, достъп, извличане и използване;

d) запомняне и запазване, включително запазване на възможността за четене;

e) контрол на измененията (например контрол на версиите) и

f) запазване и унищожаване.

Документираната информация от външен произход, определена от организацията като необходима за планиране и работа на системата за управление на сигурността на информацията, трябва да бъде идентифицирана по подходящ начин и контролирана.

ЗАБЕЛЕЖКА: Достъп означава решение, отнасящо се за разрешение само за гледане на документираната информация или за разрешение и оторизиране за гледане и изменяне на документираната информация и т.н.

8 Работа

8.1 Планиране на работата и контрол

Организацията трябва да планира, внедри и контролира процесите, необходими за отговаряне на изискванията за сигурност на информацията, и да осъществи действията, определени в 6.1. Също така

организацията трябва да внедри плановете за постигане на целите за сигурност на информацията, определени в 6.2.

Организацията трябва да съхранява документирана информация в степен, необходима за постигане на увереност, че процесите са проведени, както е планирано.

Организацията трябва да контролира планираните изменения и да извършва преглед на последствията от неволни промени, предприемайки действия за смекчаване на всякакви неблагоприятни последствия, както е необходимо.

Организацията трябва да гарантира, че процесите, изпълнявани от външни изпълнители, са определени и контролирани.

8.2 Оценяване на риска за сигурността на информацията

Организацията трябва да провежда оценяване на риска за сигурността на информацията през планирани периоди или когато са предложени или осъществени съществени изменения, отчитайки установените в 6.1.2 а) критерии.

Организацията трябва да запазва документирана информация от оценяването на риска за сигурността на информацията.

8.3 Въздействие върху риска за сигурността на информацията

Организацията трябва да реализира план за въздействие върху риска за сигурността на информацията.

Организацията трябва да запазва документирана информация за резултатите от въздействието върху риска за сигурността на информацията.

9 Оценяване на работните характеристики

9.1 Мониторинг, измерване, анализ и оценяване

Организацията трябва да оцени работните характеристики на сигурността на информацията и ефикасността на системата за управление на сигурността на информацията.

Организацията трябва да определи:

a) какво трябва да бъде наблюдавано и измервано, включително процесите и механизмите за контрол на сигурността на информацията;

b) методите за мониторинг, измерване, анализ и оценяване, както е подходящо, за гарантиране на валидни резултати;

ЗАБЕЛЕЖКА: Избраните методи трябва да дават сравними и възпроизводими резултати, за да бъдат считани за валидни.

c) кога трябва да бъдат извършвани мониторингът и измерването;

d) кой трябва да извършва мониторинг и измерване;

e) кога трябва да бъдат анализирани и оценени резултатите от мониторинга и измерването и

f) кой трябва да анализира и оцени тези резултати.

Организацията трябва да съхранява подходяща документирана информация като свидетелство за резултатите от мониторинга и измерването.

9.2 Вътрешен одит

Организацията трябва да извършва вътрешни одити през планирани интервали, за да осигури информация дали системата за управление на сигурността на информацията:

a) съответства на

1) собствените изисквания на организацията за системата за управление на сигурността на информацията и

2) изискванията на този международен стандарт;

b) е ефикасно внедрена и поддържана.

Организацията трябва:

c) да планира, създаде, внедри и поддържа програма(и) за одит, включително честотата, методите, отговорностите, изискванията за планиране и докладване. Програмата(ите) за одит трябва да взема(т) предвид важността на засегнатите процеси и резултатите от предишни одити;

d) за всеки одит да определи критериите и обхвата на одита;

e) да избере одитори и да провежда одити, които осигуряват обективност и безпристрастност на процеса на одит;

f) да осигури резултатите от одитите да бъдат докладвани на съответното ръководство и

g) да съхранява документирана информация като свидетелство за програмата(ите) за одит и за резултатите от одита.

9.3 Преглед от ръководството

Висшето ръководство трябва да извършва преглед на системата за управление на сигурността на информацията през планирани периоди от време, за да осигури нейната непрекъсната актуалност, адекватност и ефикасност.

Прегледът от ръководството трябва да включва разглеждане на:

a) състоянието на действията от предишни прегледи от ръководството;

b) промените във външни и вътрешни спорни въпроси, които имат отношение към системата за управление на сигурността на информацията;

c) обратната връзка върху работата за сигурността на информацията, включително тенденции в:

1) несъответствия и коригиращи действия;

2) резултати от мониторинг и измерване;

3) резултати от одит и

4) изпълнение на целите на сигурността на информацията;

d) обратна връзка от заинтересуваните лица;

e) резултати от оценяването на риска и състояние на плана за въздействие върху риска и

f) възможности за непрекъснато подобряване.

Резултатите от прегледа от ръководството трябва да включват решения, отнасящи се за възможностите за непрекъснато подобряване и всякакви потребности от промени в системата за управление на сигурността на информацията.

Организацията трябва да съхранява документирана информация като свидетелство за резултатите от прегледите от ръководството.

10 Подобряване

10.1 Несъответствие и коригиращо действие

Когато настъпи несъответствие, организацията трябва:

a) да реагира на несъответствието и когато е приложимо:

1) да предприеме действие за контролирането и коригирането му и

2) да се занимае с последствията;

b) да оцени необходимостта от действие за отстраняване на причините за несъответствието, с оглед то да не се повтори или да не се случи другаде, чрез:

1) разглеждане на несъответствието;

2) определяне на причините за несъответствието и

3) определяне дали съществуват подобни несъответствия или потенциално могат да възникнат;

c) приложи всяко необходимо действие;

d) да извърши преглед на ефикасността от всяко предприето коригиращо действие и

e) направи промени в системата за управление на сигурността на информацията, ако е необходимо.

Коригиращите действия трябва да съответстват на ефекта от възникналите несъответствия.

Организацията трябва да съхранява документирана информация като свидетелство за:

f) естеството на несъответствията и всякакви предприети последващи действия и

g) резултатите от всяко коригиращо действие.

10.2 Непрекъснато подобряване

Организацията трябва непрекъснато да подобрява актуалността, адекватността и ефикасността на системата за управление на сигурността на информацията.

Приложение А
(основно)

РЕФЕРЕНТНИ ЦЕЛИ НА КОНТРОЛА И МЕХАНИЗМИ ЗА КОНТРОЛ

Целите на контрола и механизмите за контрол, изброени в таблица А.1, са взети направо и уеднаквени с тези, дадени в ISO/IEC 27002:2013 [1], точки от 5 до 18, и трябва да бъдат използвани в контекста на 6.1.3.

Таблица А.1 - Цели на контрола и механизми за контрол

А.5 Политики за сигурност на информацията		
А.5.1 Насока за управление на сигурността на информацията		
Цел: Да осигури насока за управление и поддържане на сигурността на информацията в съответствие с изискванията за дейността и изискванията на съответното законодателство и нормативни актове.		
А.5.1.1	Политики по сигурност на информацията	*Контрол* Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от ръководството, разпространен и разгласен на всички служители и съответните външни страни.
А.5.1.2	Преглед на политиките за сигурност на информацията	*Контрол* Политиките за сигурност на информацията трябва да бъдат подлагани на преглед през планирани интервали или при настъпване на значителни промени, за да се гарантира постоянно тяхната актуалност, адекватност и ефикасност.
А.6 Организиране на сигурността на информацията		
А.6.1 Вътрешна организация		
Цел: Да установи управленска рамка за въвеждане и контрол на реализирането и оперирането на сигурност на информацията в рамките на организацията.		
А.6.1.1	Роли и отговорности по сигурността на информацията	*Контрол* Трябва да бъдат определени и разпределени всички отговорности по сигурността на информацията
А.6.1.2	Разделяне на задълженията	*Контрол* Трябва да бъдат разделени противоречивите задължения и области на отговорност, за да бъдат намалени възможностите за неоторизирано или неумишлено модифициране, или злоупотреба с активите на организацията.
А.6.1.3	Контакт с оторизираните органи	*Контрол* Трябва да се поддържат подходящи контакти със съответните оторизирани органи.
А.6.1.4	Контакт с групи със специален интерес	*Контрол* Трябва да бъдат поддържани подходящи контакти с групи със специален интерес или други форуми на специалисти по сигурността и професионални асоциации.
А.6.1.5	Сигурност на информацията при управление на проекти	*Контрол* Независимо от вида на проекта трябва да бъде отчетена сигурността на информацията при управление на проекти.

Таблица А.1 *(продължение)*

А.6.2 Мобилни устройства и работа от разстояние		
Цел: Да осигури сигурност при работа от разстояние и използване на мобилни устройства.		
А.6.2.1	Политика за мобилните устройства	*Контрол* Трябва да бъдат приети политика и поддържащи мерки за сигурност за управление на рисковете, внесени от използването на мобилни устройства.
А.6.2.2	Работа от разстояние	*Контрол* Трябва да бъдат приложени политика и поддържащи мерки за сигурност, за да се защити достъпната, обработваната или съхраняваната информация в местата за работа от разстояние.
А.7 Сигурност на човешките ресурси		
А.7.1 Преди наемане на работа		
Цел: Да се гарантира, че служители и доставчици разбират своите отговорности и са подходящи за ролите, които ще изпълняват.		
А.7.1.1	Подбор на кадри	*Контрол* Трябва да бъде извършвано проучване за проверка на биографичните данни на всички кандидати за наемане на работа в съответствие със съответните закони, нормативни актове и етика и съобразно изискванията, свързани с дейността, класификацията на информацията, до която имат достъп, и предполагаемите рискове.
А.7.1.2	Срокове и условия за наемане на работа	*Контрол* Договорни споразумения със служителите и доставчиците трябва да определят техните отговорности и отговорностите на организацията по отношение на сигурността на информацията.
А.7.2 По време на работа		
Цел: Да се гарантира, че служителите и доставчиците са запознати и изпълняват своите отговорности по отношение на сигурността на информацията.		
А.7.2.1	Отговорности на ръководството	*Контрол* Ръководството трябва да изисква от служителите и доставчиците да прилагат мерките за сигурност в съответствие с установените политики и процедури на организацията.
А.7.2.2	Осъзнаване, образование и обучение по сигурност на информацията	*Контрол* В съответствие със своите работни функции всички служители на организацията и, където е уместно, доставчиците трябва да получат подходящо обучение с цел осъзнаване и редовно актуализиране на знанията по политиките и процедурите на организацията.
А.7.2.3	Дисциплинарен процес	*Контрол* За служители, извършили нарушение по отношение на сигурността на информацията, трябва да има официален и оповестен дисциплинарен процес.
А.7.3 Прекратяване или промяна на трудовите отношения		
Цел: Да се защитят интересите на организацията като част от процеса за промяна или прекратяване на трудовите правоотношения.		
А.7.3.1	Отговорности при прекратяване или промяна на трудовото отношение	*Контрол* Отговорностите и задълженията по отношение сигурността на информацията при прекратяване или промяна на трудовото отношение трябва да бъдат определени, оповестени на служителя или доставчика и приведени в действие.

Таблица А.1 *(продължение)*

А.8 Управление на активи		
А.8.1 Отговорност за активите		
Цел: Да се идентифицират активите на организацията и да се определят съответните отговорности за защитата им.		
А.8.1.1	Опис на активите	*Контрол* Всички активи, свързани с информационните средства и средствата за обработване на информация, трябва да бъдат ясно идентифицирани и на тези активи трябва да бъде съставен и поддържан опис.
А.8.1.2	Притежание на активи	*Контрол* Активите, поддържани в описа, трябва да бъдат притежавани.
А.8.1.3	Допустимо използване на активи	*Контрол* Трябва да бъдат посочени, документирани и прилагани правила за допустимо използване на информация и активи, свързани с информацията и средствата за обработване на информация.
А.8.1.4	Връщане на активи	*Контрол* Всички служители и потребители от трета страна при прекратяване на тяхното трудово отношение, договор или споразумение трябва да върнат всички притежавани от тях активи на организацията.
А.8.2 Класифициране на информацията		
Цел: Да се гарантира, че информацията получава необходимата степен на защита в съответствие с важността ѝ за организацията.		
А.8.2.1	Класифициране на информацията	*Контрол* Информацията трябва да бъде класифицирана според изискванията на нормативните актове, нейната стойност, критичност и чувствителност към неоторизирано разкриване или модифициране.
А.8.2.2	Означаване на информацията	*Контрол* Трябва да бъде разработен и приложен съответен набор от процедури за означаване на информацията в съответствие с класификационната схема на информацията, приета от организацията.
А.8.2.3	Работа с активи	*Контрол* Трябва да бъдат разработени и приложени процедури за работа с активи в съответствие с класификационната схема на информацията, приета от организацията.
А.8.3 Работа с информационни носители		
Цел: Да се предотврати неоторизирано разкриване, изменение, премахване или разрушаване на информация, съхранявана върху носители.		
А.8.3.1	Управление на сменяеми носители	*Контрол* Трябва да има внедрени процедури за управлението на сменяеми информационни носители в съответствие с класификационната схема, приета от организацията.
А.8.3.2	Унищожаване на носители	*Контрол* Ненужните носители трябва да се унищожават по сигурен начин, като се използват официални процедури.

Таблица А.1 *(продължение)*

A.8.3.3	Пренасяне на физически носители	*Контрол* По време на транспортиране носителите, съдържащи информация, трябва да бъдат защитени срещу неоторизиран достъп, използване не по предназначение или подправяне.
A.9 Контрол на достъпа		
A.9.1 Изисквания за дейността за контрол на достъпа		
Цел: Да се ограничи достъпът до информацията и средствата за обработване на информация.		
A.9.1.1	Политика за контрол на достъпа	*Контрол* Трябва да бъде създадена, документирана и подлагана на преглед политика за контрол на достъпа, основана на изискванията за дейността и изискванията за сигурност на информацията.
A.9.1.2	Достъп до мрежи и мрежови услуги	*Контрол* На потребителите трябва да бъде осигурен достъп само до тези мрежи и мрежови услуги, за които те са изрично оторизирани да използват.
A.9.2 Управление на достъпа на потребителите		
Цел: Да се гарантира оторизиран достъп на потребителите и да се предотврати неоторизиран достъп до системи и услуги.		
A.9.2.1	Регистрация и прекратяване на регистрацията на потребители	*Контрол* Трябва да бъде реализиран официален процес за регистрация и прекратяване на регистрацията на потребителите, който да предостави присвояване на права за достъп.
A.9.2.2	Осигуряване на достъп на потребители	*Контрол* Трябва да бъде реализиран официален процес за предоставяне на достъп на потребителите, който да предостави или отнеме правата за достъп на всички видове потребители до всички системи и услуги.
A.9.2.3	Управление на привилегировани права за достъп	*Контрол* Предоставянето и използването на привилегировани права за достъп трябва да бъде ограничено и контролирано.
A.9.2.4	Управление на тайната информация за автентификация на потребителите	*Контрол* Предоставянето на тайна информация за автентификация трябва да бъде контролирано чрез официален процес за управление.
A.9.2.5	Преглед на правата за достъп на потребителите	*Контрол* Собствениците на активи трябва да преглеждат правата за достъп на потребителите през редовни интервали.
A.9.2.6	Отнемане или коригиране на права за достъп	*Контрол* Правата за достъп на всички служители или потребители от трета страна до информацията и до средствата за обработване на информация трябва да бъдат отнети при прекратяване на тяхното трудово отношение, договор или споразумение или коригирани при настъпване на промяна.
A.9.3 Отговорности на потребителите		
Цел: Да се държат потребителите отговорни за защита на тяхната информация за автентификация.		

Таблица А.1 *(продължение)*

A.9.3.1	Използване на тайна информация за автентификация	*Контрол* Трябва да се изисква от потребителите да следват практиките на организацията при използването на тайна информация за автентификация.
A.9.4 Контрол на достъпа до системи и приложения		
Цел: Да се предотврати неоторизиран достъп до системи и приложения.		
A.9.4.1	Ограничаване на достъпа до информация	*Контрол* Трябва да бъде ограничен достъпът до информация и функциите на приложните системи в съответствие с политиката за контрол на достъпа.
A.9.4.2	Процедури за сигурно влизане в системата	*Контрол* Когато се изисква от политиката за контрол на достъпа, достъпът до системи и приложения трябва да бъде контролиран чрез процедура за сигурно влизане в системата.
A.9.4.3	Система за управление на пароли	*Контрол* Системите за управление на пароли трябва да бъдат интерактивни и да осигуряват качество на паролите.
A.9.4.4	Използване на привилегировани обслужващи програми	*Контрол* Използването на обслужващи програми, които биха могли да преодолеят механизмите за контрол на системата и приложенията, трябва да бъде ограничено и строго контролирано.
A.9.4.5	Контрол на достъпа до изходен код на програмите	*Контрол* Достъпът до изходния код на програмите трябва да бъде ограничен.
A.10 Криптография		
A.10.1 Криптографски механизми за контрол		
Цел: Да се защитят поверителността, достоверността и/или цялостността на информацията чрез правилно и ефикасно използване на криптография.		
A.10.1.1	Политика за използване на криптографски механизми за контрол	*Контрол* Трябва да бъде разработена и провеждана политика за използването на криптографски механизми за контрол с цел защита на информацията.
A.10.1.2	Управление на ключове	*Контрол* Трябва да се разработи и внедри управление на използването, защитата и времето на живот на криптографските ключове през целия им жизнен цикъл.
A.11 Физическа сигурност и сигурност на заобикалящата среда		
A.11.1 Сигурни зони		
Цел: Да се предотврати неоторизиран физически достъп, вреда и вмешателство в информацията и средствата за обработване на информация на организацията.		
A.11.1.1	Граници за физическа сигурност	*Контрол* За защита на зони, които съдържат или чувствителна, или критична информация и средства за обработване на информация, трябва да се определят и използват граници за сигурност.

Таблица А.1 *(продължение)*

A.11.1.2	Механизми за контрол на физическо влизане	*Контрол* Сигурните зони трябва да бъдат защитени със съответни механизми за контрол на влизане, за да се гарантира, че само оторизираният персонал има разрешен достъп.
A.11.1.3	Осигуряване на офиси, зали и съоръжения	*Контрол* Трябва да бъде проектирана и приложена физическа защита за офиси, зали и съоръжения.
A.11.1.4	Защита от външни заплахи и заплахи от околната среда	*Контрол* Трябва да бъде проектирана и приложена физическа защита от природни бедствия, злонамерени атаки или инциденти.
A.11.1.5	Работа в сигурни зони	*Контрол* Трябва да бъдат разработени и приложени процедури за работа в сигурни зони.
A.11.1.6	Зони за доставки и зареждане	*Контрол* Местата за достъп като зони за доставки и зареждане и други места, където неупълномощени лица могат да влязат в помещенията, трябва да бъдат контролирани и ако е възможно, изолирани от средствата за обработване на информация, за да се избегне неоторизиран достъп.
A.11.2 Устройства		
Цел: Да се предотвратят загуби, повреди, кражби или излагане на риск на активите и прекъсване на дейностите на организацията.		
A.11.2.1	Разполагане и защита на устройствата	*Контрол* Устройствата трябва да бъдат разположени и защитени, така че да се намалят рисковете от заплахи и опасности от околната среда и възможности за неоторизиран достъп.
A.11.2.2	Поддържащи комунални системи	*Контрол* Устройствата трябва да бъдат защитени от повреди в електрозахранването и други разриви, предизвикани от откази в поддържащите комунални системи.
A.11.2.3	Сигурност на окабеляването	*Контрол* Окабеляването за електрозахранване и телекомуникации, носещо данни или поддържащо информационни услуги, трябва да бъде защитено от подслушване, смущения или повреда.
A.11.2.4	Поддържане на устройствата	*Контрол* Устройствата трябва да бъдат правилно поддържани, за да се осигури тяхната непрекъсната готовност и цялостност.
A.11.2.5	Изнасяне на собственост	*Контрол* Устройства, информация или софтуер не трябва да бъдат изнасяни извън организацията без предварително разрешение.
A.11.2.6	Сигурност на устройства и активи извън помещенията	*Контрол* Сигурността трябва да бъде прилагана и към активи, които са извън организацията, като се отчитат различните рискове при работа извън помещенията на организацията.

Таблица А.1 *(продължение)*

А.11.2.7	Сигурно унищожаване или повторно използване на устройства	*Контрол* Всички елементи на устройство, съдържащо запаметяващи носители, трябва да бъдат проверявани, за да се гарантира, че всякакви чувствителни данни и лицензиран софтуер са премахнати или сигурно презаписани преди унищожаването или повторното използване.
А.11.2.8	Ненадзиравани потребителски устройства	*Контрол* Потребителите трябва да осигурят оставените без надзор устройства да са подходящо защитени.
А.11.2.9	Политика за чисто бюро и чист екран	*Контрол* Трябва да бъде приета политика за бюро, чисто от хартиени документи и преносими информационни носители, и политика за чист екран при средствата за обработване на информация.
А.12 Сигурност на работата		
А.12.1 Процедури за работа и отговорности		
Цел: Да се осигури правилна и сигурна работа на средствата за обработване на информация.		
А.12.1.1	Документирани процедури за работа	*Контрол* Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях.
А.12.1.2	Управление на измененията	*Контрол* Измененията в организацията, процесите на дейността и средствата и системите за обработване на информация трябва да бъдат контролирани.
А.12.1.3	Управление на капацитета	*Контрол* Използването на ресурсите трябва да бъде наблюдавано, регулирано и да се предвиждат бъдещи изисквания за капацитета, за да се гарантира изискваната производителност на системата.
А.12.1.4	Отделяне на средите за разработване, изпитване и работа	*Контрол* Средите за разработване, изпитване и работа трябва да бъдат отделени, за да се намалят рисковете от неоторизиран достъп или изменения в средата на работа.
А.12.2 Защита от злонамерен софтуер		
Цел: Да се осигури защитата на информацията и средствата за обработване на информация от злонамерен софтуер.		
А.12.2.1	Механизми за контрол срещу злонамерен софтуер	*Контрол* Трябва да бъдат прилагани механизми за контрол за откриване, предотвратяване и възстановяване, които да защитят от злонамерен софтуер и които са съчетани с подходящо осведомяване на потребителите.
А.12.3 Резервиране		
Цел: Да защити от загуба на данни.		
А.12.3.1	Резервиране на информация	*Контрол* Трябва да бъдат направени и редовно изпитвани резервни копия на информация, софтуер и образи на системите в съответствие с договорената политика за резервиране.
А.12.4 Регистриране и наблюдение		
Цел: Да се записват събития и да се създадат доказателства.		

Таблица А.1 *(продължение)*

А.12.4.1	Регистриране на събития	*Контрол* Трябва да бъдат изработвани, съхранявани и редовно извършвани прегледи на регистри за събития, записващи дейности на потребители, изключителни случаи, грешки и събития, свързани със сигурността на информацията.
А.12.4.2	Защита на регистрираната информация	*Контрол* Средствата за регистрация и регистрираната информация трябва да бъдат защитени от подправяне и неоторизиран достъп.
А.12.4.3	Дневници на действията на системния администратор и оператора	*Контрол* Действията на системния администратор и оператора трябва да бъдат регистрирани, като дневниците трябва да бъдат защитени и редовно преглеждани.
А.12.4.4	Синхронизация на часовниците	*Контрол* Часовниците на всички системи за обработване на информация в организацията или зоната за сигурност трябва да бъдат синхронизирани с един единствен опорен източник на точно време.
А.12.5 Контрол на работещия софтуер		
Цел: Да се осигури цялостността на работещите системи.		
А.12.5.1	Инсталиране на софтуер върху работещи системи	*Контрол* Трябва да има внедрени процедури, контролиращи инсталирането на софтуер върху работещи системи.
А.12.6 Управление на техническата уязвимост		
Цел: Да се предотврати използването на технически уязвимости.		
А.12.6.1	Управление на техническите уязвимости	*Контрол* Трябва да бъде получена навременна информация за техническа уязвимост на използваните информационни системи; излагането на организацията на такава уязвимост трябва да бъде оценено и трябва да бъдат предприети мерки, за да се отговори на свързания с това риск.
А.12.6.2	Ограничения при инсталиране на софтуер	*Контрол* Трябва да бъдат създадени и приложени правила, определящи инсталирането на софтуер от потребители.
А.12.7 Разглеждане на одита на информационни системи		
Цел: Минимизиране на въздействието на процеса на одит върху работещите системи.		
А.12.7.1	Механизми за контрол при одит на информационни системи	*Контрол* Изискванията за одит и действията, включващи проверки на работещи системи, трябва да бъдат внимателно планирани и съгласувани, за да се минимизират нарушенията на процесите на дейността.
А.13 Сигурност на комуникациите		
А.13.1 Управление на сигурността на мрежите		
Цел: Да се осигури защита на информацията в мрежите и поддържащите ги средства за обработване на информация.		
А.13.1.1	Механизми за контрол на мрежите	*Контрол* Мрежите трябва да бъдат управлявани и контролирани, за да защитят информацията в системите и приложенията.

Таблица А.1 *(продължение)*

А.13.1.2	Сигурност на мрежови услуги	*Контрол* Механизмите за сигурност, нивата на услугата и изискванията за управление на всички мрежови услуги трябва да бъдат определени и включени във всяко споразумение за мрежови услуги, независимо от това, дали тези услуги се предоставят от самата организация или от външна организация.
А.13.1.3	Разделяне в мрежите	*Контрол* Вътре в мрежите групите информационни услуги, потребители и информационни системи трябва да бъдат разделени.
А.13.2 Обмен на информация		
Цел: Да се поддържа сигурността на информацията, обменяна вътре в организацията или с външни страни.		
А.13.2.1	Политики и процедури за обмен на информация	*Контрол* Трябва да съществуват официални политики, процедури и механизми за контрол, за да се защити обменът на информация чрез използване на всички средства за комуникация.
А.13.2.2	Споразумения за обмен на информация	*Контрол* При прехвърляне на информация за дейността между организацията и външни страни трябва да бъдат сключвани споразумения.
А.13.2.3	Електронен обмен на съобщения	*Контрол* Информацията, съдържаща се в електронните съобщения, трябва да бъде подходящо защитена.
А.13.2.4	Споразумения за поверителност или неразкриване на тайна	*Контрол* Трябва да бъдат определени, редовно преглеждани и документирани изисквания за споразумения за поверителност или за неразкриване на тайна, отразяващи потребностите на организацията от защита на информацията.
А.14 Придобиване, разработване и поддържане на системи		
А.14.1 Изисквания за сигурност на информационните системи		
Цел: Да се гарантира, че сигурността на информацията е неразделна част от информационните системи през целия им жизнен цикъл. Това включва също изисквания към информационни системи, които предоставят услуги през обществени мрежи.		
А.14.1.1	Анализ и спецификация на изискванията за сигурност на информацията	*Контрол* Изискванията, имащи отношение към сигурността на информацията, трябва да бъдат включени в изискванията за нови информационни системи или подобряване на съществуващи информационни системи.
А.14.1.2	Осигуряване на приложни услуги през обществени мрежи	*Контрол* Информацията, включена в приложни услуги, която преминава през обществени мрежи, трябва да бъде защитена от измамни действия, оспорване на договорни задължения и неоторизирано разкриване и изменение.

Таблица А.1 *(продължение)*

A.14.1.3	Защита на транзакции на приложни услуги	*Контрол* Информацията, включена в транзакции на приложни услуги, трябва да бъде защитена, за да се предотврати непълно предаване, погрешно маршрутизиране, неоторизирано изменение на съобщението, неоторизирано разкриване, неоторизирано дублиране на съобщение или атака чрез възпроизвеждане.
A.14.2 Сигурност при процесите на разработване и поддържане		
Цел: Да се осигури, че сигурността на информацията е проектирана и осъществена в рамките на цикъла на разработване на информационните системи.		
A.14.2.1	Политика за сигурно разработване	*Контрол* В рамките на организацията трябва да бъдат установени и приложени правила за разработване на софтуер и системи.
A.14.2.2	Процедури за контрол на измененията в системите	*Контрол* Извършването на изменения в системите в рамките на цикъла на разработване трябва да бъде контролирано чрез използване на официални процедури за контрол на измененията.
A.14.2.3	Технически преглед на приложенията след изменения в оперативната платформа	*Контрол* При изменения в оперативните платформи критичните приложения на дейностите трябва да бъдат преглеждани и изпитвани, за да се гарантира, че няма неблагоприятно въздействие върху работата или сигурността на организацията.
A.14.2.4	Ограничения върху измененията на софтуерните пакети	*Контрол* Модификации в софтуерните пакети трябва да бъдат избягвани, ограничени до необходимата степен и всички изменения трябва да бъдат строго контролирани.
A.14.2.5	Инженерни принципи за сигурни системи	*Контрол* Инженерни принципи за сигурни системи трябва да бъдат създадени, документирани, поддържани и приложени при всеки опит за реализиране на информационна система.
A.14.2.6	Сигурна среда за разработване	*Контрол* Организациите трябва да създадат и защитят по подходящ начин сигурна среда за разработване на опитите за разработване и интегриране на системи, която да обхваща целия цикъл на разработките.
A.14.2.7	Разработване на софтуер от външни страни	*Контрол* Разработването на софтуер от външни страни трябва да бъде следено и наблюдавано от организацията.
A.14.2.8	Изпитване на сигурността на системата	*Контрол* По време на разработването трябва да бъдат изпитани функционалните възможности по отношение на сигурността.
A.14.2.9	Приемни изпитвания на системата	*Контрол* За нови информационни системи, подобрения и нови версии трябва да бъдат създадени програми за приемно изпитване и свързани с тях критерии.
A.14.3 Данни при изпитване		
Цел: Да се осигури защита на данните, използвани при изпитване.		

Таблица А.1 *(продължение)*

A.14.3.1	Защита на данните при изпитване	*Контрол* Данните за изпитването трябва да бъдат внимателно подбрани, защитени и контролирани.
A.15 Взаимоотношения с доставчици		
A.15.1 Сигурност на информацията при взаимоотношения с доставчици		
Цел: Да се осигури защита на активите на организацията, които са достъпни за доставчика.		
A.15.1.1	Политика за сигурността на информацията при взаимоотношения с доставчици	*Контрол* С доставчика трябва да бъдат договорени и документирани изисквания за сигурност на информацията, които намаляват рисковете, свързани с достъпа на доставчика до активите на организацията.
A.15.1.2	Разглеждане на сигурността в рамките на споразумения с доставчици	*Контрол* Всички приложими изисквания към сигурността на информацията трябва да бъдат въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията.
A.15.1.3	Верига за доставки за информационни и комуникационни технологии	*Контрол* Споразуменията с доставчиците трябва да включват изисквания, отнасящи се за рисковете за сигурността на информацията, свързани с веригата за доставки на услуги и продукти на информационни и комуникационни технологии.
A.15.2 Управление на предоставянето на услуги от доставчици		
Цел: Да се поддържа договореното ниво на сигурност на информацията и предоставянето на услуги в съответствие със споразуменията с доставчици.		
A.15.2.1	Наблюдение и преглед на услуги, предоставяни от доставчици	*Контрол* Организациите трябва редовно да наблюдават, преглеждат и одитират предоставянето на услуги от доставчиците.
A.15.2.2	Управление на измененията на услугите, предоставяни от доставчици	*Контрол* Измененията на предоставянето на услуги от доставчици, съдържащи поддържане и усъвършенстване на съществуващи политики, процедури и механизми за контрол за сигурност на информацията, трябва да бъдат управлявани, като се отчита критичността на информацията, системите и процесите, свързани с дейността и повторно оценяване на рисковете.
A.16 Управление на инциденти със сигурността на информацията		
A.16.1 Управление на инциденти и подобряване на сигурността на информацията		
Цел: Да се осигури последователен и ефикасен подход към управление на инцидентите със сигурността на информацията, включително съобщаване за събития и слабости, свързани със сигурността.		
A.16.1.1	Отговорности и процедури	*Контрол* Трябва да бъдат установени отговорности и процедури за управление, за да се осигури бърза, ефикасна и системна реакция на инцидентите със сигурността на информацията.

Таблица А.1 *(продължение)*

A.16.1.2	Докладване за събития, свързани със сигурността на информацията	*Контрол* Събитията, свързани със сигурността на информацията, трябва да бъдат докладвани по съответни управленски канали възможно най- бързо.
A.16.1.3	Докладване за слабости в сигурността на информацията	*Контрол* Трябва да се изисква от служителите и доставчиците, използващи информационните системи и услуги на организацията, да отбелязват и докладват всяка наблюдавана или предполагаема слабост в сигурността в системите или услугите.
A.16.1.4	Оценяване на събития, свързани със сигурността на информацията, и вземане на решения за тях	*Контрол* Събитията, свързани със сигурността на информацията, трябва да бъдат оценени, като трябва да бъде решено дали те трябва да бъдат класифицирани като инциденти със сигурността.
A.16.1.5	Реакция на инциденти със сигурността на информацията	*Контрол* На инцидентите със сигурността на информацията трябва да се реагира в съответствие с документирани процедури.
A.16.1.6	Изводи от инцидентите със сигурността на информацията	*Контрол* Познанията, придобити при анализирането и разрешаването на инциденти със сигурността на информацията, трябва да бъдат използвани за намаляване на вероятността или въздействието на бъдещи инциденти.
A.16.1.7	Събиране на доказателства	*Контрол* Организацията трябва да определи и прилага процедури за идентифициране, събиране, придобиване и съхраняване на информация, която може да послужи като доказателство.
A.17 Аспекти на сигурността на информацията при управление на непрекъснатостта на дейността		
A.17.1 Непрекъснатост на сигурността на информацията		
Цел: Непрекъснатостта на сигурността на информацията трябва да бъде заложена в системите за управление на непрекъснатостта на дейността на организацията.		
A.17.1.1	Планиране на непрекъснатост на сигурността на информацията	*Контрол* Организацията трябва да определи своите изисквания за сигурност на информацията и за непрекъснатост на управлението на сигурността на информацията в неблагоприятни случаи, например по време на криза или бедствие.
A.17.1.2	Осъществяване на непрекъснатост на сигурността на информацията	*Контрол* Организацията трябва да създаде, документира, осъществи и поддържа процеси, процедури и механизми за контрол, за да осигури необходимото ниво на непрекъснатост за сигурността на информацията по време на неблагоприятни случаи.
A.17.1.3	Проверка, преглед и оценяване на непрекъснатостта на сигурността на информацията	*Контрол* Организацията трябва да проверява през редовни интервали създадените и осъществени механизми за контрол на непрекъснатостта на сигурността на информацията, така че да осигури, че те са действащи и ефикасни по време на неблагоприятни случаи.

Таблица А.1 *(продължение)*

А.17.2 Излишък		
Цел: Да се осигури готовност на средствата за обработване на информация.		
А.17.2.1	Готовност на средствата за обработване на информация	*Контрол* Средствата за обработване на информация трябва да бъдат осъществени с излишък, достатъчен за отговаряне на изискванията за готовност.
А.18 Съответствие		
А.18.1 Съответствие със законови и договорни изисквания		
Цел: Да се избегнат нарушения на правни, законови, нормативни или договорни задължения, отнасящи се за сигурността на информацията, както и на всички изисквания за сигурност.		
А.18.1.1	Идентифициране на приложимите законови и договорни изисквания	*Контрол* Всички съответни правни, законови, нормативни и договорни изисквания и подходът на организацията за удовлетворяване на тези изисквания трябва да бъдат изрично идентифицирани, документирани и актуализирани за всяка информационна система и за организацията.
А.18.1.2	Права на интелектуална собственост	*Контрол* Трябва да бъдат изпълнени съответни процедури, за да се осигури съответствие със законовите, нормативните и договорните изисквания по отношение на правата на интелектуална собственост и използване на патентовани софтуерни продукти.
А.18.1.3	Защита на записите	*Контрол* Записите трябва да бъдат защитени от изгубване, разрушаване, фалшифициране, неоторизиран достъп или неоторизирано огласяване в съответствие със законовите, нормативните и договорните изисквания и изискванията за дейността.
А.18.1.4	Тайна и защита на информацията за самоличността	*Контрол* Трябва да бъде осигурена тайната и защитата на информацията за самоличността според изискванията на съответните нормативни актове и регламенти, където са приложими.
А.18.1.5	Регламентиране на криптографските механизми за контрол	*Контрол* Криптографските механизми за контрол трябва да се използват в съответствие с всички приложими споразумения, нормативни актове и регламенти.
А.18.2 Прегледи на сигурността на информацията		
Цел: Да се осигури, че сигурността на информацията е осъществена и функционира в съответствие с политиките и процедурите на организацията.		
А.18.2.1	Независим преглед на сигурността на информацията	*Контрол* През планирани интервали или при настъпили съществени промени трябва да се извършва независим преглед на подхода на организацията за управление на сигурността на информацията и неговото прилагане (т.е. целите на контрола, механизмите за контрол, политиките, процесите и процедурите за сигурност на информацията).

Таблица А.1 *(продължение)*

A.18.2.2	Съответствие с политиката и стандартите за сигурност	*Контрол* Ръководителите трябва редовно да преглеждат доколко обработването на информация и процедурите в тяхната област на отговорност съответстват на подходящите политики за сигурност, стандарти и всякакви други изисквания за сигурност.
A.18.2.3	Преглед на техническото съответствие	*Контрол* Информационните системи трябва редовно да се преглеждат за съответствие с политиките за сигурност на информацията в организацията и стандартите.

БИБЛИОГРАФИЯ

[1] ISO/IEC 27002:2013 *Information technology — Security Techniques — Code of practice for information security controls [Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията]*

[2] ISO/IEC 27003 *Information technology — Security techniques — Information security management system implementation guidance [Информационни технологии. Методи за сигурност. Указания за внедряване на системи за управление на сигурността на информацията]*

[3] ISO/IEC 27004 *Information technology — Security techniques — Information security management — Measurement [Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Измерване]*

[4] ISO/IEC 27005 *Information technology—Security techniques—Information security risk management [Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията]*

[5] ISO 31000:2009 *Risk management — Principles and guidelines [Управление на риска. Принципи и указания]*

[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement - Procedures specific to ISO*, 2012 [*Директиви на ISO/IEC, част 1, Обединено допълнение на ISO, Приложение SL, Процедури специфични за ISO]*