# Доставка на софтуер - особености и процеси

## Тема №4

Разпространени стандарти и регулации, гарантиращи определени характеристики на даден продукт и услуга

Част 5: ISO/IEC 27001

## Съдържание



## 1 Въведение

С увеличаването на случаите на киберпрестъпност и постоянната поява на нови заплахи във виртуалното пространство, може да изглежда трудно и дори невъзможно да управляваме киберрисковете. Именно за това са предназначени стандартите от серията ISO/IEC 27000. Те представляват множество взаимно допълващи се стандарти за информационна сигурност, които заедно създават основа за изграждане на световно-призната система за управление на информационната сигурност в организациите. Във времена на масова дигитализация в огромна част от отраслите на бизнеса, такава система за информационна сигурност придобива ключово значение.

В тази лекция ще разгледаме в повече детайли един конкретен стандарт от серията – ISO/IEC 27001.

# 2 Същност

ISO/IEC 27001 е вероятно най – популярния в световен мащаб стандарт за системи за управление на информационната сигурност (СУИС, information security management systems, ISMS). Той дефинира набор от изисквания, които една такава система трябва да удовлетвори. Стандартът дава на компании от всякакъв размер и характер на дейността насоки за създаване, внедряване, поддръжка и постоянно подобряване на СУИС.

## 2.1 Какво е СУИС?

Система за управление на информационна сигурност (СУИС) е структурирана рамка от политики и процедури за систематично управление на чувствителната информация на организацията.

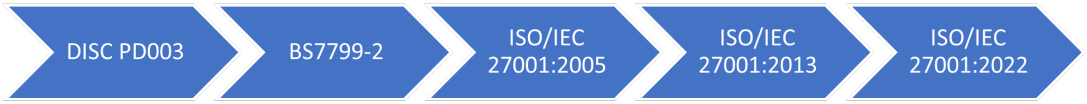
Включва процеси, хора, технологии и процедури, проектирани да предпазват от неоторизиран достъп, използване, разкриване, нарушение, модификация или унищожаване на информация.

СУИС също така определя ролите и отговорностите на персонала, участващ в управлението на информационната сигурност, и предоставя насоки за идентифициране, оценка и намаляване на рисковете.

Тя може също така да бъде използвана за наблюдение на ефективността на мерките за сигурност и предоставяне на доказателства за съответствие с приложимите закони и регулации.

## 2.2 История

В началото на 90-те години на 20-ти век, все повече компании започват да осъзнават важността на сигурността на информацията. По поръчка на Британското правителство се разработва документ наречен DISC PD003. Той има за цел да представи набор от добри практики за информационна сигурност. Работата по него в последствие се разделя на две – BS7799-1 и BS7799-2. Вторият от тях създава формален стандарт за разработка на СУИС. Публикуван е през 1998 от Британския институт за стандартизация (British Standards Institution, BSI) и в последствие се превръща в ISO/IEC 27001, публикуван от международната организация по стандартизация (ISO) в партньорство с международната електротехническа комисия (IEC) през 2005. В последствие следват две ревизии на стандарта - през 2013 и 2022 година. Актуалния стандарт е ISO/IEC 27001:2022.




Фиг. 1: Времева линия на ISO/IEC 27001

## 2.3 Основни принципи

Основната цел на стандарта и на СУИС е да осигури три аспекта на предпазването на информацията:

- **Конфиденциалност (confidentiality)** - само оторизирани лица имат достъп до информацията.
- **Интегритет (integrity)** - само оторизирани лица могат да променят информацията. Изисква се и проследимост на направените промени.
- **Наличност (availability)**- информацията трябва да е достъпна за оторизирани лица винаги, когато е нужна.

Тези принципи се постигат, използвайки техники и процеси за управление на риска, давайки гаранции на всички заинтересовани лица, че рисковете са задоволително обработени.

## 2.4 Ползи от стандарта

Имплементацията на стандарта има неоспорими ползи. Някои от тях са:

- **Съответствие с нормативната уредба** – все по–голям е броят на законите, регулациите и договорните отношения, отнасящи се до информационната сигурност. Голяма част от тези изисквания могат да бъдат удовлетворени чрез стандарта.

- **Създаване на конкурентно предимство** – организация би изглеждала по–привлекателна за потенциални клиенти, от гледна точка вероятността данните да бъдат предпазени при използването на продуктите/услугите.
- **Намалени разходи** – основна философия на стандарта е да предотврати инцидентите, свързани с информационната сигурност. А всеки инцидент, без значение от размера, води до разходи. Предотвратявайки инцидентите, организацията елиминира и въпросните разходи.
- **По–добра организация** – често компании не обръщат необходимото внимание на дефинирането и документирането на своите процеси. Стандарта стимулира компаниите да обърнат внимание на този проблем и да документират процесите си, спестявайки време и гарантирайки приемственост на знанията.

# 3 Изисквания

Всяко едно от тези изисквания е задължително, за да може да кажем че една организация отговаря на стандарта. Изискванията са групирани тематично в 7 групи.

## 3.1 Контекст на организацията

- **Разбиране на организацията и нейния контекст** – определяне на външните и вътрешни проблеми, имащи отношение към постигането на желаните резултати от управлението на информационната сигурност.
- **Разбиране на нуждите и очакванията на заинтересовани страни** – определяне кои са заинтересованите лица за СУИС, техните изисквания и кои от тях могат да се адресират чрез СУИС.
- **Определяне на обхвата на СУИС** – определяне границите и приложимостта на СУИС и нейния обхват. Трябва да вземе предвид идентифицираното в предните две изисквания и взаимовръзките с други организации.
- **СУИС** – установяване, имплементация, поддръжка и постоянно подобряване на СУИС, включително нужните процеси, според стандарта.

## 3.2 Лидерство

- **Лидерство и ангажираност** – мениджмънта трябва да демонстрира лидерство и ангажираност по отношение СУИС.
- **Политики** – висшето ръководство трябва да установи политика за сигурност на информацията, която:
  - е подходяща за целите на организацията;
  - включва цели за сигурност на информацията или предоставя рамката за формулиране на цели за сигурност на информацията;
  - включва ангажимент за удовлетворяване на приложимите изисквания, свързани със сигурността на информацията;
  - включва ангажимент за непрекъснато подобрение на системата за управление на сигурността на информацията.

  Политиката за сигурност на информацията трябва да:
  - бъде налична като документирана информация;
  - бъде комуникирана в организацията;
  - бъде налична за заинтересованите страни, ако е подходящо.
- **Роли, отговорности и пълномощия** – трябва да се осигури, че различните роли, свързани с информационната сигурност са възложени и това е ясно комуникирано.

## 3.3 Планиране

- **Действия за адресиране на рискове и възможности** – при планиране на СУИС, трябва да се определят рисковете и възможностите. Създава се план за действие в случай, че възникнат. Нужни са ясно дефинирани и прилагани процеси за оценка и справяне с рисковете.
- **Цели на информационната сигурност и планиране за постигането им** – да се установят ясни, комуникирани цели по отношение на информационната сигурност. Те трябва постоянно да се следят, измерват и, при нужда, адаптират.
- **Планиране на промени** – при нужда от изменения по СУИС, те трябва да бъдат приложени по планиран начин.

## 3.4 Поддържане

- **Ресурси** – трябва да се определят и предоставят необходимите за СУИС ресурси.
- **Компетентности** – организацията трябва да:
  1. определи необходимата компетентност на лицата, извършващи работа под нейно контрол, които влияят на нейната производителност в областта на сигурността на информацията;
  2. осигури, че тези лица са компетентни на базата на подходящо образование, обучение или опит;
  3. където е приложимо, предприеме действия за придобиване на необходимата компетентност и оцени ефективността на предприетите мерки;
  4. съхранява подходяща документирана информация като доказателство за компетентността.

  Приложимите действия могат да включват, например: предоставяне на обучение, наставничество или преквалификация на текущи служители; или наемане или наемане на компетентни лица.
- **Осъзнаване** – лицата, извършващи работа под контрола на организацията, трябва да бъдат осведомени за:
  1. информационната политика за сигурност;
  2. техния принос за ефективността на системата за управление на сигурността на информацията, включително ползите от подобряване на производителността в областта на сигурността на информацията;
  3. последствията от непридържане към изискванията на системата за управление на сигурността на информацията.
- **Комуникация** – определя се нуждата от външна и вътрешна комуникация по отношение на СУИС.
- **Документирана информация** – трябва да се осигури всичката необходима документация според изискванията на стандарта и да се следи за нейното качество, контрол на промените и други.

## 3.5 Работа

- **Планиране на работата и контрол** – процесите, необходими за постигане на изискванията и изпълнение на идентифицираните действия трябва да се планират, имплементират и контролират.
- **Оценяване на риска** – рисковете трябва да се оценяват регулярно и в случай на настъпване на сериозни промени.
- **Справяне с рисковете** – планът за справяне с рисковете трябва да се изпълнява от организацията.

## 3.6 Оценяване на работните характеристики

- **Наблюдаване, измерване, анализ и оценяване** – определяне на ефективността на СУИС чрез обективни и сравними критерии.
- **Вътрешен одит** – организацията трябва да провежда вътрешни одити на планираните интервали, за да предостави информация дали системата за управление на сигурността на информацията:

  1. отговаря на
     (a) изискванията на самата организация за нейната система за управление на сигурността на информацията;
     (b) изискванията на ISO/IEC 27001;
  2. се прилага и поддържа ефективно.

  Организацията трябва да планира, установява, въвежда и поддържа програма (или програми) за одит, включително честотата, методите, отговорностите, изискванията за планиране и предоставяне на доклади.

  При установяването на програмата за вътрешен одит, организацията трябва да обмисли важността на съответните процеси и резултатите от предишни одити.

  Организацията трябва да:

  1. дефинира критериите и обхвата на одита за всеки одит;
  2. избира одитори и провежда одити, които гарантират обективността и безпристрастността на одиторския процес;
  3. осигурява, че резултатите от одитите се докладват на съответното управление.

  Документирана информация трябва да бъде налична като доказателство за изпълнението на програмата (или програмите) за одит и резултатите от одитите.

- **Преглед от ръководството** – ръководството трябва да преглежда информационната система за управление на сигурността на информацията в организацията на планирани интервали, за да осигури нейната продължаваща пригодност, достатъчност и ефективност.

  Прегледът на управлението трябва да включва разглеждане на:

  1. статуса на действията от предишните прегледи на управлението;
  2. промени във външните и вътрешни въпроси, които са от значение за системата за управление на сигурността на информацията;
  3. промени в нуждите и очакванията на заинтересованите страни, които са от значение за системата за управление на сигурността на информацията;
  4. обратна връзка за представянето на сигурността на информацията, включително тенденции в:
     (a) несъответствията и коригиращите действия;
     (b) резултатите от наблюдение и измерване;
     (c) резултатите от аудитите;
     (d) изпълнението на целите за сигурност на информацията;
  5. обратна връзка от заинтересованите страни;
  6. резултати от оценката на риска и статуса на плана за управление на риска;
  7. възможности за продължително подобрение.

  Резултатите от прегледа на управлението трябва да включват решения, свързани с възможности за продължително подобрение и всички нужди от промени в системата за управление на сигурността на информацията. Документирана информация трябва да бъде налична като доказателство за резултатите от прегледите на управлението.

### 3.7 Подобряване

- **Непрекъснато подобряване** – СУИС постоянно трябва да се подобрява на база събраните данни и промените в бизнес средата.
- **Несъответствие и коригиращо действие** – когато възникне несъответствие, организацията трябва да:

  1. Реагира на несъответствието и, ако е приложимо:
     (a) Предприеме действия за контрол и коригиране.
     (b) Се справи с последствията.
  2. Оцени необходимостта от действия за премахване на причините за несъответствие, с цел да се предотврати повторение или поява на друго място, чрез:
     (a) Преглеждане на несъответствието.
     (b) Определяне на причините за несъответствието.
     (c) Определяне дали съществуват подобни несъответствия или те е възможно да възникнат.
  3. Изпълнение на необходимите действия.
  4. Преглед на ефективността на предприетите коректривни действия.
  5. Въвеждане на промени в системата за управление на информационната сигурност, ако е необходимо.

  Коректривните действия трябва да бъдат подходящи за последиците от проявилите се несъответствия. Документирана информация трябва да бъде налична като доказателство за:

  1. Характера на несъответствията и всички последващи действия.
  2. Резултатите от предприетите коректривни действия.

## 4 Контроли

Стандарта включва Приложение А - списък на всички контроли за сигурност и контролни цели, които могат да бъдат приложени в СУИС. В последното издание на стандарта броят на контролите е намален от 114 на 93, чрез обединяването на много от тях. Контролите са оформени в четири контролни групи (спрямо 14 в предното издание от 2013):

- Организационни контроли — 37 броя.
- Контроли, свързани с управлението на човешките ресурси — 8 броя.
- Контроли, свързани с физическата сигурност — 14 броя.
- Технологични контроли — 34 броя.

Ще представим кратко описание на всяка група и по 5 примерни контроли.

### 4.1 Организационни

Организационните контроли включват регламенти и мерки, които определят общата насоченост на организацията към защита на данните по широк кръг от въпроси. Тези контроли включват политики, правила, процеси, процедури, организационни структури и други.

#### Примери

- **5.1 Политиките за информационна сигурност** - Политиката за информационна сигурност и политиките, свързани с конкретни теми, трябва да бъдат разработени, одобрени от ръководството, публикувани, предоставени за запознаване на съответния персонал и съответните заинтересовани страни и преразглеждани на планирани интервали и при значителни промени.
- **5.3 Разделяне на задълженията** - Противоречащите си задължения и противоречащите си области на отговорност следва да бъдат разделени (да не се изпълняват от един човек или хора, обвързани помежду си под някаква форма (като директна мениджмънт връзка)).

- **5.7 Интелигентност за заплахи** - Информация, свързана със заплахите за информационната сигурност, трябва да бъде събирана и анализирана, за да се постигне интелигентност относно заплахите.
- **5.14 Трансфер на информация** - За всички видове трансферни средства в рамките на организацията и между организацията и други страни трябва да бъдат налице правила, процедури или споразумения за трансфер на информация.
- **5.35 Независим преглед на информационната сигурност** - Подходът на организацията към управлението на информационната сигурност и неговата реализация, включително хора, процеси и технологии, трябва да се преглежда независимо на планирани интервали или при значителни промени.

## 4.2 Свързани с управлението на човешките ресурси

Контролите, свързани с управлението на човешките ресурси позволяват на организациите да регулират човешкия компонент на тяхната програма за информационна сигурност, като определят начина, по който персоналът взаимодейства с данните и помежду си. Тези контроли включват сигурно управление на човешките ресурси, персонална сигурност и осведоменост и обучение.

**Примери**

- **6.1 Скрининг** - Проверки на миналото на всички кандидати за работа трябва да се извършват преди тяхното присъединяване към организацията и също така след това, като се вземат предвид съответните закони, регламенти и етика, и се адаптират пропорционално на бизнес изискванията, класификацията на информацията, до която трябва да има достъп, и възможните рискове.
- **6.3 Съзнание за информационна сигурност, образование и обучение** - Персоналът на организацията и съответните заинтересовани страни трябва да получават подходящо обучение и информация по отношение на информационната сигурност, както и редовни актуализации на политиката за информационна сигурност на организацията, политиките и процедурите, специфични за темата, колкото е необходимо за изпълнението на техните работни задължения.
- **6.6 Споразумения за поверителност или неразкриване на информация** - Споразумения за поверителност или неразкриване на информация, отразяващи нуждите на организацията за защита на информацията, трябва да бъдат идентифицирани, документирани, редовно преглеждани и подписвани от персонала и други съответни заинтересовани страни.
- **6.7 Работа от разстояние** - Мерки за сигурност трябва да бъдат внедрени, когато персоналът работи отдалечено, за да се защити информацията, към която се осъществява достъп, която се обработва или се съхранява извън предприятието.
- **6.8 Докладване за събития в областта на информационната сигурност** - Организацията трябва да предостави механизъм, чрез който персоналът може да докладва наблюдавани събития или подозрения за такива в областта на информационната сигурност чрез подходящи канали своевременно.

## 4.3 Свързани с физическата сигурност

Контролите, свързани с физическата сигурност са мерки, използвани за гарантиране на сигурността на материалните активи. Те могат да включват системи за влизане, протоколи за достъп на гости, процеси за унищожаване на активи, протоколи за съхранение на носители на информация и политики за чисти бюра. Такива защити са от съществено значение за запазването на поверителна информация.

**Примери**

- **7.2 Физически вход** - Защитените зони трябва да бъдат предпазени с подходящи контроли на достъпа и точки за влизане.

- **7.4 Физическо наблюдение за сигурност** - Обектите трябва да бъдат непрекъснато наблюдавани за неоторизиран физически достъп.
- **7.5 Защита срещу физически и екологични заплахи** - Защита срещу физически и екологични заплахи, като природни бедствия и други преднамерени или непреднамерени физически заплахи към инфраструктурата, трябва да бъде проектирана и внедрена.
- **7.7 Чисти бюро и екран** - Правила за чистота на бюрото за хартии и преносими средства за съхранение, както и правила за чист екран за средствата за обработка на информация, трябва да бъдат определени и подходящо спазвани.
- **7.14 Сигурно изхвърляне или повторно използване на оборудване** - Оборудването, съдържащо носители на информация, трябва да бъде проверено, за да се гарантира, че всякаква чувствителна информация и лицензиран софтуер са били премахнати или сигурно изтрити преди изхвърлянето или повторното използване.

### 4.4 Технологични

Технологичните ограничения определят цифровите регулации и процедури, които корпорациите следва да приемат, за да изградят защитена и съответстваща информационна инфраструктура. Това включва методи за удостоверяване, настройки, стратегии за резервно копиране и възстановяване след бедствия (B(U)DR) и логване на информацията.

**Примери**

- **8.4 Достъп до изходен код** - Достъпът за четене и писане на изходен код, инструменти за разработка и софтуерни библиотеки трябва да бъде адекватно управляван.
- **8.5 Сигурно удостоверяване** - Сигурни технологии и процедури за удостоверяване трябва да бъдат внедрени въз основа на ограниченията за достъп до информация и тематичната политика за контрол на достъпа.
- **8.8 Управление на техническите уязвимости** - Информация за техническите уязвимости на използваните информационни системи трябва да бъде събрана, валидността за организацията на тези уязвимости трябва да бъде оценено, и трябва да бъдат предприети подходящи мерки.
- **8.12 Предпазване от изтичане на данни** - Мерки за предпазване от изтичане на данни трябва да бъдат приложени към системи, мрежи и всички други устройства, които обработват, съхраняват или предават чувствителна информация.
- **8.24 Използване на криптография** - Правила за ефективното използване на криптография, включително управлението на криптографските ключове, трябва да бъдат определени и внедрени.

## 5 Сертификация

Сертификацията на организация по ISO/IEC 27001 дава ясен сигнал вътре и извън нея за предприетите практики относно информационната сигурност и важността ѝ за организацията. За това много организации предприемат тази стъпка. Сертификацията се получава в резултат на одит.

Одитът първо разглежда документацията на СУИС, за да провери съответствието с изискванията на стандарта и наличието на всички необходими контроли. При идентифициране на всякакви несъответствия, организацията има възможност да ги поправи преди финалния одит.

По време на финалния одит се разглеждат цялостно процесите и дейностите в практиката, за да се провери дали съответстват на документираните политики и стандарти. При успех, сертификацията е валидна за 3 години.


Фиг. 2: Процес за сертификация

# 6 Заключение

ISO/IEC 27001 е генерален (неспецифичен), общо приложим стандарт, наложил се в софтуерната индустрия. Той е от огромно значение в постоянния стремеж за постигане на високи нива на сигурност, предотвратяване на атаки и справяне с рисковете за сигурността. Познаването му и спазването на предписанията му е ключове за високото доверие към организациите по отношение на сигурността. А във времена, когато чувствителността към сигурността става все повече първостепенен фактор при взимане на решения, гаранциите, които стандарта дава могат да се окажат ключови.