Одит на информационната сигурност

Въведение в стандарта за управление на информационната сигурност ISO 27001:2005

Александър Станев
alex@stanev.org

Асоциация за информационна сигурност
www.iseca.org

Стандарти – въведение

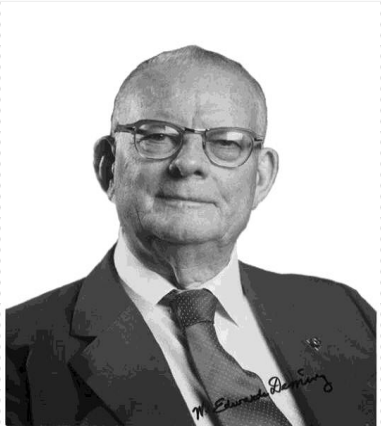
- Видове стандарти:
  - Индустриални (USB, VGA …)
  - Указателни (ISO 17799:2005)
  - Сертификационни (ISO/BS 7799-2:2002; ISO 27001:2005)
- Организации, изготвящи стандарти
  - International Standardization Organization (ISO)
  - British Standards (BS)
  - ANSI
  - …

Стандарти за управление

- Процесен подход
  - Постигането на бизнес-целите е по-ефективно, когато използваните ресурси и дейности се управляват като процес
- Видове системи за управление
  - Система за управление на качеството (СУК) ISO 9001:2000
  - Система за управление на околната среда (СУОС) ISO 14001:2004
  - Системи за безопасни условия на труд OHSAS
  - Системи за безопасно производство на хранителни продукти HACCAP
- Интегрирани системи за управление

Цикъл на Деминг (PDCA)

- Етапи на внедряване и поддръжка на система за управление
  - Планиране / Plan – разработват се необходимите документи за работата на системата (СУ)
  - Действие / Do – внедряване на СУ
  - Проверка / Check – оценка и измерване на дейностите спрямо целите
  - Усъвършенстане / Act – предприемане на коригиращи и превантивни действия



Система за управление на информационната сигурност

- Част от общата система за управление
- Целта е да се разработят, внедрят, инициират, наблюдават и подобряват дейности, свързани с информационната сигурност
- Базирана на подхода за бизнес риска

Термини и дефиниции

- Политика по информационната сигурност
- Наръчник по информационна сигурност
- Процедури по информационна сигурност
- Контрола по информационна сигурност
- Декларация за приложимост – описва целите и механизмите на контрол, които са приложими към СУИС в дадена организация. Базира се на резултатите от извършен анализ за оценка и третиране на риска

Структура на ISO 27001:2005

1. Обхват
2. Връзки
3. Термини и дефиниции
4. Система за управление на информационната сигурност (СУИС)
5. Отговорност на ръководството
6. Преглед на Ръководството на СУИС
7. Подобрения на СУИС

Приложение A: Цели по контрола и контроли – от ISO/IEC 17799:2005 (задължително)

Приложение B: Указания за приложението на стандарта (информативно)

Приложение C: Съответствия между EN ISO 9001:2000, EN 14001:2004 (информативно)

Приложение D: Промени във вътрешното номериране (информативно)

ISO 27001:2005 - Клауза 1

1. Обхват

1.1. Общи положения

За какво се отнася стандарта

1.2. Приложение

Изискванията на стандарта са така описани, че да са приложими за всякакъв вид организации. Ако все пак някои са нерелевантни поради типа и/или дейността на организацията, по това изискване може да се направи **изключение**. Тези изключения трябва да бъдат обосновани. Това е описано в Декларацията за приложимост.

Не могат да се правят изключения по клаузи 4, 5, 6 и 7.

ISO 27001:2005 - Клауза 4 - I

4. Система за управление на информационната сигурност (СУИС)

4.1. Общи изисквания

4.2. Създаване и управление на СУИС

4.2.1. Създаване на СУИС

- Определя се обхвата и Политиката по СУИС.
- Дефинира се подхода при оценка на риска
- Идентификация, оценка и възможности за третиране на рисковете
- Избират се контроли за третиране на риска
- Разработва се Декларация за приложимост

ISO 27001:2005 - Клауза 4 - II

4.2.2. Внедряване и действие на СУИС

- Разработване и внедряване на План за третиране на риска
- Внедряване на избраните в 4.2.1. контроли и процедурите за тяхното прилагане
- Внедряване на програма за обучение и осъзнатост
- Управление на дейността и ресурсите в организацията

4.2.3. Наблюдение и преглед на СУИС

- Изпълнение на процедури и контроли за наблюдение
- Извършване на прегледи на ефективността
- Извършване на прегледи на нивото на остатъчния и приемливия риск
- Планиране и провеждане на вътрешни одити
- Провеждане на Прегледи от ръководството на СУИС
- Водене на записи за събития, които могат да въздействат на СУИС

ISO 27001:2005 - Клауза 4 - III

4.2.3. Поддръжка и подобрение на СУИС

- Внедряване на идентифицираните подобрения
- Предприемане на подходящи превантивни и коригиращи действия
- Комуникиране на действията си и резултатите от тях към заинтересованите страни
- Гарантиране, че подобренията постигат набелязаните цели

4.3. Изисквания към документацията

4.3.1. Общи изисквания – СУИС трябва да включва:

- Политика по сигурността и цели по контрола
- Доклад за оценка на риска
- План за третиране на риска
- Документирани процедури по СУИС
- Записи, изисквани от стандарта
- Декларация за приложимост

ISO 27001:2005 - Клауза 4 - IV

4.3.2. Контрол на документите

Необходимо е да се внедри специална процедура за това.

- Кой одобрява документите
- Преглед, актуализиране и при нужда – повторна оценка
- Идентифициране на промените от версия към версия и достъп до актуалните версии
- Създаване на предпоставки за идентифициране на вътрешни и външни документи
- Контролиране на разпространението

4.3.3. Контрол на записите

Записите трябва да бъдат създавани, за да се гарантира изпълнението на изискванията на стандарта. Трябва да се гарантира тяхната необратимост и контрол. Нуждата им в конкретните области и обемът им се определя от Ръководството. (Пример:mail log, документи от одит, разрешения за физически достъп и т.н.)

Одити

- Целта на одита е да открие достоверни доказателства за правилното функциониране на внедрената система за управление
- Видове одити
  - Сертификационен
  - Контролен
  - Партньор ?
  - Вътрешен
- Процес на сертификация
  - Проектиране, разработка и внедряване на системата
  - Одитиране от акредитирна сертифицираща организация
  - Поддържане и усъвършенстване на системата
  - Ресертификация

Checklists

- Целта на одита е да открие достоверни доказателства за правилното функциониране на внедрената система за управление
- Видове одити
  - Сертификационен
  - Контролен
  - Партньор ?
  - Вътрешен
- Процес на сертификация
  - Проектиране, разработка и внедряване на системата
  - Одитиране от акредитирна сертифицираща организация
  - Поддържане и усъвършенстване на системата
  - Ресертификация

Въпроси

TPILB.

This page intentionally left blank.