Въведение в международния стандарт ISO/IEC 27001:2005

Име и история

- Пълно име:
  - “ISO/IEC 27001:2005 – Информационни технологии – Методи за сигурност – Системи за управление на сигурността на информацията – Изисквания”
- История:
  - 1995 – Британски стандарт BS7799 – добри практики
  - 2000 – BS7799 е включен в списъка на ISO стандартите под името ISO/IEC 17999
  - 2002 – BS7799-2 – спецификация с изисквания
  - 2005 – нова версия на ISO/IEC 17999
  - 2005 – ISO/IEC 27001 заменя BS7799-2
  - 2007 – ISO/IEC 17999:2005 е преименуван на ISO/IEC 27002:2005

Принципи на информационната сигурност

- Наличност - свойството за достъпност и използваемост на информацията при заявка от упълномощено лице
- Цялостност - свойството за опазване на точността и целостта на информацията
- Конфиденциалност - свойството информацията да не се предоставя или разкрива пред неупълномощени лица, служители или процеси

- Правно съответствие – информацията да се събира, съхранява, обработва и унищожава в съответствие с нормативните актове и договорните отношения

Система за управление на сигурността на информацията (СУСИ)

- Създаване и управление на СУСИ
  - Създаване
  - Внедряване и функциониране
  - Наблюдение и преглед
  - Поддържане и подобряване
- Изисквания към документацията
  - Управление на документите
  - Управление на записите
- Други задължителни елементи
  - Вътрешни одити
  - Преглед от ръководството
  - Коригиращи и превантивни действия

Управление на риска

- Оценка на риска
  - Опис на информационните активи
  - Идентификация на заплахите към активите
  - Оценка на риска на базата на приета методика
    - Количествени методики
    - Качествени методики
  - Доклад за оценката на риска
- Третиране на риска (План за третиране на риска)
  - Намаляване на риска чрез прилагане на подходящи механизми на контрол
  - Приемане на риска
  - Избягване на риска
  - Прехвърляне на риска

Приложение А - контроли

- 11 области, 39 цели по контрола и 133 механизми за контрол
- Области
  - A.5 Политика по сигурност
  - A.6 Организиране на сигурността на информацията
  - A.7 Управление на активи
  - A.8 Сигурност на човешките ресурси
  - A.9 Физическа сигурност и сигурност на заобикалящата среда
  - A.10 Управление на средствата за информация и операциите
  - A.11 Контрол на достъпа
  - A.12 Придобиване, разработване и поддържане на информационните системи
  - A.13 Управление на инциденти със сигурността на информацията
  - A.14 Управление на непрекъснатостта на дейността
  - A.15 Съответствие
- Избор и внедряване на механизми за контрол
  - ISO 27002 съдържа добри практики за имплементиране на различните механизми за контрол
  - Организациите избират свои контроли на базата на оценката на риска, които да покрият изискванията на стандарта
  - Избраните механизми за контрол се описват в Декларация за приложимост
- Видове контроли – организационни, технически и физически

Разработване, внедряване и сертификация

- Определяне обхвата на СУСИ
- Методика за оценка на риска
- Опис на активите и оценка на риска
- Разработване на документацията на СУСИ
- Внедряване
- Вътрешен одит
- Преглед от ръководството
- Сертификационен одит
  - Извършва се от акредитирани организации
  - Етап 1 – преглед на документацията
  - Етап 2 – същински одит

Наредба за оперативна съвместимост и информационна сигурност

- Сертификация и одит на администрациите в съответствие с международния стандарт ISO 27001:2005
- Преносимост на всички данни в информационните системи в случаи на непредвидени обстоятелства
- Политиката за мрежова и информационна сигурност
  - Достъпност, автентичност, цялостност и конфиденциалност
- Вътрешни правила за мрежовата и информационната сигурност като Система за управление на информационната сигурност (СУИС)
- Сертификация на СУИС по смисъла на ISO 27001:2005
- Съвет за мрежова и информационна сигурност на ИС
  - Постоянно действащ консултативен орган
  - Предлага препоръчителни управленски мерки за предотвратяване на инциденти
- Оценка и управление на риска
  - Според т. 4.2.1 от ISO 27001:2005
  - Потенциалните рискови фактори от ISO 13335:2000 (ISO 27005)
  - Методика за оценка на риска - Приложение №3

Наредба за оперативна съвместимост и информационна сигурност

- Национален център за действие при инциденти
  - Актуална информация за всички опити за проникване на нежелан софтуер в информационните системи (ИС)
  - Незабавно уведомяване при възникване на инцидент
  - Мониторинг на събитията и инцидентите
    - Според т. 4.2.3 от ISO 27001:2005
  - План за действие с цел осигуряване непрекъсваемост на дейността
- Нива на защита от неправомерен достъп
  - 0 или D (най-ниско), 1 или C, 2 или B, 3 или A (най-високо)
- Срокове за изпълнение
  - В срок от 3 месеца - попълване на Регистъра на стандартите
  - В срок от 12 месеца - разработване на вътрешни правила и извършване на сертификацията им като СУИС по ISO 27001:2005
  - В срок 24 месеца - провеждането на одит от оторизирана независима организация за признаване на съответствие между СУИС и международния стандарт ISO 27001:2005

Въпроси