Стандарти за качество

ИЛИНА МАНОВА

РИЛА СОЛЮШЪНС

Съдържание

Стандарти и софтуер

Сертификационни организации и процес на сертификация

Популярни стандарти
- ISO 9000
- ISO 27000
- ISO 20000 (ITIL)

Нови предизвикателства – GDPR / Регламент (ЕС) 2016/679

Система за управление на качеството, базирана на стандарти

Сертификационни организации и процес на сертификация

Дейности по стандартизация

- Консултации за разработка и внедряване на системи за управление на качеството
- Обучения на одитори и сертификация на одитори
- Сертификационни одити и сертификация на организации (на базата на определени акредитации)

Друго:

- Принцип – една сертификационна организация не може да консултира и да сертифицира една и съща организация
- Съответствието на Система за Управление на Качеството (СУК) се проверява посредством Одит.
- Съществуват каталози с информация на сертифицираните фирми – пример http://www.club9000.org/bg/ISO9001-Certified-Firms.php

Акредитация

Всяка държава има **един единствен** орган за акредитация

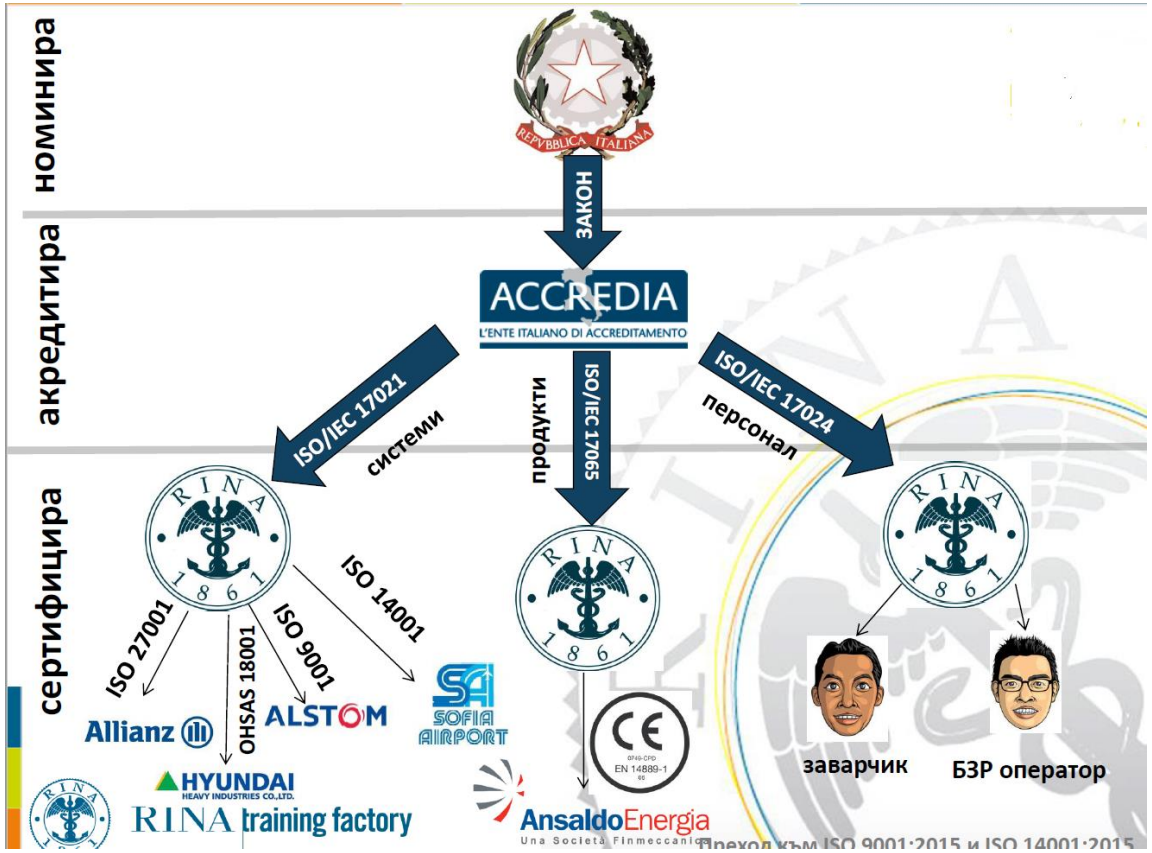
Органът по акредитация се определя със **закон**, **декрет** или **указ**

Органът е с **идеална цел** в полза на обществото

Основни функции:

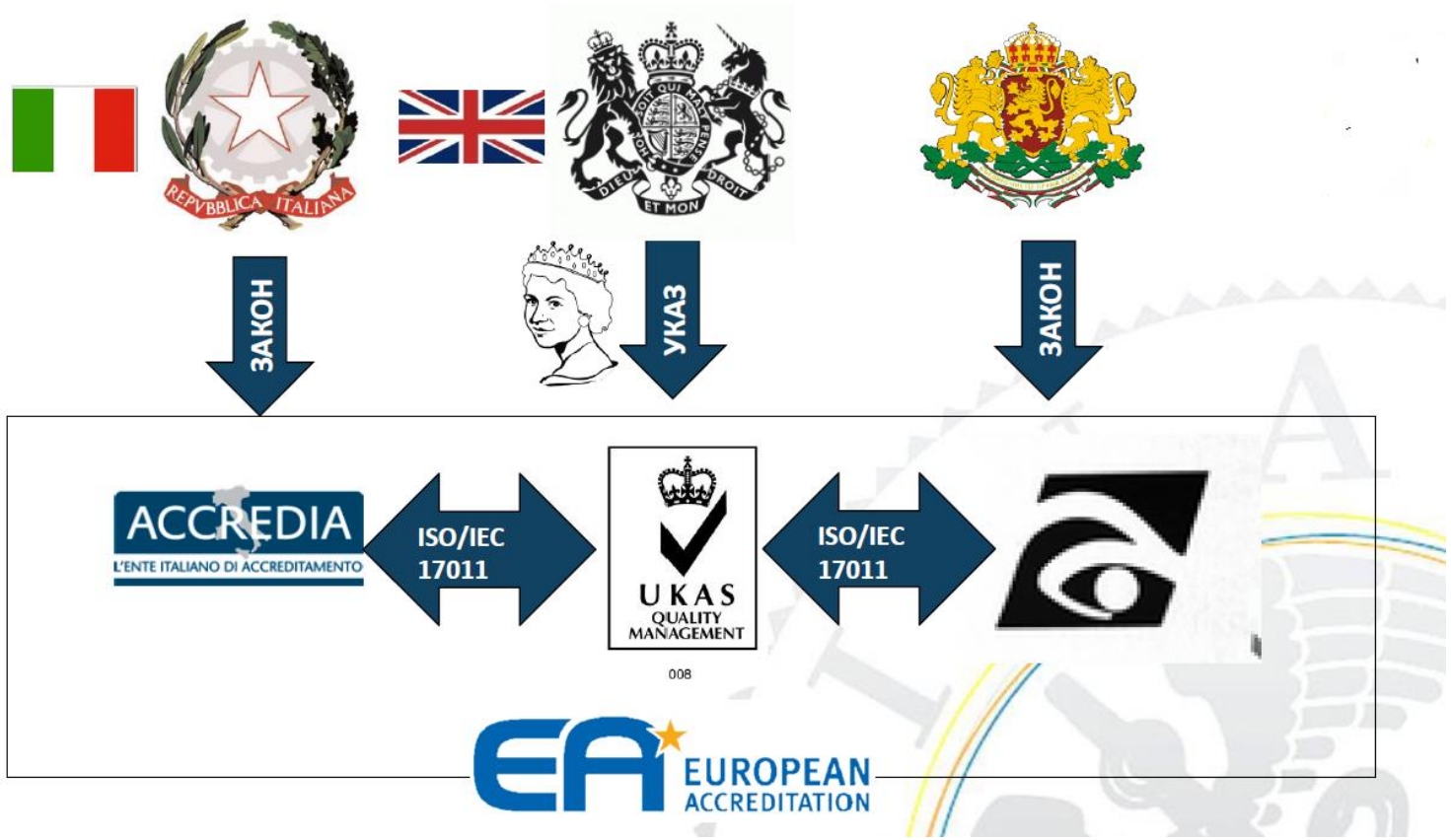
- мониторинг на пазара;
- осигуряване на безопасни продукти и услуги;
- оценка на техническата компетентност на органите за оценка;
- осигурява безусловно признаване на държавно ниво.

Пример за йерархия в стандартизацията



Примерът е предоставен от RINA Bulgaria

Акредитационните органи се проверяват взаимно



Проверка за съответствие към определен стандарт – чрез одити

Външни одити (сертификационни, ре-сертификационни, междинни)

- От сертифициращата организация
- На фиксирани периоди по зададен план, преглежда се внедрената СУК за съответствие спрямо декларираните клаузи на стандарта

- Вътрешни одити
  - Извършват се на регулярен период – по статична структура на организацията и по процеси, приложени в актуални проекти – от вътрешни одитори. Вътрешните одити са планирани дейности в СУК на организацията. Вътрешните одитори трябва да притежават сертификат за одитор за съответния стандарт.

ISO 9001
Еволюция на стандарта

ISO 9001:2015

Основен стандарт при разработката на система за качество (СУК) в дадена организация, налага процесен подход за описание на дейностите и релациите между тях (http://sertifiointi.com/wp-content/uploads/2014/06/ISO-9001-2015-Draft.pdf)

Стандартът се основава на следните основни принципи, които гарантират успешно ръководене и функциониране на една организация:

- насоченост към клиента;
- лидерство;
- приобщаване на персонала;
- процесен подход;
- подобряване;
- взимане на решение, основани на доказателства;
- управление на взаимоотношенията.

ISO 9001:2015 Базова структура

ISO 27001:2013

Дефинира изисквания към Системите за управление на сигурността (ISMS) на информацията, те се развиват в интеграция (надграждане) към системите по ISO 9001

Основна цел е гарантирането на **поверителността, цялостност и наличността** на информацията в дадена компания.

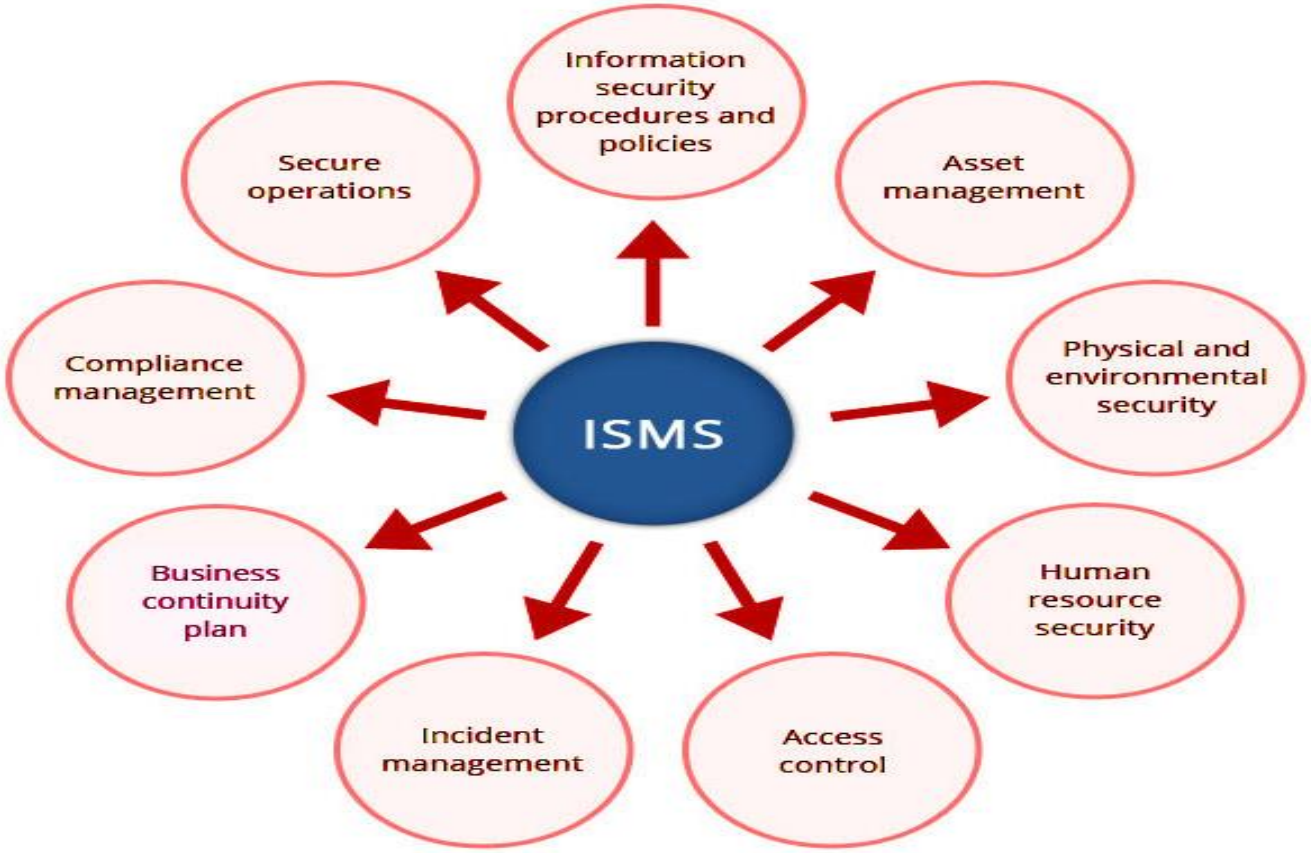
Гарантира **непрекъсваемост** на бизнес процесите в дадена организация, които се отнасят до сигурността на данните

Полезен лин за въведение в стандарта

- https://iapp.org/media/presentations/14Symposium/CS14_Introduction%20to%20ISO.pdf

Приложение на стандарта

Дейности



ISO 20000

Този стандарт надгражда съществуваща СУК по 9001

ISO/IEC 20000, Информационни технологии – Управление на услугите, е разработен с цел да се повиши качеството на услугите в IT сектора. Стандартът се базира на стандарта BS 15000 и **ITIL** и е разработен в две части:

- **ISO/IEC 20000-1 Информационни технологии. Управление на услуги. Част 1: Изисквания относно системата за управление на услуги -** Съдържа изискванията за управление на IT услугите и се отнася за тези, които отговарят за внедряването и поддържането на Системата за управление на IT услугите;
- **ISO/IEC 20000-2 Информационни технологии. Управление на услуги. Част 2: Кодекс за добра практика - на IT услугите.** Ръководство за подобряване на услугите и одитиране на Системата за управление

Полезен линк

https://advisera.com/20000academy/free-downloads/

Основни процеси

РЕГЛАМЕНТ (ЕС) 2016/679 General Data Protection Regulation (GDPR)

Ще бъде задължителен от пролетта на 2018

Отнася се до защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни

Правен аспект и IT решения (надграждат ISO 27001)

Регламентира хармонизирането на законодателството на ЕС по отношение на надеждността на сигурността при свободното движение на потоците от лични данни

За допълнителна информация

https://www.itgovernance.eu/eu-general-data-protection-regulation-gdpr?gclid=EAIaIQobChMI37yej5yC2AIV4bDtCh2wnwmoEAAYASAAEgJoKPD_BwE

Система за управление на качеството / Quality Management System (QMS)

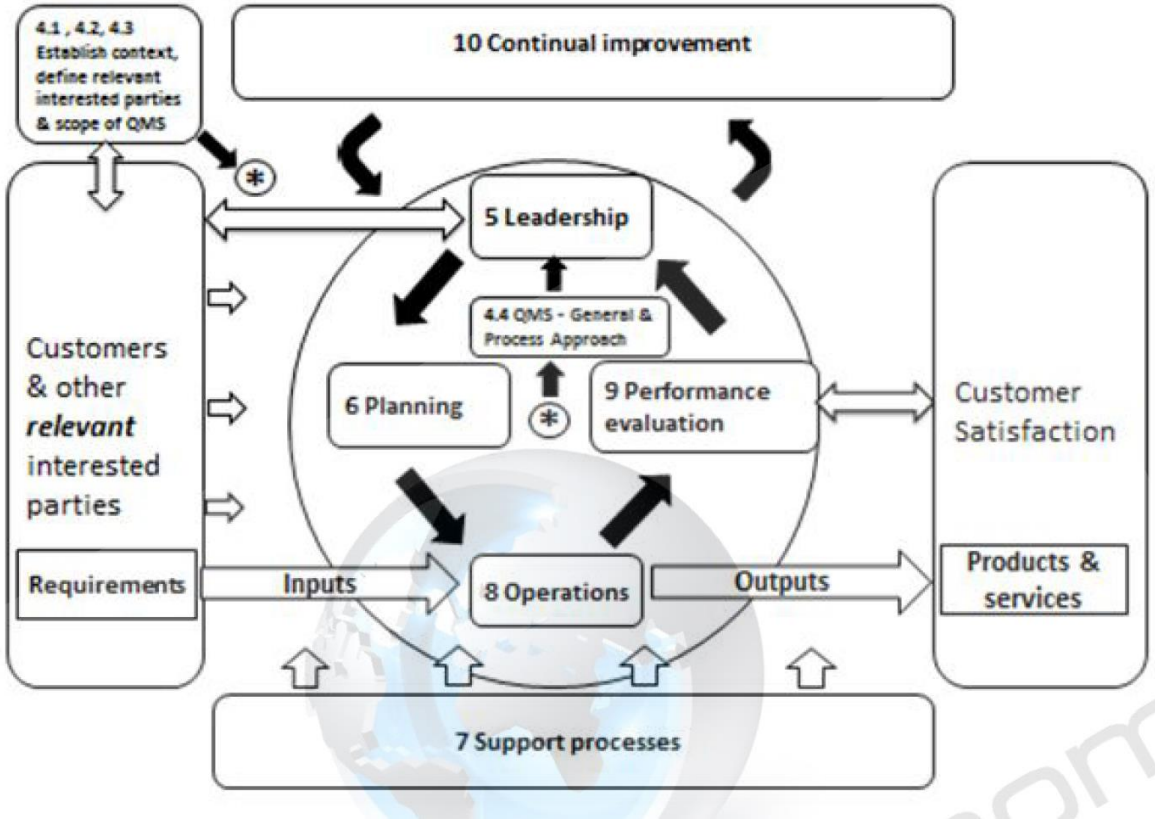
- За софтуерни фирми: Най-често стартират със СУК, които са в съответствие с ISO 9001, след което те се надграждат с ISO 27001 и ISO 20000
- Ако се разработват приложения, третиращи лични данни – ще трябва да се приложи и GDPR
- Реализират се като WEB базирани системи. Добрата практика е всеки да има достъп до частта, която го засяга в зависимост от неговата роля/длъжност
- Целта е да се работи с унифицирани процеси на ниво Организация, които са допълнени с богат набор от шаблони (templates) – така се постига оптимизация на софтуерната разработка
- Средата за управление и реализация на проектите е контролирана
- Има ясно дефинирани точки за контрол на изпълнението на проектите / на фирмените цели, което подобрява управлението на риска
- Има ясно дефинирани правила за управление на ресурсите, включително и HR
- Дават се правила за сигурност – на ниво фирмени активи и активи на подизпълнители и клиенти
- Регламентират се комуникационните процедури с Клиентите, което повишава взаимното доверието

Примерна структура на СУК (ISO 9001&ISO 27001 & ISO 20000)

Основни процеси

- Управление на основния процес за разработка – класически, гъвкав..
  - Включва описание на основния работен поток, тригери за преход, шаблони, роли и отговорности, отчетност
  - Управление на качеството – QA & QC
  - Механизъм за управление на Риска
  - Механизъм за Управление на промените
  - Среда за разработка и управление на проекти, софтуерни инструменти
- Поддръжка на разработения софтуер
- Управление на човешките ресурси – назначения, обучение, кариерно развитие
- Управление на клиентите
- Управление на доставките

Процесите в единна СУК /QMS (Quality Management System)



Структура на СУК - продължение

Технически процедури
- Управление на средствата за измерване (testing tools)
- Управление на информацията (код и документация)
- Управление на конфигурации
- Технически инспекции
- ……

Политики, процедури и планове по сигурността
- План за непрекъсваемост на бизнес процесите
- Процедура за управление на инциденти
- ……..

Защита на лични данни

Записи по сигурност
- Опис на активи, Контроли

Пример – Политики по сигурността в СУК на софтуерна фирма

Категория: *Политики по сигурност на информацията*

15. **Р-01 Допустимо използване на активи**
16. **Р-02 Контрол на достъпа**
17. **Р-03 Резервиране на информацията**
18. **Р-04 Чисто бюро и екран**
19. **Р-05 Сигурен код**
20. **Р-06 Политика (Декларация) по Информационна сигурност**
21. **Р-07 Управление на паролите**
22. **Р-08 Информационни системи**
23. **Р-09 Физическа сигурност**

Примерен въпрос за тест по темата

Стандартът, който регламентира управлението на услуги в IT сектора е:

A) ISO 9001

B) ISO 27001

C) ISO 20000- верен отговор.

D) ISO 14001

Приложения
Приложение 1 / 7 принципа в ISO 9001
1. Customer focus

- Understand the needs of existing and future customers
- Align organizational objectives with customer needs and expectations
- Meet customer requirements
- Measure customer satisfaction
- Manage customer relationships
- Aim to exceed customer expectations

2. Leadership

Establish a vision and direction for the organization

Set challenging goals

Model organizational values

Establish trust

Equip and empower employees

Recognize employee contributions

3. Engagement of people

Ensure that people's abilities are used and valued

Make people accountable

Enable participation in continual improvement

Evaluate individual performance

Enable learning and knowledge sharing

Enable open discussion of problems, constraints

4. Process approach

Manage activities as processes

Measure the capability of activities

Identify linkages between activities

Prioritize improvement opportunities

Deploy resources effectively

5. Improvement

Improve organizational performance and capabilities

Align improvement activities

Empower people to make improvements

Measure improvement consistently

Celebrate improvements

6. Evidence-based decision-making

Ensure the accessibility of accurate and reliable data

Use appropriate methods to analyze data

Make decisions based on analysis

Balance data analysis with practical experience

7. Relationship management

Identify and select suppliers to manage costs, optimize resources, and create value

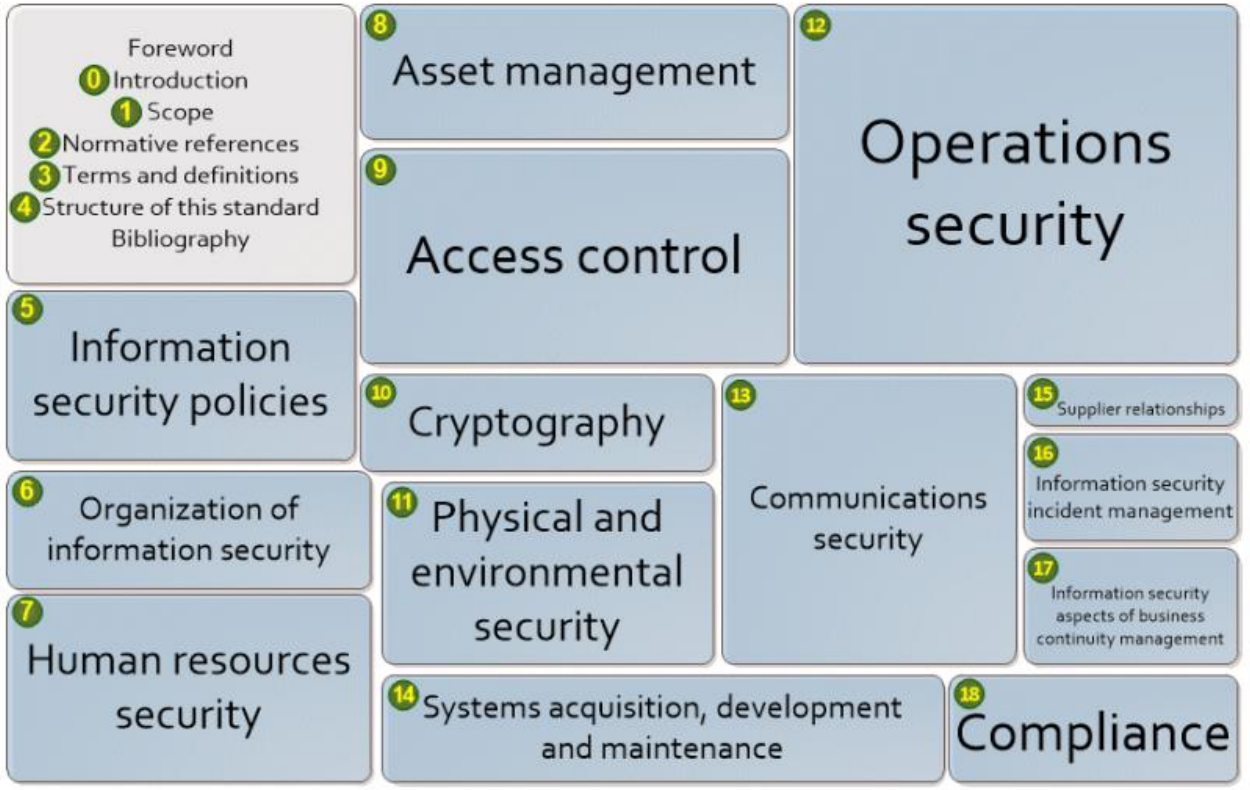
Establish relationships considering both the short and long term

Share expertise, resources, information, and plans with partners

Collaborate on improvement and development activities

Recognize supplier successes

Приложение 2 / Структура на ISO 27001



ISO 27001 – сертифициране по региони