# Практика внутреннего аудита СМИБ

Алексей Евменков, CISM

isqa.ru

2018-04-20

# О чем разговор

- Ключевые знания, необходимые для внутреннего аудитора СМИБ
- Требования ИСО 27001/ИСО 19011 и внешних органов сертификации – к процессу, к аудиторам
- Организация процесса внутр. аудита – процедуры, инструменты
- Практические особенности проведения аудита

isqa.ru Information Security

# Представление

- Специалист по **ИБ** (CISM), по **процессам** и качеству в ИТ области
- Практический опыт по подготовке к сертификации **ИСО 27001 и 9001**
- Профессиональный **аудитор** по ИБ и процессам
- Веду блог по ИБ и процессам [isqa.ru](isqa.ru)

IS SOFT

# Теория по внутреннему аудиту СМИБ

# Кто такой внутренний аудитор СМИБ

Внутренний аудитор СМИБ – тот, кто знает как должны работать эти требования

## Требования ИСО 27001

**9.2 Внутренний аудит**

Организация должна проводить внутренние аудиты через запланированных интервалы времени, чтобы получать информацию о том,

a) соответствует ли система менеджмента информационной безопасности

1) собственным требованиям организации к ее системе менеджмента информационной безопасности; и

2) требованиям Настоящего Международного Стандарта;

b) что система менеджмента качества результативно внедрена и функционирует.

Организация должна:

c) планировать, выполнять и управлять программой(ами) аудитов, включая периодичность их проведения, методы, ответственность, требования к планированию и отчетности. Программа (ы) аудитов должна учитывать значимость проверяемых процессов и результаты предыдущих аудитов;

d) определить критерии и область аудита для каждой проверки;

e) выбирать аудиторов и проводить аудиты так, чтобы гарантировать объективность и беспристрастность процесса аудита;

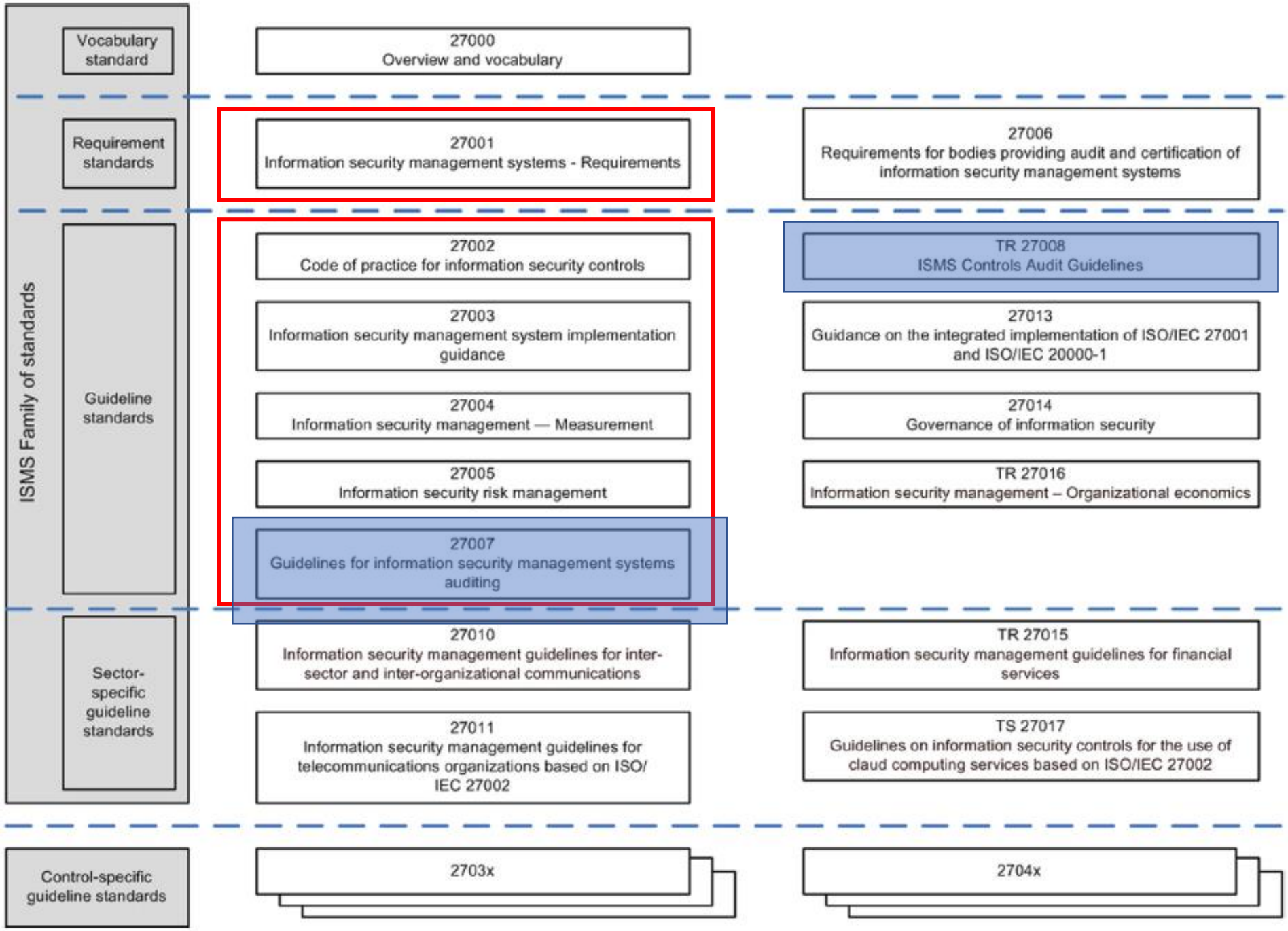
f) гарантировать, что результаты аудитов переданы на соответствующие уровни управления для оценки,

g) сохранять программу аудита и его результаты как документированную информацию.

# Что должен знать аудитор

- Терминология ИБ, ИСО 27001, 27002, 19011 и др.
- СМИБ – как строить, как эксплуатировать
  В идеале – бывший/практикующий ИБэшник
- Все основные процессы СМИБ: управление рисками, инцидентами, аудитами и тд.

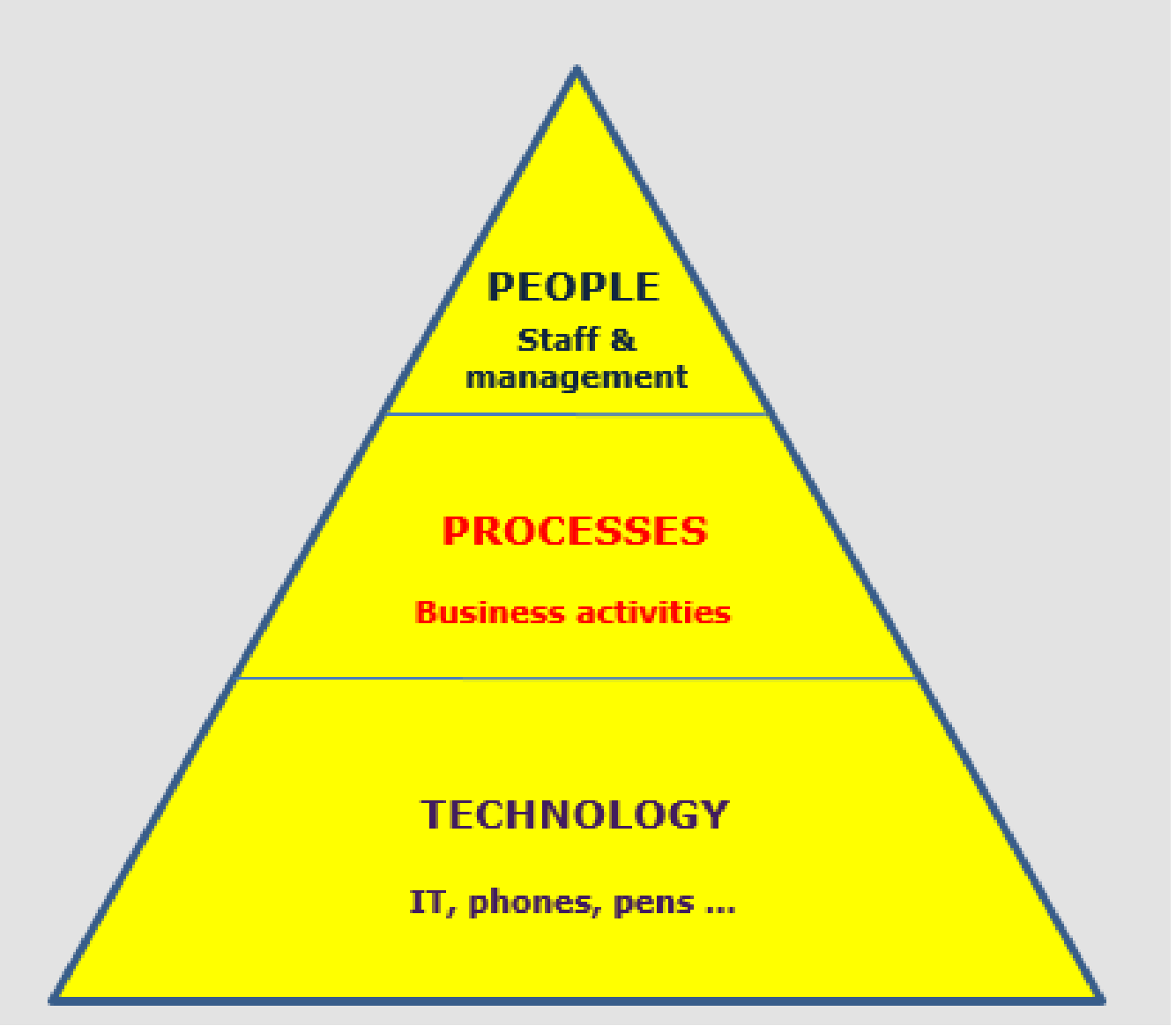
isqa.ru
Information Security



# Замечание о важности аудитов СМИБ

- В (ИТ) безопасности важнее всего конечно же.. Люди

- Важность процесса аудирования – п.ч. это непосредственная работа с людьми:
  - обучение,
  - разбор практических ситуаций
- Через аудит – происходит связь с бизнесом



| ISO 27001 |
| --- |
| 4 Контекст организации |
| 5 Лидерство |
| 6 Планирование |
| 7 Обеспечение |
| 8 Функционирование |
| 9 Оценка результатов деятельности |
| 10 Улучшение |
| **ISO 27002** |
| A.5 Политики информационной безопасности |
| A.6 Организация системы информационной безопасности |
| A.7 Безопасность, связанная с персоналом |
| A.8 Управление активами |
| A.9 Управление доступом |
| A.10 Криптография |
| A.11 Физическая безопасность и защита от природных угроз |
| A.12 Безопасность в период эксплуатации |
| A.13 Сетевая безопасность |
| A.14 Приобретение, разработка и обслуживание систем |
| A.15 Отношения с поставщиками |
| A.16 Управление инцидентами в сфере информационной безопасности |
| A.17 Аспекты информационной безопасности управления непрерывностью бизнеса |
| A.18 Соответствие |

isqa.ru Information Security

- Знание практических особенностей по внедрению каждого пункта стандарта
- Парадокс внутреннего и внешнего аудитора (разная парадигма)
  - Внутренний проверяет на более детальном уровне
- Взаимосвязь между отдельными требованиями (функционирование-оценка-улучшение и тд)

- Вероятно, можно быть аудитором-теоретиком, но и найденные несоответствия будут формальными

| Clause | Description | Documentation Requirements | Implementation Requirements | Audit Requirements |
|---|---|---|---|---|
| **4** | **Context of the organization** | | | |
| 4.1 | Understanding the organization and its context | 'About the Organization' in the IS Policy document | Understand the organization, its nature of business and defining it in the IS Policy document. | Review the IS Policy document |
| 4.2 | Understanding the needs and expectations of interested parties | 'Target Audience' in the IS Policy document | Brainstorming with Management and including it in the IS Policy document. | Review the IS Policy document |
| 4.3 | Determining the scope of the ISMS | 'ISMS Scope' in the IS Policy document | Brainstorming with Management and including it in the IS Policy document. | Review the IS Policy document |
| 4.4 | ISMS | The IS Policy document | • Establishment of IS<br>• Appointment of IS Manager<br>• Conducting IS Trainings and Awareness<br>• Defining RACI | Review the IS Policy document |

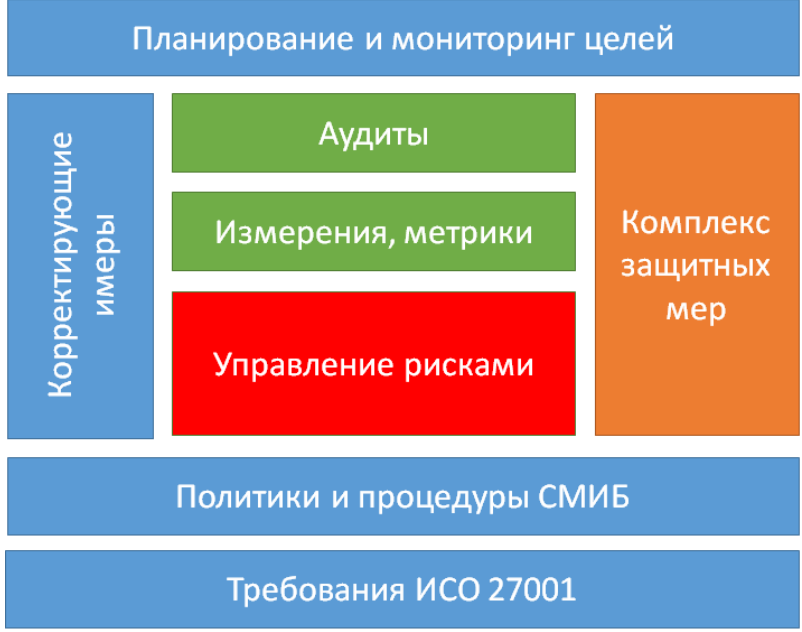
Пример проверочных точек для аудитора

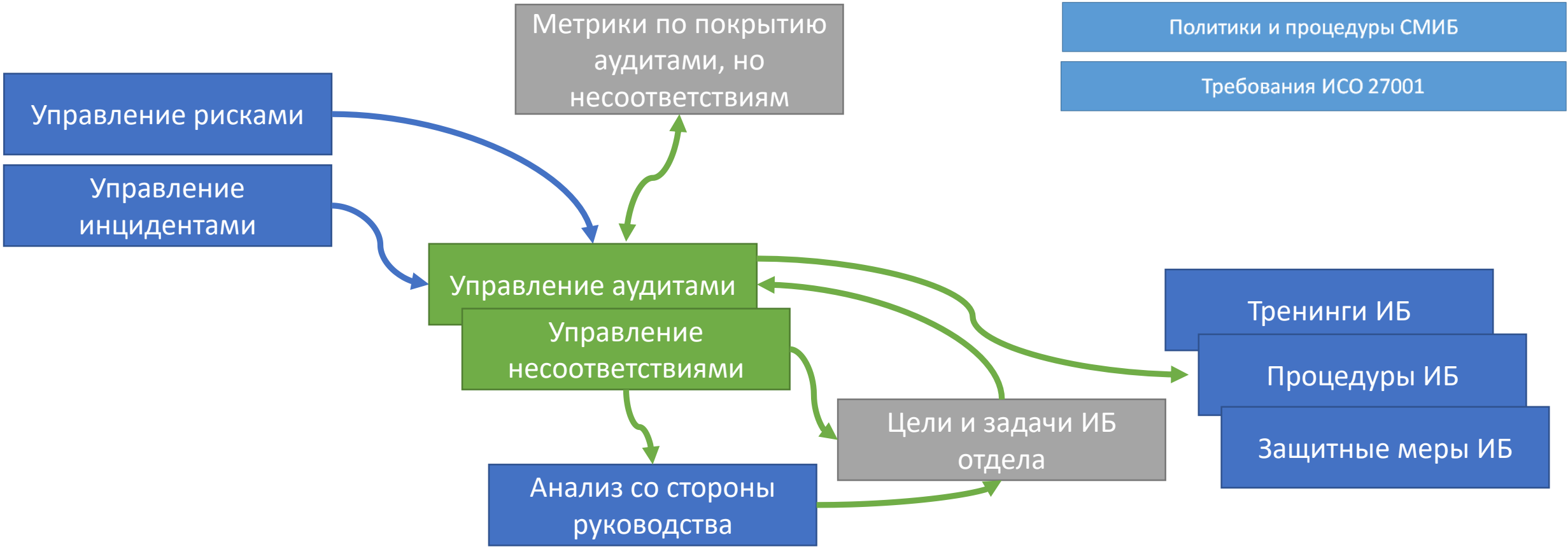
Source: https://www.slideshare.net/uppalaanand/iso-27001-2013-standard-requirements

| Clause | Description | Documentation Requirements | Implementation Requirements | Audit Requirements |
|---|---|---|---|---|
| 7.5.1 | General | All documents identified as necessary by the ISO and Organization | | |
| 7.5.2 | Creating and Updating | • ISMS Documentation Process<br>• Revision/Document History to be included in all ISMS documentation<br>• Document distribution List | Define ISMS Documentation process | • Review ISMS Documentation process<br>• Check for Revision/Document History in ISMS documentation |
| 7.5.3 | Control of documented information | • List of all ISMS related Documents (policies, processes, procedures) and Records (Decisions, Change Records, Communications, Reports, Alerts, Logs)<br>• Data Labeling process (distribution and access)<br>• Data Retention & Archival process<br>• Adding Revision/Document History for all ISMS documents (Labeling, Version control, list of changes) | • Identification and gathering of all ISMS related documents and records<br>• Defining controls for developing and maintaining documented information – including Revision/Document History, labeling, distribution, access, versioning and changes | • Review of ISMS Documents and Records<br>• Review documents labeling, distribution, version and change details |

Information
curity

# Связь процесса Аудитов с другими процессами СМИБ



# Принципы проведения аудита 1/2

- **Целостность.**
  *Является основой профессионализма.*
  - Одинаковые подходы, рассматривать как единое целое
- **Беспристрастное представление результатов.**
  *Является обязательством представлять правдивые и точные отчеты.*
  - Неважно, кого аудируем – начальство, админов..
- **Надлежащая профессиональная тщательность.**
  *Означает приложение усердия (прилежания) и проявление рассудительности при проведении аудита.*
  - Аудит – это тяжелая работа, которую нужно максимально последовательно и скурпулезно сделать

# Принципы проведения аудита 2/2

Если я аудитор, то должен задуматься над этими принципами. Хотя бы раз)

- **Конфиденциальность.**
  *Означает обеспечение безопасности полученной информации.*
  - Все, что сказано на аудите – не должно выйти за пределы (исповедь). Необходимо разделять рабочее и персональное.
- **Независимость.**
  *Это основа беспристрастности при проведении аудита и объективности заключений по аудиту.*
  - Не аудировать себя.
- **Подход, основанный на свидетельствах.**
  *Является разумным способом получения надежных и воспроизводимых заключений по аудиту в процессе систематически проводимых аудитов.*
  - Субъективные заключения должны остаться при аудиторе. В официальный отчет идут только факты, основанные на фактах.

isqa.ru
Information Security

# ISO/IEC 27007:2017 и ISO 19011:2011

- **ISO/IEC 27007:2017** — Information technology — Security techniques — **Guidelines for information security management systems auditing**
- **ISO 19011:2011** Guidelines for auditing management systems

- Одинаковая структура: 27007 повторяет 19011, с доп. разъяснениями

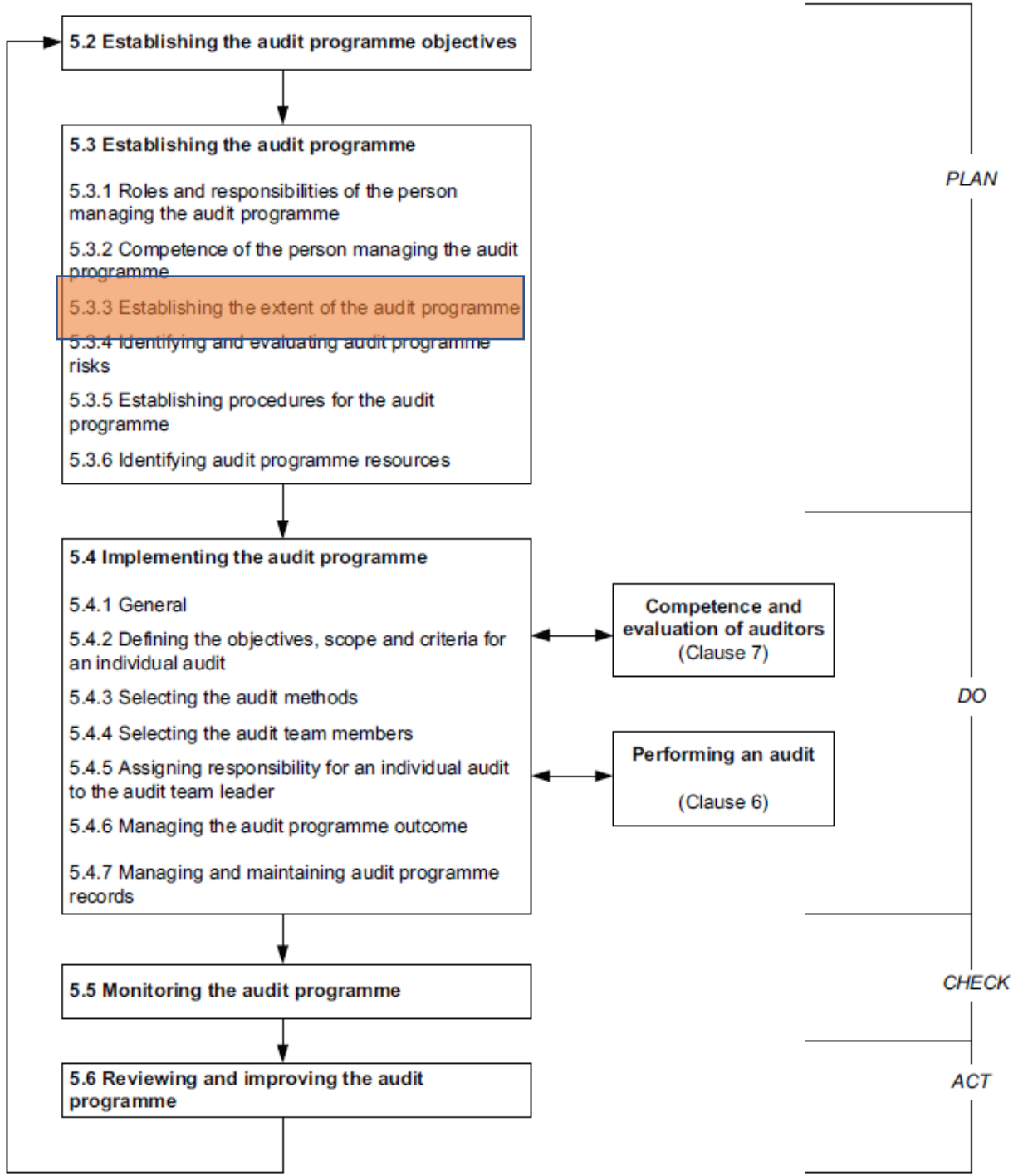
# Структура ИСО 19011


1 Scope ..... 1
2 Normative references ..... 1
3 Terms and definitions ..... 1
4 Principles of auditing ..... 4
5 Managing an audit programme ..... 5
5.1 General ..... 5
5.2 Establishing the audit programme objectives ..... 6
5.3 Establishing the audit programme ..... 7
5.4 Implementing the audit programme ..... 10
5.5 Monitoring the audit programme ..... 13
5.6 Reviewing and improving the audit programme ..... 14
6 Conducting an audit ..... 14
6.1 General ..... 14
6.2 Initiating the audit ..... 15
6.3 Preparing audit activities ..... 16
6.4 Conducting the audit activities ..... 18
6.5 Preparing and distributing the audit report ..... 23
6.6 Completing the audit ..... 24
6.7 Conducting audit follow-up ..... 24
7 Competence and evaluation of auditors ..... 24
7.1 General ..... 24
7.2 Determining auditor competence to fulfil the needs of the audit programme ..... 25
7.3 Establishing the auditor evaluation criteria ..... 29
7.4 Selecting the appropriate auditor evaluation method ..... 29
7.5 Conducting auditor evaluation ..... 29
7.6 Maintaining and improving auditor competence ..... 29
Annex A (informative) Guidance and illustrative examples of discipline-specific knowledge and skills of auditors ..... 31
Annex B (informative) Additional guidance for auditors for planning and conducting audits ..... 37


Насколько полезен ИСО 19011 для бизнеса? Вопрос открытый.

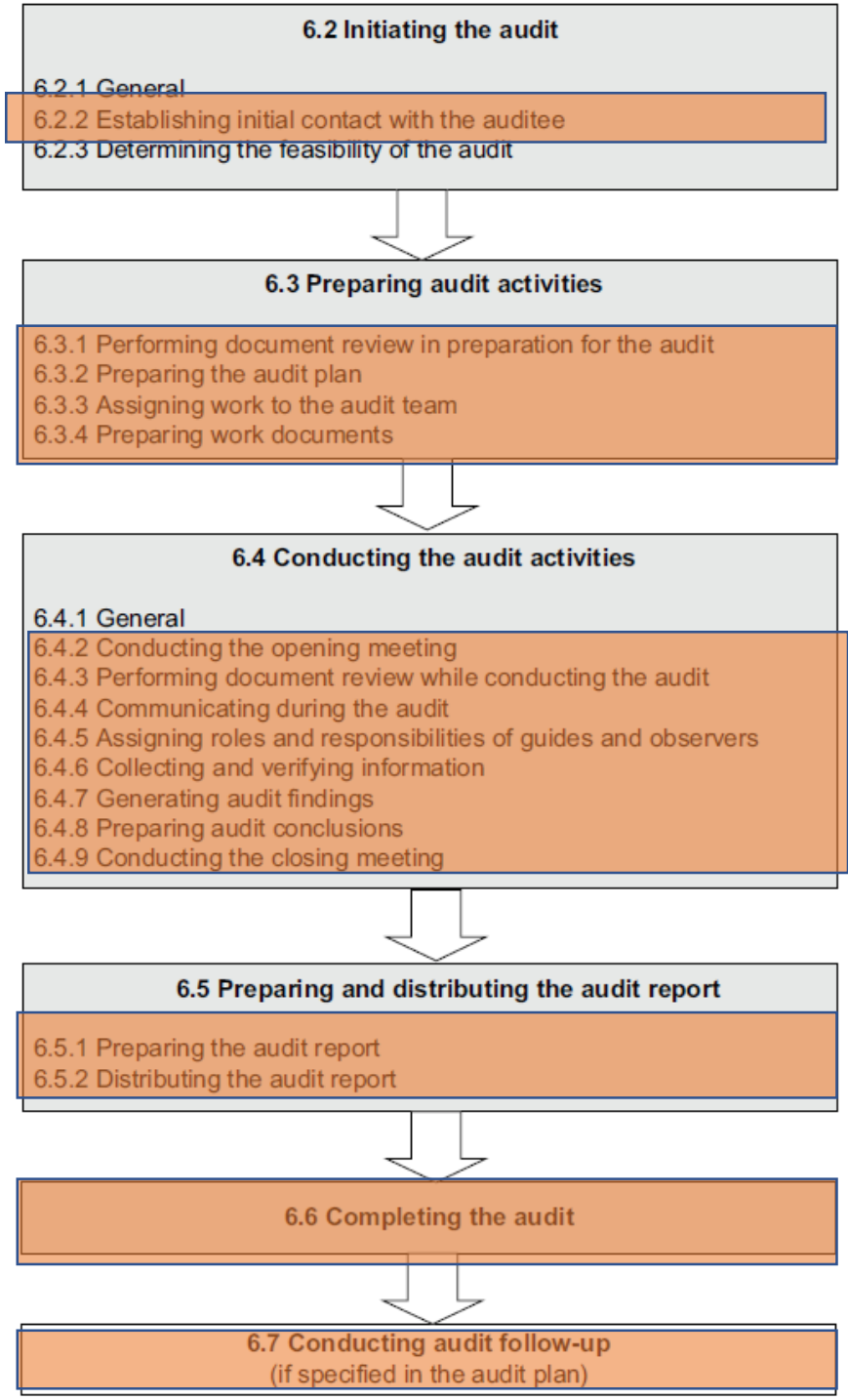
# Управление программой аудита

- Как правило, вначале разрабатывается процедура по аудитам
- Программа аудита разрабатывается согласно требованиям процедуры



# Проведение аудита

- Важны все требования, описанные в стандарте
- Практические особенности см. далее.



# Общий процесс управления аудитами

isqa.ru
Information Security

# Общий процесс аудита

# Ключевые роли

- Ведущий аудитор (Менеджер ИБ)
  - Планирование программы аудита и отдельных аудитов
  - Руководство группой аудиторов и координация действий;
  - Контроль за ведением соответствующих записей по аудиту;
  - Анализ выявленных в ходе аудита СМИБ несоответствий, определение необходимой коррекции и корректирующих действий;
  - Подготовка суммирующего отчета по внутреннему аудиту;
- Аудитор (Инженер ИБ)
  - Доведение до сведения всех сотрудников проверяемого подразделения объекта и целей проверки;
  - Полная и объективная проверка выполнения требований процессов СМИБ сотрудниками компании;
  - Составление отчета по аудиту проверяемого подразделения;
  - Проверка эффективности корректирующих действий, принятых по результатам аудита
- Аудируемые
  - Предоставляют запрашиваемую информацию
  - Исправляют найденные несоответствия

# Программа и план аудитов

- План аудита – план для одного конкретного аудита
  - Например, аудит подразделения Software Testing
  - Может охватывать несколько встреч (если подразделение/проект большой)
- Программа – совокупность планов аудитов, для достижения определенной цели
  - Обычно составляется на год,
  - Основная часть – график аудитов

# Разработка Программы аудита

- Установление объема программы аудита (п.ч. всех не проаудируешь)
  - Классическое правило покрытия 25% бизнеса
  - Например, на отдел в 20 человек – проводится 1 аудит для проекта с командой в 3-5 человек.
  - На отдел в 50 человек – берется 2 проекта с командой в 3-5 человек.
- Разработка процедур, выявление ресурсов – заранее продумываем
  - График аудитов, способы коммуникации, безопасность данных
  - Пост аудит активности – отчеты, коммуникации и др.
  - Физическое расположение, конфрумы и др.
- Учет результатов прошлого цикла при планировании нового цикла аудитов в рамках программы аудита
- Учет потребностей и ожиданий заинтересованных сторон ;
- Отбор членов команды
  - Компетентность аудиторов, способность следовать принципам аудита
  - Сложность аудита (сколько людей приглашать)

Инструментальная поддержка:

- обычный эксель, или
- дашборд в JIRA (состоящий из отдельных аудитов)

# Разработка Плана аудита

- Содержит информацию (пример):
  - Аудируемое подразделение
  - Руководитель подразделения
  - Список аудируемых
  - Список аудиторов
  - Дата, время, место проведения аудита
  - Ссылка на чеклист с предполагаемыми вопросами
  - Общее описание – что будет аудироваться

Инструментальная поддержка:
- обычный эксель, или
- тикет в JIRA (состоящий из набора требуемых полей)

# Перед тем, как начать аудит

- Предварительный контакт с аудируемыми
  - Информировать о цели, объеме, графике аудита; услышать пожелания
  - Получить доступ к требуемым материалам
- Предварительный анализ документации
  - Планы проектов, записи отделов
- Завершение подготовки плана аудита – чеклист сделанного
  - Команда сформирована,
  - Приглашения на встречи высланы
  - Рабочие документы (чеклисты) готовы,
  - Карточка аудита заполнена

Правило: аудит никогда не должен мешать бизнесу!

# Проведение аудита

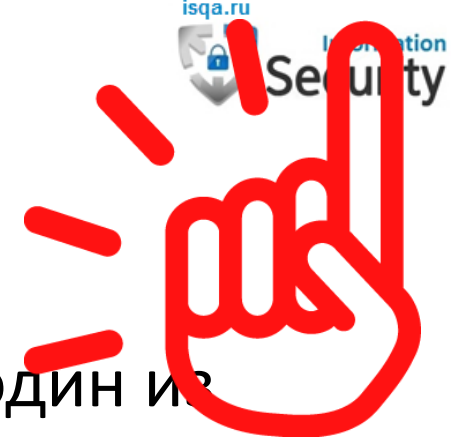
Мало кто использует мощь вступительного слова. Создание правильной атмосферы – начинается именно с вступления

- Вступительное слово\совещание
  - Представление друг другу
  - Объяснить цель аудита, последовательность действий, ожидаемые результаты
- Проведение аудита - методы сбора информации
  - Интервью (наиболее часто)
  - Наблюдение за деятельностью (попросить показать операцию)
  - Анализ документов и записей
- Формирование результатов аудита
  - Список несоответствий, заполненный чеклист, заключение
- Заключительное слово\совещание

# Практические аспекты проведения аудита

- Открытая атмосфера
  - Доброжелательность, убирание барьеров, желание помочь
  - Презумция невиновности – мы настраиваемся что все отлично функционирует)
  - Мы делаем общее дело (улучшение, оптимизация)
  - При планировании нужно заложить время на создание атмосферы
- Энергия?
  - Дружелюбность, искренность, эмпатия, честность, открытость
  - И энергичность (пример унылого аудитора:)

# Убрать страхи



- Аудитор – воспринимается как экзаменатор, угроза.
- Показывать что пишешь (в зависимости от ситуации, но это один из мощнейших сближающих факторов)
- Рабочее место сотрудника – его дом, возможно это идеальное место для аудита
- Вложить максимум – доказать что ты пытаешься дать объективную оценку, а не ищешь несоответствия (мы делаем общее дело).
- Показать – мы аудируем процессы, деятельность, а не людей.
  - Не обсуждать/оценивать людей, не поддерживать подобные разговоры
- Не «показывать свою эрудицию», не надмеваться
  - Фразы вроде «Это же всем известно», «На самом деле…»

# Практические аспекты проведения аудита

- Время
  - Не приходить слишком заранее – чтобы не думали что пришел подловить
  - Не нарушать привычный режим дня!
    Учитывать обед, перерывы. Не стоит начинать с самого утра, после раб.дня.
- Физическое расположение
  - Избегаем противосопоставления (идеально – круглый стол)
  - Сохраняем личное пространство
  - Рукопожатие? Для нашей культуры важно
  - Удобство для участников, расслабленно-рабочая атмосфера, чай и тд.
- Визуальный контакт
  - Для нашей культуры важен.
  - В некоторых культурах является признаком неуважения

isqa.ru
Information Security

# Язык телодвижений

Вообще это не оч. практично.
Цель – как можно быстрее понять в какую сторону «двигать» атмосферу

- Язык телодвижений – поза, жесты, выражение лица
  - Важный канал сообщений
  - Расхождение между словами и языком тела?
  - Взгляд вправо/влево? Смотрите сериал Обмани меня)
  - Возможно, имеет смысл пройти обучение
- Невербальный язык
  - скорость речи, громкость, мягкость речи, покашливание…
  - Говорит о неуверенности…

Рис. 51. *Прикрытие рта рукой*

Рис. 70. *Демонстрируется чувство превосходства.*

Рис. 67. *Стандартный жест - скрещенные руки на груди.*

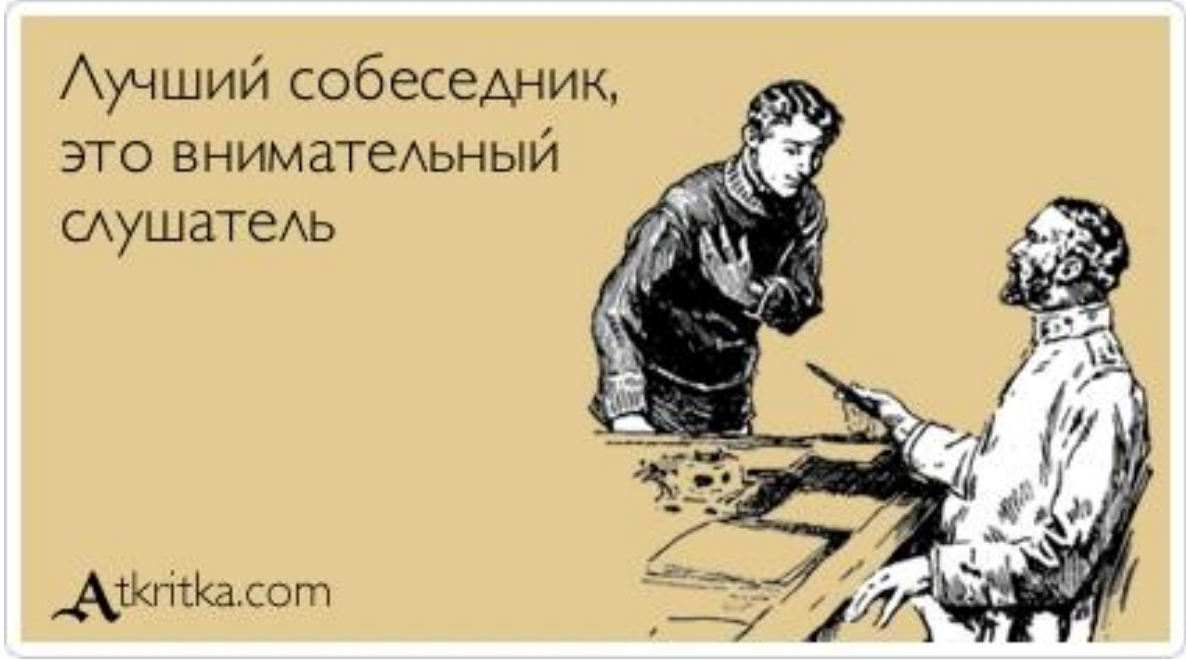
Рис. 56. *Оттягивание воротничка.*

Рис.37. *Сцепленные пальцы рук в поднятом положении.*

Рис.38. *Среднее положение сцепленных рук*

# Исскуство слушать

- Слушать чтобы слышать, достижение ясности
- Привносить комфорт для аудируемого, возможность открытого общения, получения конфиденциальных данных
- Как?
  - Убрать отвлекающие факторы
  - Не выносить преждевременных суждений (аудит =сбор)
  - Ясность – суммируй и повторяй
  - Думаем в 4 раза быстрее чем говорим – поэтому используй преимущество
- Должен быть разговор, а не допрос




Не стоит:

- Отвлекаться, не смотреть на собеседника
- Обдумывать планы пока слушаешь)
- Эмоционально реагировать на личное..

# Вопросы

В том то и искусство аудитора – правильные вопросы

Как остановить беспрерывно болтающего аудируемого?)

- Использование чеклистов
  - Это направляющие, не догма
  - Не обязательно пройти все пункты чеклиста.
  - И не обязательно ограничиваться чеклистом
- Использование вопросов
  - Открытые вместо закрытых (и наоборот)
  - Не должны предполагать ответ
  - Не должны содержать эмоциональных слов или намеков
  - Никогда не задавать вопросы, могущие враждебно настроить (после этого амба)
- Баланс в вопросах
  - Контролирование «болтовни»
  - Отслеживание времени, не позволять тратить впустую
  - Использование «покажите мне», для разговора по делу

# Окончание аудита

- Рекомендуется выделить время – посетить рабочее место
  - Показать/проверить/уточнить выясненные во время аудита факты
  - Увидеть контекст работы
- Не задерживать!
- Заключительное слово
  - Не испортить сделанную работу – неосторожным словом, суждением
  - Описать последующие события – отчет, работа с несоответствиями и тд

# По результатам аудита

- Заполненная карточка аудита, содержащая
  - Ссылку на заполненный чеклист
  - Кол-во несоответствий
  - Заключение и комментарии аудитора
- Набор согласованных несоответствий
  - ! Сами несоответствия, их сроки обычно согласовываются во время аудита
- Проверка устраненных несоответствий – отдельная тема

# Мониторинг и контроль

- Анализ найденных несоответствий, подготовка отчета для руководства (в рамках анализа со стороны руководства –
- В отчет входят:
  - Топ несоответствия
  - Детальная статистика по несоответствиям
  - Тренды по несоответствиям, рекомендации по превентивным мерам
- Анализ результатов предыдущих аудитов, подготовка к следующему циклу аудитов


# Ложный успех аудита

Формальные вопросы,
формальные ответы,
формальные результаты

# Работа с несоответствиями

# Термины

- **Несоответствие** - невыполнение установленных требований;
- **Коррекция** - действие, предпринятое для устранения обнаруженного несоответствия.
- **Корректирующее действие (КД)** – действие, предпринятое для устранения причины обнаруженного несоответствия или другой нежелательной ситуации. Другими словами, корректирующие действия направлены на предотвращения нежелательного события повторно;

# Анализ несоответствий

- Рекомендованная последовательность анализа:
  1. Анализ причины несоответствия (с помощью инструментов RCA)
  2. Разработка **Коррекции**
  3. Разработка **Корректирующего действия**
- После анализа - регистрируем в системе управления аудитом (JIRA?)
- Во время анализа необходимо использовать инструменты/подходы по RCA
  - Во время анализа необходимо использовать инструменты/подходы по RCA
  - Аудитор при анализе следует убедиться, что предоставлены документация и **объективные свидетельства**, касающиеся всех трех частей – и коррекции, и анализа причин, и корректирующих действий, и что они являются релевантными

# Анализ коренных причин (RCA)

- Шаг 1. Соберите информацию о проблеме
  - Метод 5W 2H
- Шаг 2. Определите факторы повлиявшие на появление проблемы
  - Ответы на вопросы:
    - Какая последовательность событий привела к этой проблеме?
    - Какие условия позволили данной проблеме появиться?
    - Какие сопутсвующие проблемы взникли вместе с обсуждаемой центральной проблемой?
  - Диаграмма Ишикавы (“Рыбья кость”)
  - Метод 5 Почему
- Шаг 3. Разработайте корректирующие действия

# Метод 5 Почему - пример

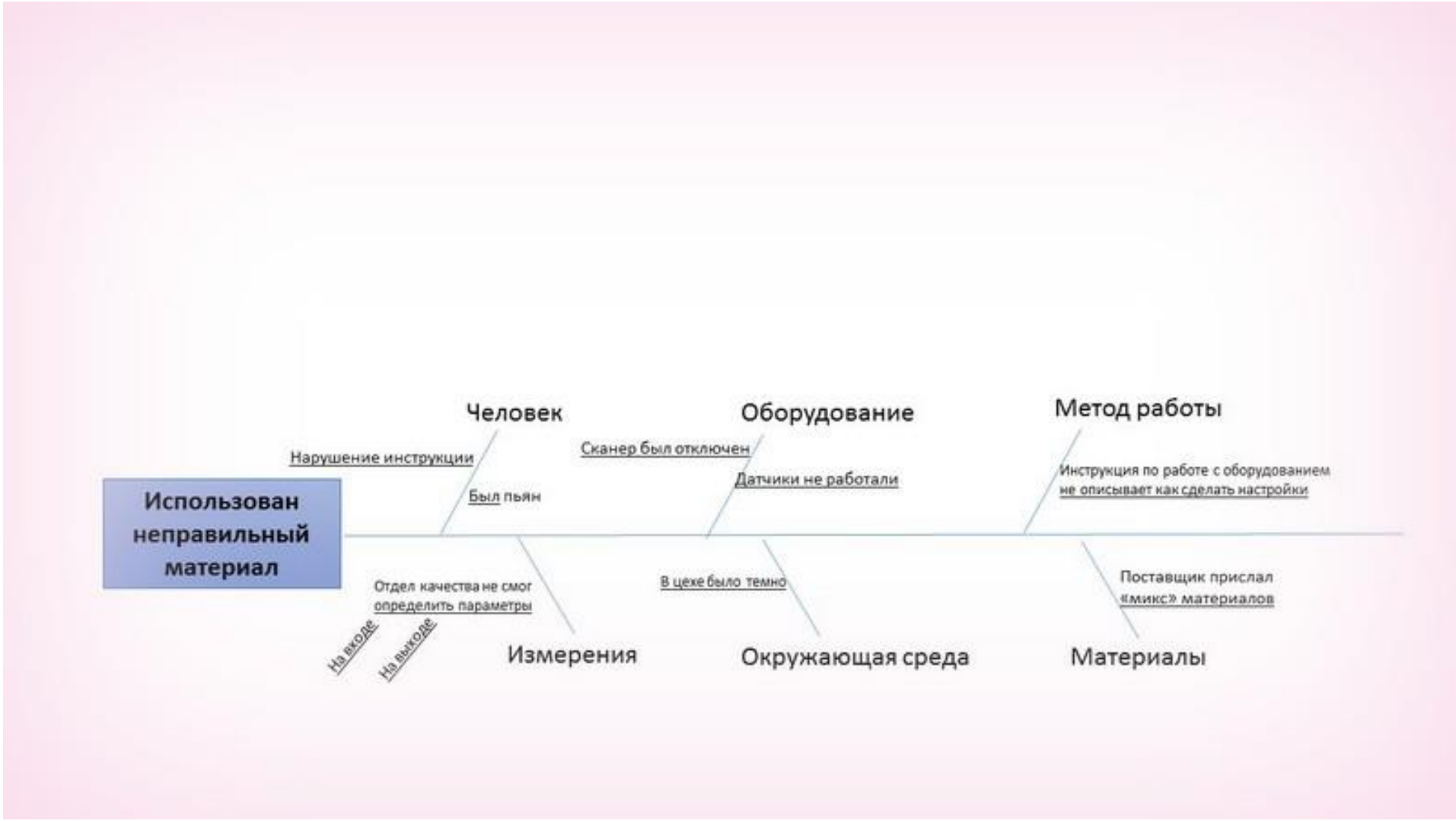
isqa.ru
Information Security

| Почему? | Потому что |
|---|---|
| Несоответствие – Почему вирус попал в компьютер? | Потому что компьютер не был защищен от вируса! |
| Компьютер не был защищен от вируса? | Не установлена антивирусная программа! |
| Не установлена антивирусная программа? | Не определены ответственные за установку и обновление антивирусной программы в организации |
| Не определены ответственные за установку и обновление антивирусной программы в организации? | Данный процесс не формализован в организации и не определены необходимые ресурсы и персонал для его реализации! |
| Данный процесс не формализован в организации и не определены необходимые ресурсы и персонал для его реализации? | Процесс обслуживания компьютерной техники не определен в рамках организации! |

isqa.ru
Information Security

# Диаграмма Ишикавы (“Рыбья кость”)

- Факторы влияющие на проблему
- Возможные причины
- Анализ диаграммы



# Мониторинг несоответствий

- Необходимо определить подход
  - Частота проверки
  - Кто?
  - Каким образом?
- Например:
  - Раз в 2 недели Инженер ИБ контактирует с ответственными за несоответствия (по скайпу, письмо, лично)
  - Уточняет статус, помогает принять решения
- Либо формальный подход (не рекомендуется)
  - Проверять несоответствия при следующем аудите

# Требования к внутренним аудиторам (формальные и живые)

# Требования к внутренним аудиторам

- Должны быть установлены и зафиксированы в обязательном порядке
- Пример:

  - Опыт работы не менее 1 года в ИТ области
  - Знание стандартов ИСО 27001 и ИСО 27002
  - Знание процедур, политик СМИБ Компании
  - Знание процесса проведения аудита (на практическом уровне)
  - Личные качества
    - Независимость
    - Беспристрастность
    - Компетентность
  - Постоянное совершенствование навыков

# Практическая реализация

- Менеджер ИБ отвечает за ведение и своевременное обновление **Списка внутренних аудиторов**
  - Т.е. необходимо создать такой список, регулярно обновлять
- Зафиксировать факты:
  - тренинга был *Обучение было проведено сертифицированным внутренним аудитором Великим Аудитором - < ссылка на подтверждающие материалы>*
  - С использованием материалов - ссылка на презентации
  - По итогу выслан тест и выставлена оценка - ссылка на тест с результатами

| Аудитор | Должность | Последнее обучение | Локация | Прохождение экзамена | Комментарий |
|---|---|---|---|---|---|
| Иванов Андрей | Менеджер ИБ | 06.04.2018 | Минск | Да | |
| Петр Курицкий | Специалист ИБ | 06.04.2018 | Минск | | |
| Владимир Фьюжн | Специалист ИБ | 06.04.2018 | Минск | | |

# Хитрые вопросы

- Как произвести оценку работы внутренних аудиторов?
- Как сформировать команду внутренних аудиторов?
- Как получить реальный анализ причин несоответствия? Как убедиться что все несоответствия исправлены вовремя, и не вызвали новых несоответствий?

# Программа курса: Внутренний аудитор СМИБ

isqa.ru Information Security

- 1-дневный курс, на базе Softline
- Ускоренный тренинг (1 день) рассчитан на получение знаний по подготовке и проведению внутреннего аудита СМИБ в соответствии со стандартами ISO 27001 и ISO 19011.
- По результатам курса, слушатели получат знания как по практическим особенностям аудита, так и по формальным критериям, предъявляемым к процессу аудита и аудиторам со стороны сертифицирующих органов во время сертификации ИСО 27001

Модуль 1 Стандарт ISO/IEC 27001, СМИБ
- Термины ИБ и аудита
- Серия стандартов ИСО 2700х
- Структура ИСО 27001 и ИСО 27002 – в контексте аудита
- Связь процесса «Аудит ИБ» с другими процессами СМИБ

Модуль 2 ИСО 19011 и 27007
- Виды аудитов, способы работы
- Стандарты ИСО 19011 и 27007

Модуль 3 Внутренний аудит СМИБ
- Общий процесс управления аудитами СМИБ
- Процедурная и инструментальная поддержка внутреннего аудита ИБ
- Планирование, управление программой и планом аудита
- Проведение аудита: структура встреч, практические особенности взаимодействия
- Пост-аудит активности: отчетность, мониторинг

Модуль 4 Работа с несоответствиями
- Инструменты/подходы анализа причин несоответствий (Root Cause Analysis)
- Метод 5W2H, 5Why, диаграмма Ишикавы и др.
- Мониторинг несоответствий

Модуль 5 Требования к внутренним аудиторам
- Требования к внутренним аудиторам, оформление
- Обучение аудиторов

Модуль 6 Экзамен внутреннего аудитора

Алексей Евменков, CISM
ISACA
evmenkov@gmail.com