Внедрение СУИБ, соответствующей ИСО 27001, в ИТ компании

Алексей Евменков. Tieto

Software Engineering Forum

S·E·F

План презентации

- Введение
- Теория
- Практика
- Заключение

Software Engineering Forum

S·E·F

Введение

Software Engineering Forum
S·E·F

Термины и определения

- ИБ = Информационная Безопасность (information security):
  - свойство информации сохранять **конфиденциальность**, **целостность** и **доступность**. [Источник: ГОСТ Р ИСО/МЭК 27001:2006]

- СУИБ = Система Управления Информационной Безопасностью:
  - **часть** общей системы менеджмента,
  - основанная на использовании методов оценки **бизнес-рисков**
  - для разработки, внедрения,функционирования, мониторинга, анализа, поддержки и улучшения **информационной безопасности**. [Источник: ГОСТ Р ИСО/МЭК 27001:2006]

- Альтернативное определение СУИБ:
  - Система, основанная на управлении **бизнес-рисками**
  - Для защиты **активов** (assets) выбираются и внедряются **соответствующие защитные меры** (security controls)

Software Engineering Forum
S·E·F

Зачем необходима СУИБ?

- Бизнес-риски срабатывают, а Вы о них даже не подозревали?
- Ваши партнеры не считают Вас вполне надежными?
- Ваша внутренняя информация не всегда под контролем?
- Ваши процессы не совсем зрелые в области ИБ?
- Вы более пассивны чем проактивны в области ИБ?

- У Вас воруют лаптопы? ☺

Пора внедрять СУИБ !

Software Engineering Forum
S·E·F

Преимущества сертифицированной СУИБ

- Стандарт содержит разумную, выверенную последовательность действий, которую всегда можно подправить под собственные нужды
- Один раз сертифицирован, признан везде!
- Ежегодное подтверждение сертификата поддерживает тонус

Software Engineering Forum
S·E·F

Основная причина сертификации СУИБ

- Заказчик требует\повышение конкурентоспособности

Software Engineering Forum

SEF

Сколько ИСО 27001 сертификатов в мире?

Number of Certificates Per Country

Japan	2999*	France	12	Oman	
India	441	Iceland	12	Peru	
UK	395	Pakistan	12	Portugal	
USA	86	Slovenia	9	Kazakhstan	
Czech Republic	71	Sweden	9	Morocco	
Hungary	64	Slovakia	6	Ukraine	
Italy	59	South Africa	6	Argentina	
Poland	39	Switzerland	6	Armenia	
Spain	35	Bahrain	5	Belgium	1
Hong Kong	31	Colombia	5	Kyrgyzstan	1
Austria	30	Croatia	5	Lebanon	1
Australia	29	Indonesia	5	Lithuania	1
Ireland	29	Kuwait	5	Luxembourg	1
Malaysia	26	Bulgaria	4	Macedonia	1
Brazil	21	Gibraltar	4	Belarus	1
Thailand	21	Norway	4	Mauritius	1
Mexico	20	Qatar	4	Moldova	1
UAE	18	Sri Lanka	4	New Zealand	1
Turkey	18	Chile	3	Uruguay	1
Greece	15	Egypt	3	Yemen	1
Romania	15	Iran	3	Relative Total	5333
Netherlands	13	Macau	3	**Absolute Total**	**5314**

Macedonia 1

Belarus 1

Uruguay 1

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 o ISO/IEC 27001:2005
TietoEnator JLLC	Belarus	IND82117	Bureau Veritas Certification	ISO/IEC 27001:2005

Software Engineering Forum

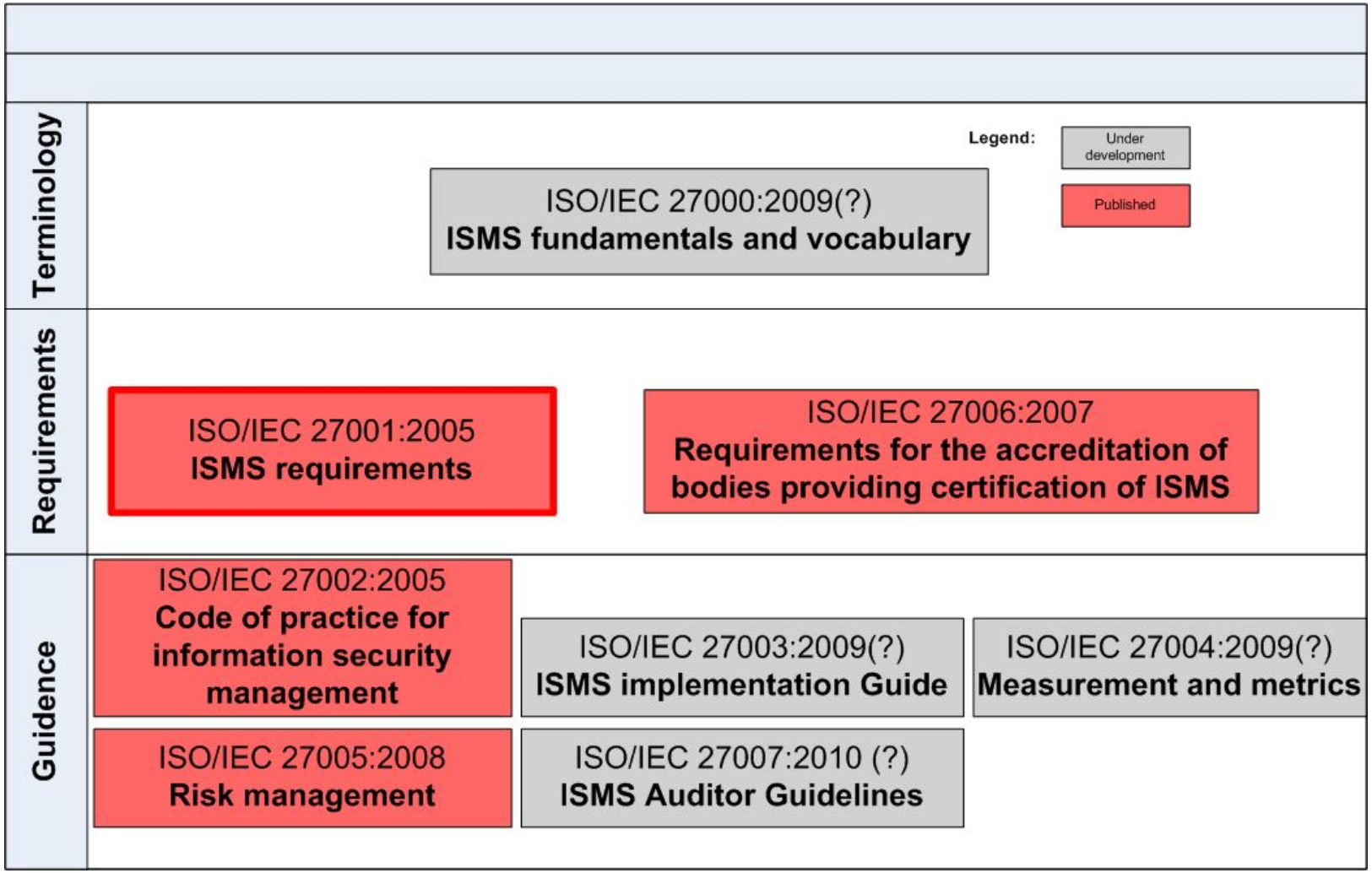
S·E·F

Теория

Software Engineering Forum

S·E·F

Семейство стандартов ИСО 27000



Software Engineering Forum

S·E·F

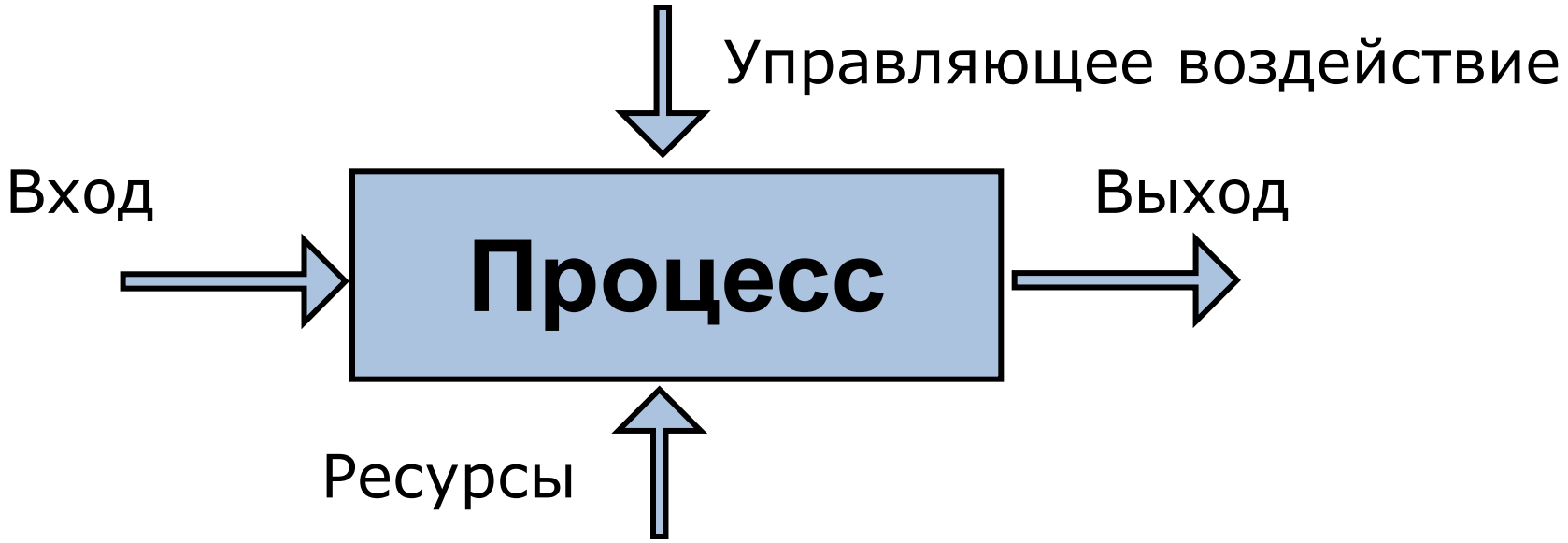
Принципы ИСО 27001

- Процессный подход
- Цикл PDCA (Plan-Do-Check-Act)

Software Engineering Forum

S·E·F

Процессный подход



Процессный подход (пример)

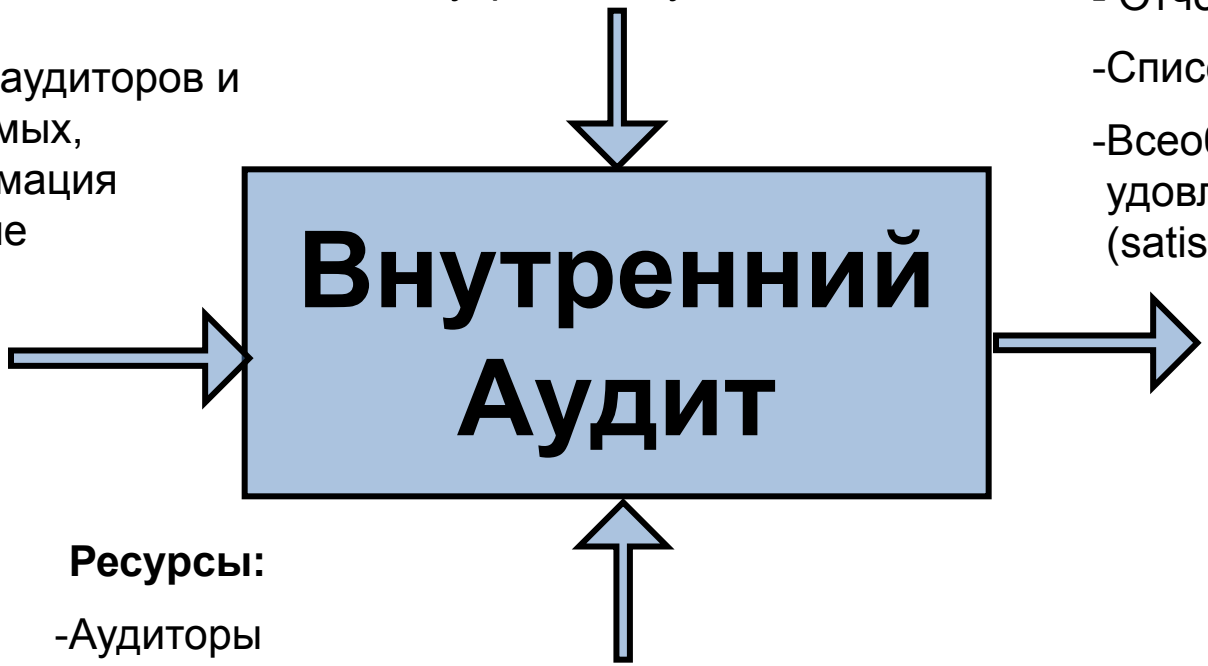
Вход:

- Название отдела,
- План,
- Имена аудиторов и аудируемых,
- Информация об отделе

Управление: процедура «Внутренний аудит»

Выход:

- Отчет по аудиту
- Список несоответствий
- Всеобщее удовлетворение (satisfaction) ☺



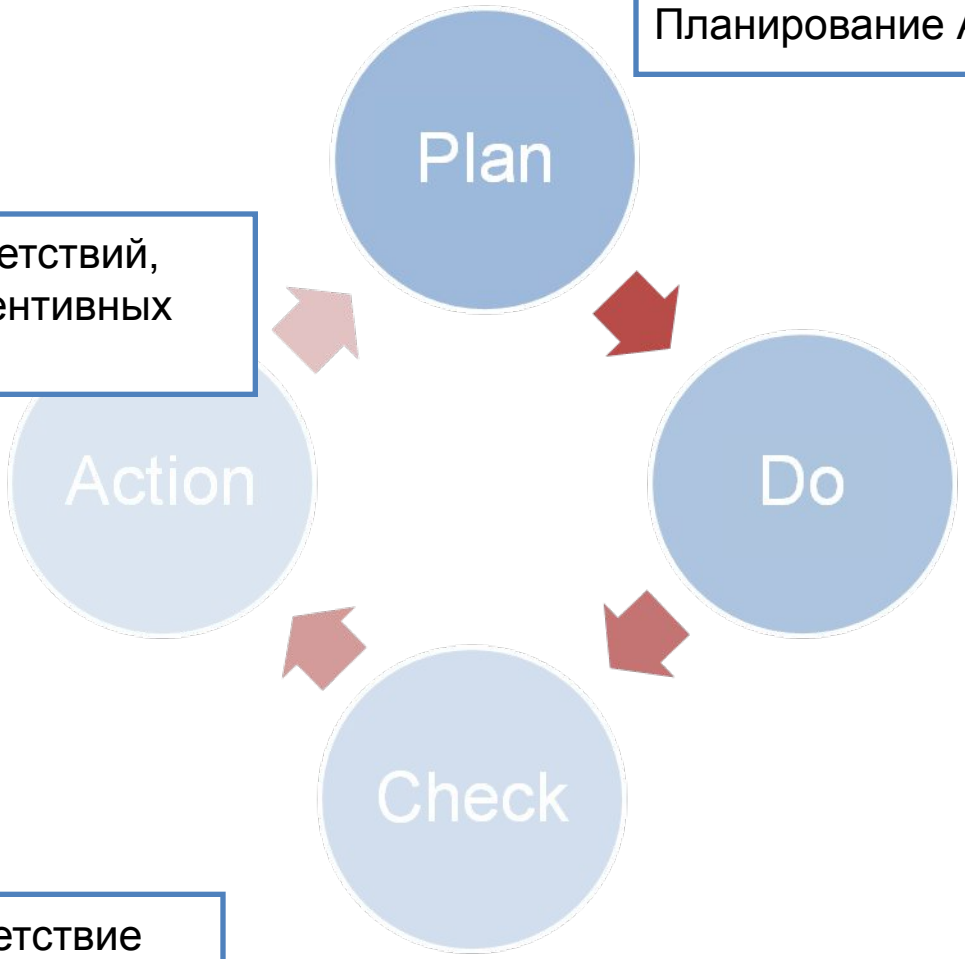
Ресурсы:

- Аудиторы
- Аудируемые

Software Engineering Forum
S·E·F

Цикл PDCA (пример)

Планирование Аудитов



Осуществление аудитов

Проверка на соответствие требованиям ИБ

Устранение несоответствий, планирование превентивных действий

Software Engineering Forum
S·E·F

Риски – центральная тема СУИБ

- Мало кто знает, что ...
- За год от падения кокосов погибает в десятки раз больше людей, чем от акул
  - Часто мы боимся не то, что нужно

- Мужчины поражаемы молнией в 4 раза более часто чем женщины
  - В жизни бывают странные закономерности

- Шанс выйграть в лотерею обычно ~1 из 14млн. Шанс заболеть птичьим гриппом 1 из 100млн.
  - Наши ожидания и страхи зачастую иррациональны, пока не проанализируешь их

Риски – центральная тема СУИБ

- Риски необходимо **учитывать**
- **Разные** риски должны обрабатываться «по-разному»

- СУИБ предоставляет набор инструментов по управлению рисками

Software Engineering Forum

S·E·F

Управление рисками в СУИБ

- **Угроза** - причина нежелательного инцидента, который может привести к негативным последствиям для организации .
- **Уязвимость** – недостаток нформационного ресурса или группы ресурсов, который способствует реализации угрозы.
- **Риск** - комбинация вероятности срабатывания угрозы через уязвимость, с последующим уроном для активов организации
- **Защитная мера** – действия по минимизации риска

Некто может пробраться в офис и украсть лаптоп

- Нет системы доступа в офис
- Отсутствуют кабели-замки для компьютеров

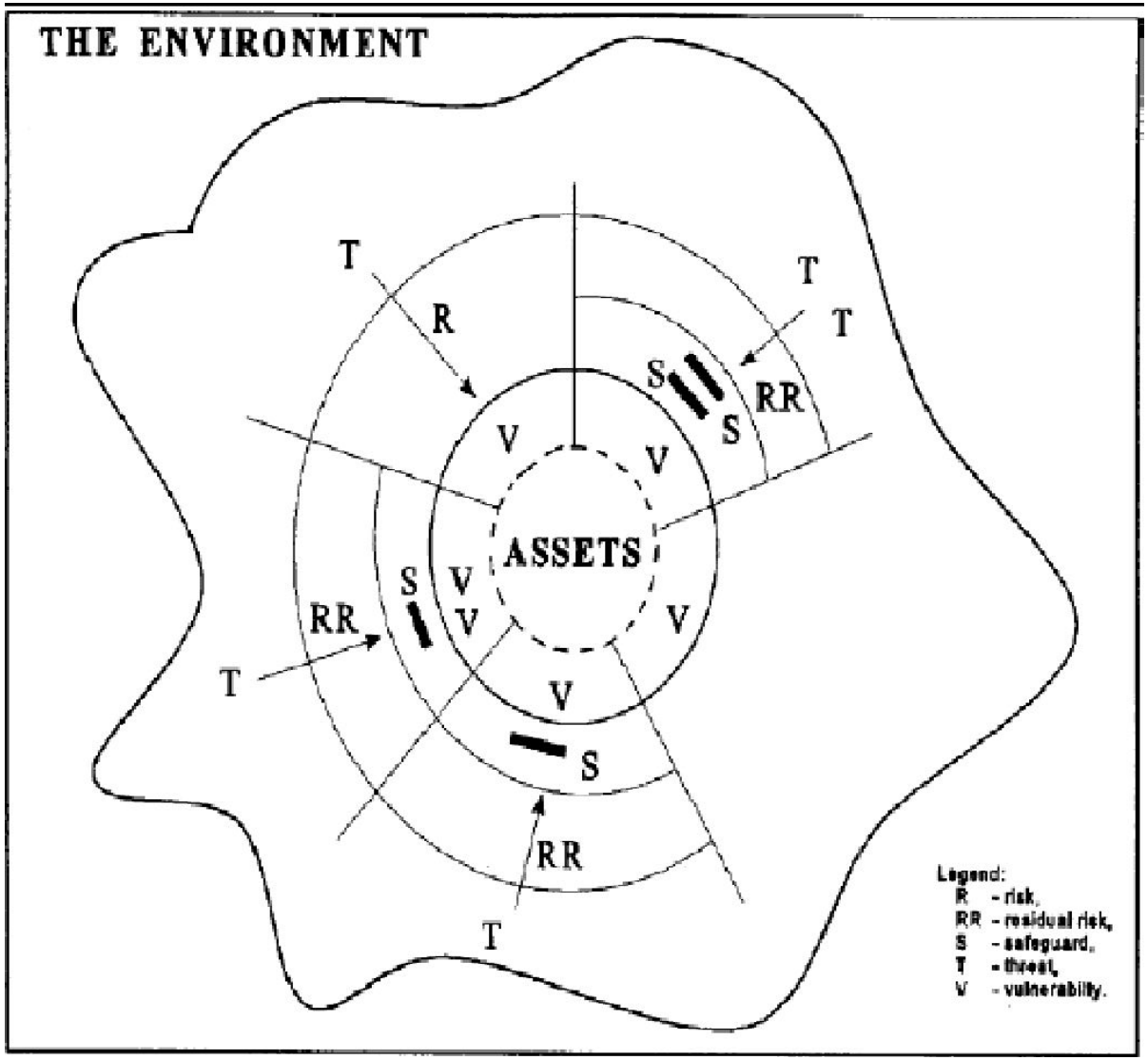
Некто проникнет в офис и украдет компьютер по причине отсутствия кабеля-замка

Внедрить в практику использование специальных кабелей-замков для всех портативных компьютеров

Software Engineering Forum

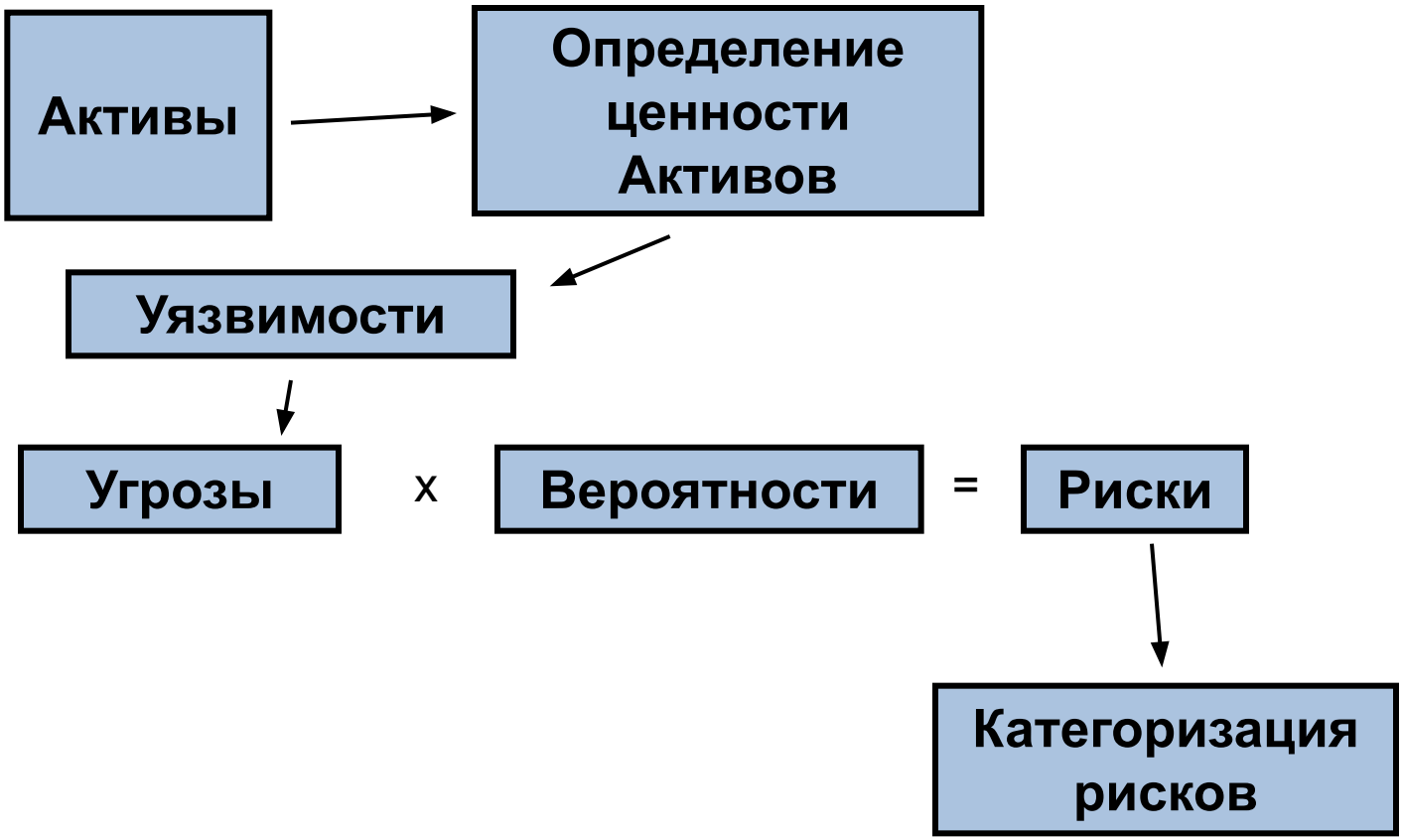
S·E·F

Управление рисками в СУИБ



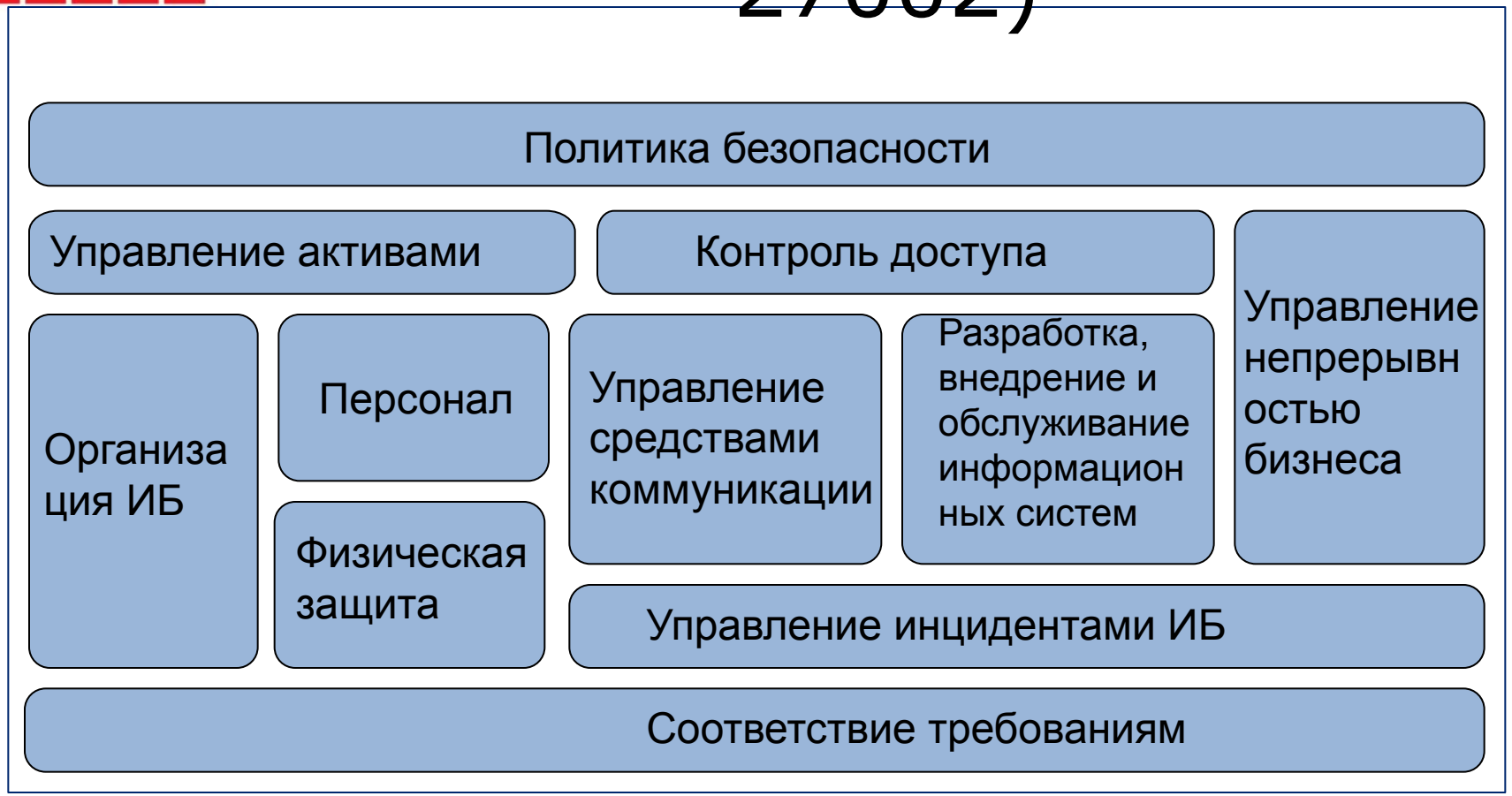
Software Engineering Forum
S·E·F

Процесс оценки рисков



Software Engineering Forum
S·E·F

Список защитных мер (ИСО 27002)



Software Engineering Forum

S·E·F

Практика

Software Engineering Forum

S·E·F

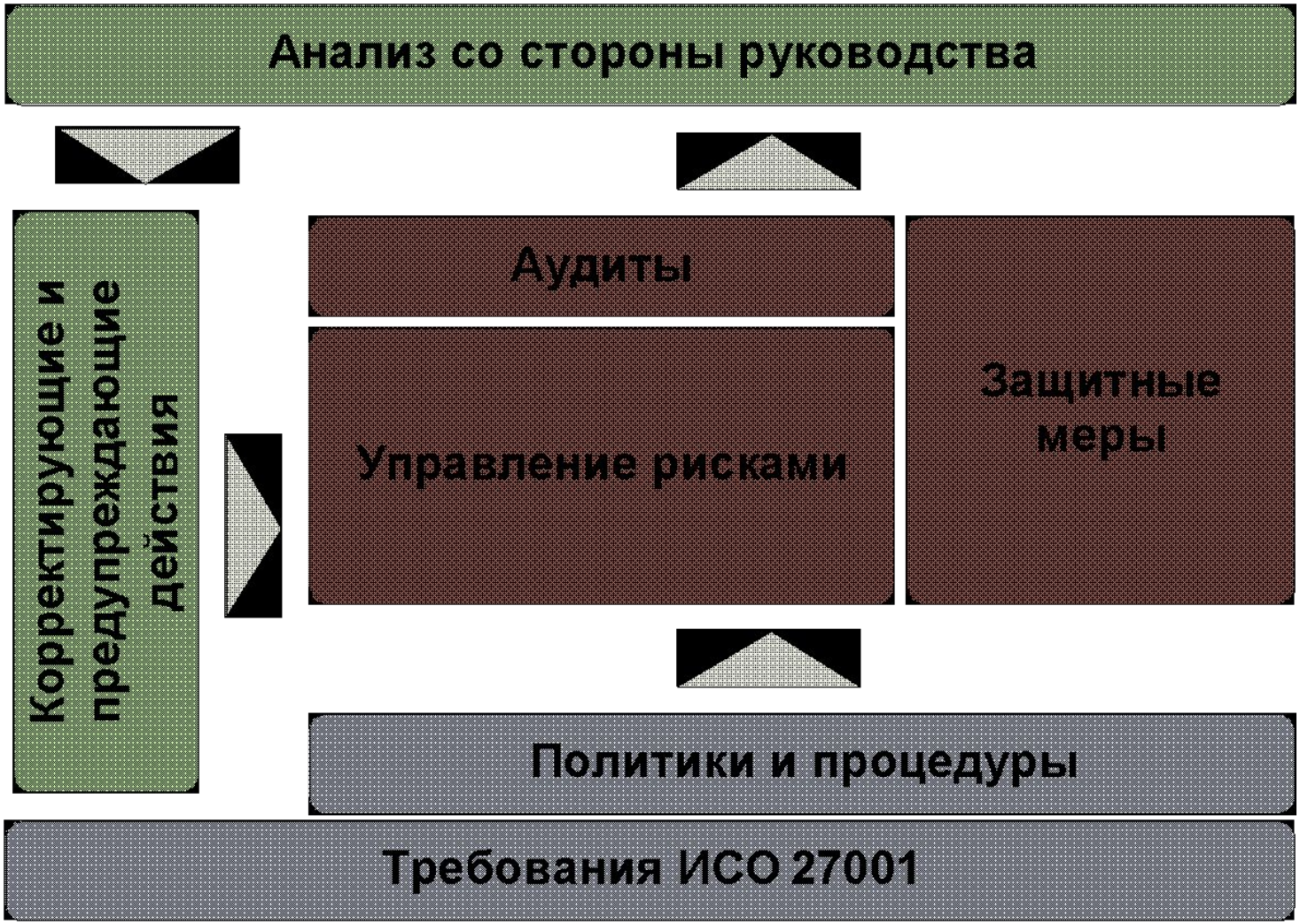
Вызовы при создании СУИБ

- Необходимость в установлении специфических процессов
  - Например, измерение эффективности защитных мер, аудиты по безопасности
- Создание комплекта документации
  - Шаблоны, практики, собственно сам документооборот
- Необходимость в автоматизация процессов
  - Например, управление рисков очень трудоемко без автоматизации
- Организационные аспекты
  - Ответственные за политики, тренинг персонала, как получить «вовлеченность менежмента» (management commitment)
- Сложный процесс сертификации

Software Engineering Forum

S·E·F

Схема функционирования СУИБ

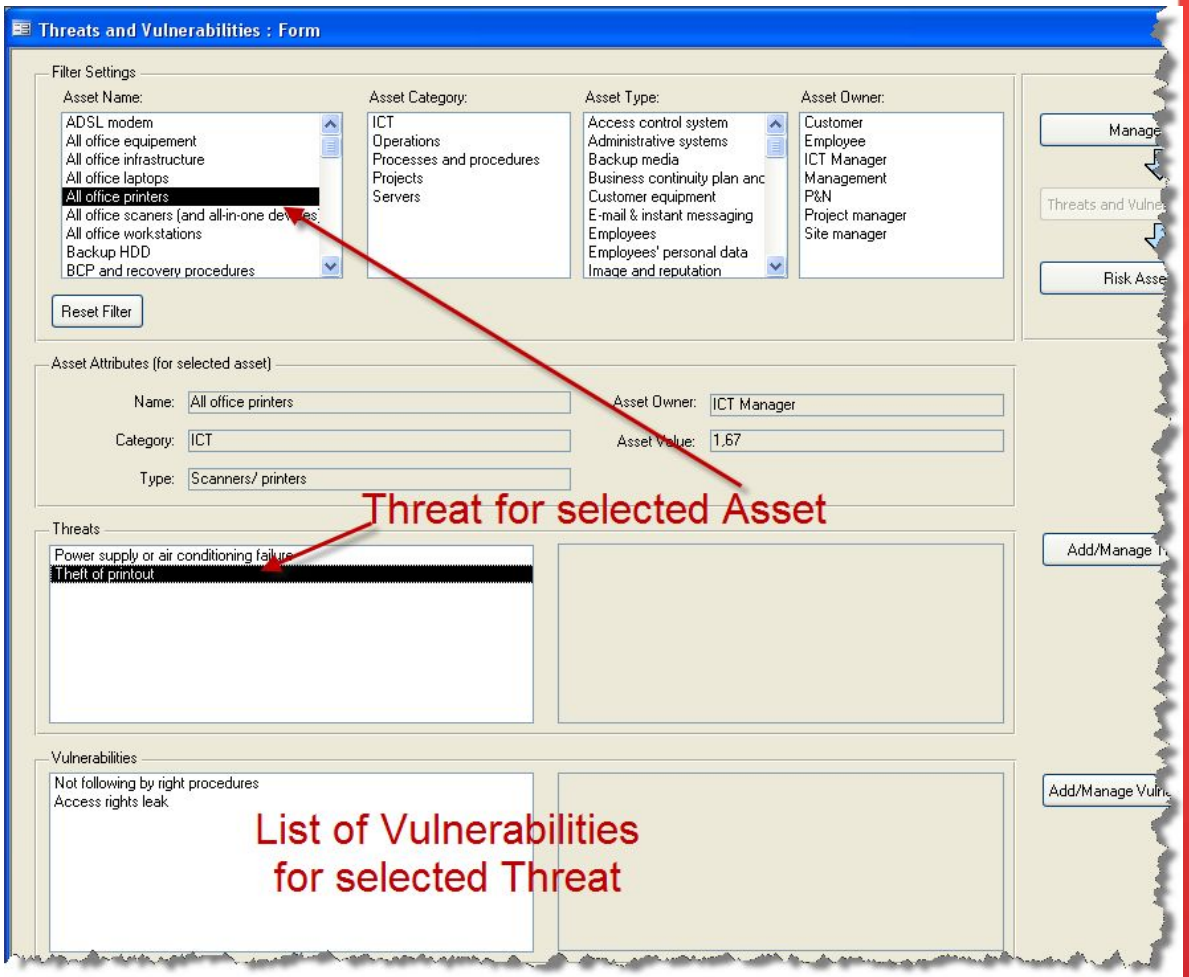


Software Engineering Forum

S·E·F

Пример определения угроз и уязвимостей

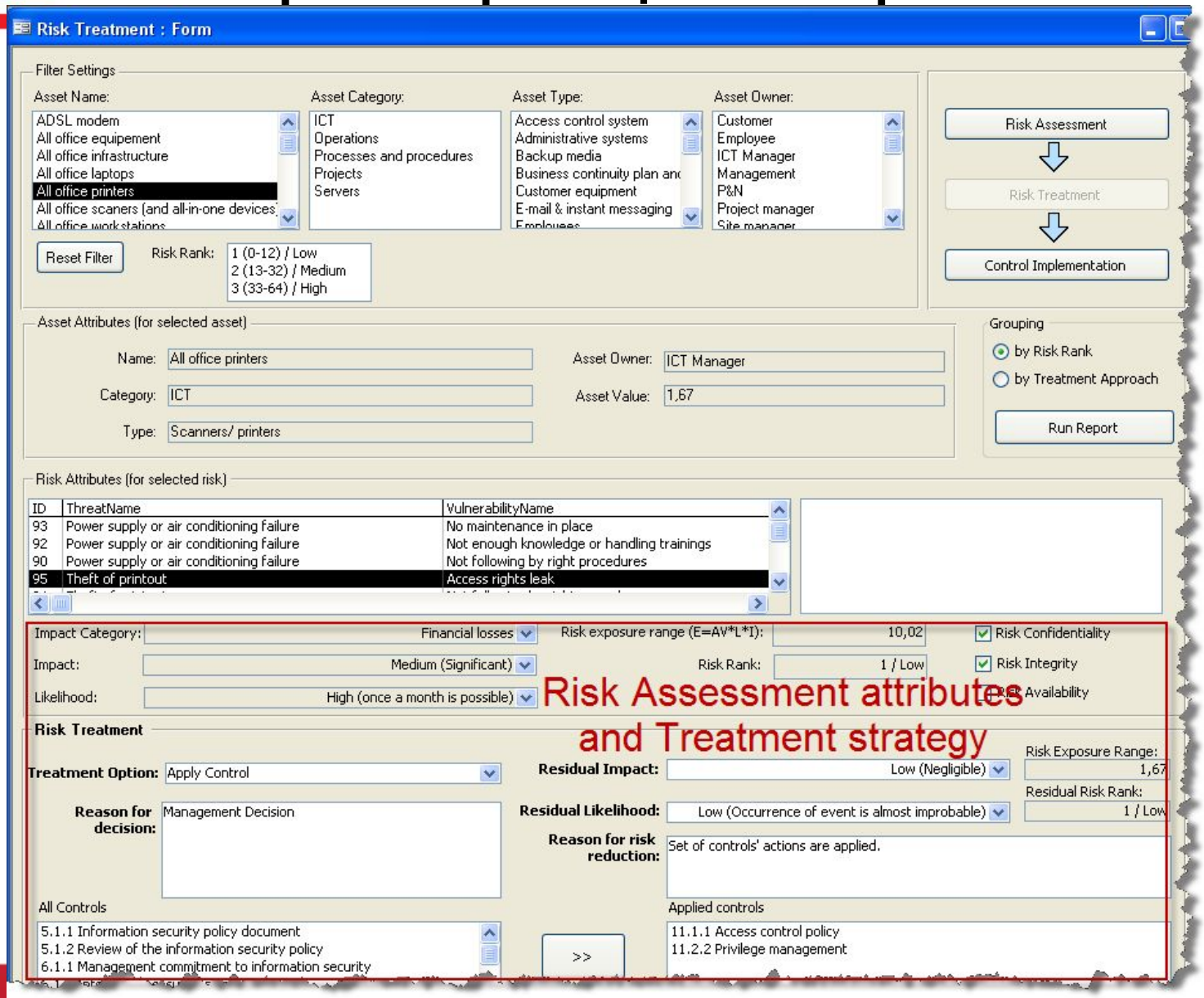
- Фильтрация по доступным активам
- Определение списка угроз для выделенного актива
- Определение уязвимостей, посредством которых данная угроза может реализоваться



Software Engineering Forum

SEF

Пример оценки рисков

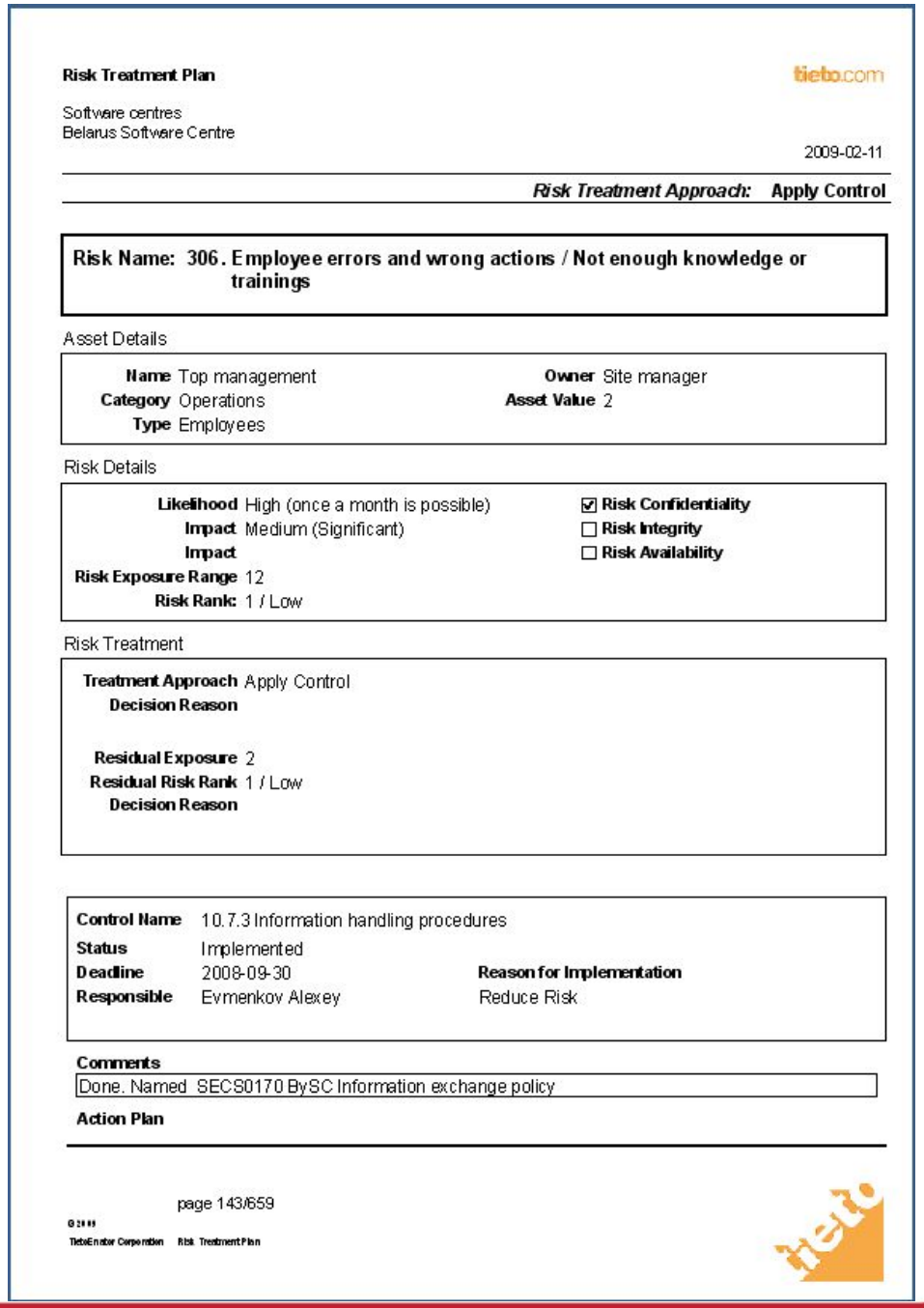


Software Engineering Forum

SEF

Отчеты

- Стандарт требует некоторые обязательные отчеты
  - Например план по обработке рисков (Risk Treatment Plan)
  - Положение о применимости (Statement of Applicability)
- Важно динамическая генерация отчетов
- Доступ к любой информации в базе



Risk Treatment Plan tieto.com

Software centres
Belarus Software Centre

2009-02-11

Risk Treatment Approach: **Apply Control**

Risk Name: 306. Employee errors and wrong actions / Not enough knowledge or trainings

Asset Details

Name Top management
Category Operations
Type Employees
Owner Site manager
Asset Value 2

Risk Details

Likelihood High (once a month is possible)
Impact Medium (Significant)
Impact
Risk Exposure Range 12
Risk Rank: 1 / Low

☑ **Risk Confidentiality**
☐ **Risk Integrity**
☐ **Risk Availability**

Risk Treatment

Treatment Approach Apply Control
Decision Reason

Residual Exposure 2
Residual Risk Rank 1 / Low
Decision Reason

Control Name 10.7.3 Information handling procedures
Status Implemented
Deadline 2008-09-30
Responsible Evmenkov Alexey
Reason for Implementation Reduce Risk

Comments
Done. Named SECS0170 BySC Information exchange policy

Action Plan

page 143/659

©2008
TietoEnator Corporation Risk Treatment Plan

Software Engineering Forum
S·E·F

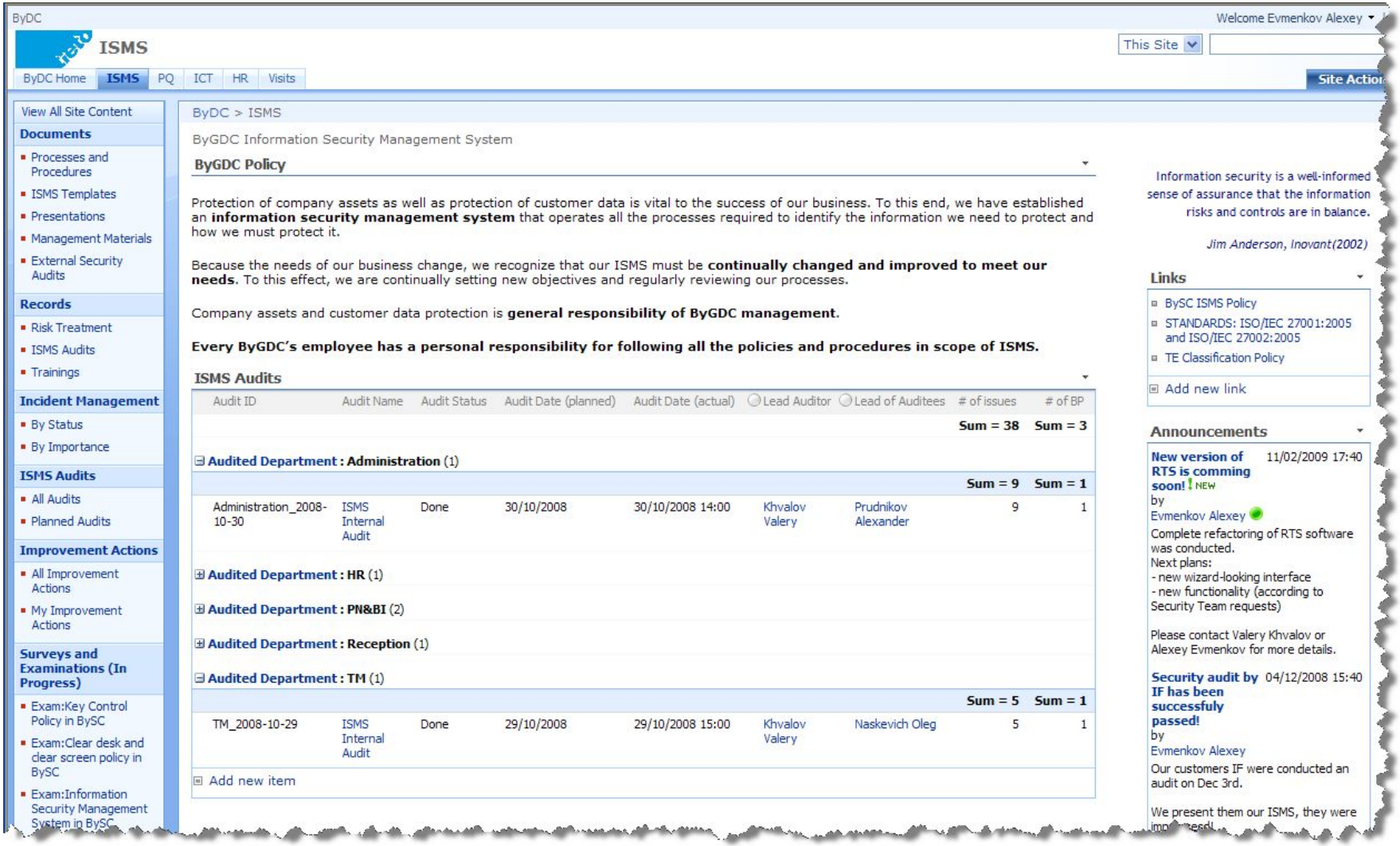
ISMS Portal

- Необходимо создать «единую точку входа» для всех сотрудников организации
- Автоматизированный документооборот (версионность, workflows)

Software Engineering Forum

S·E·F

ISMS Portal - реализация

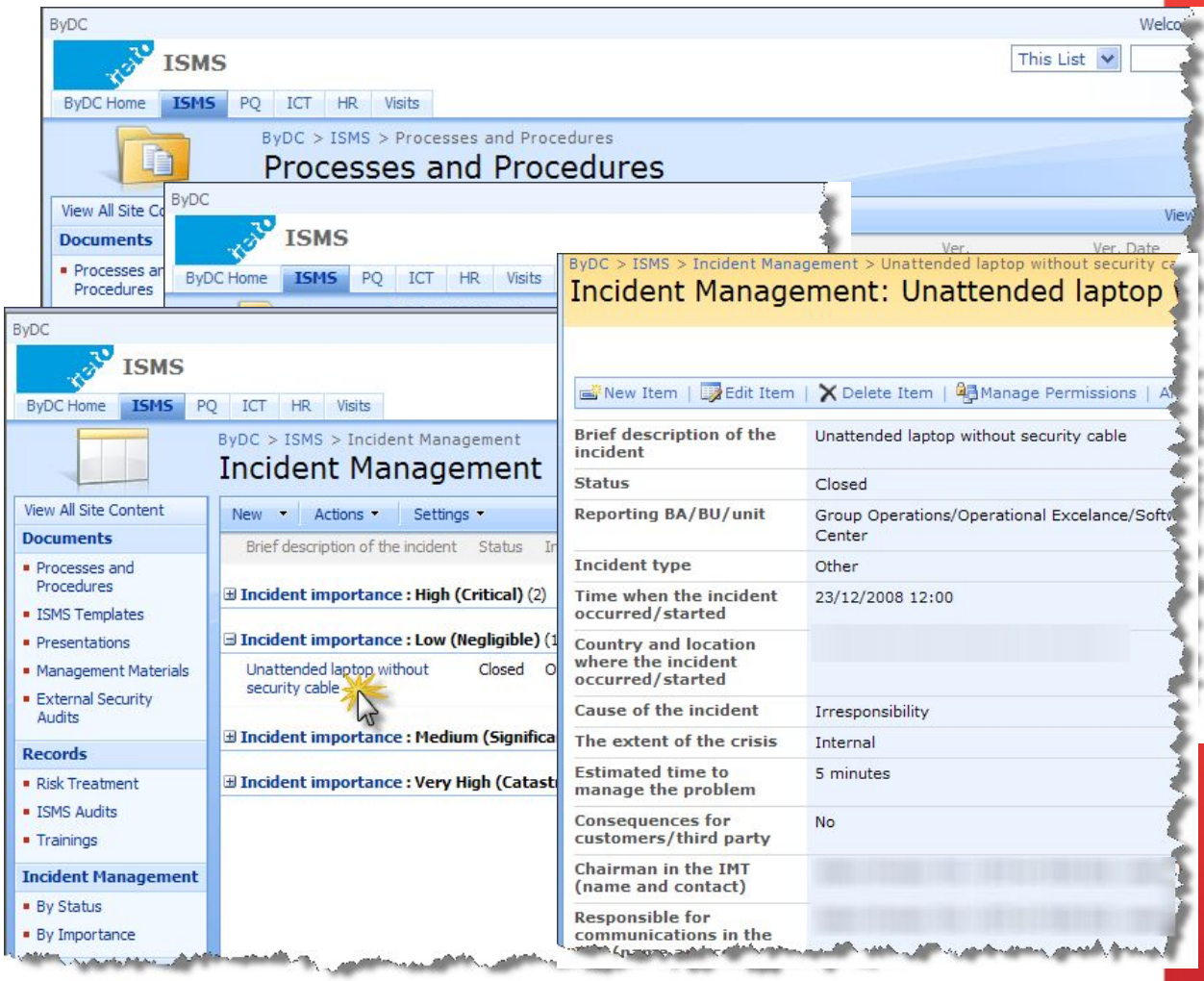


Software Engineering Forum

SEF

ISMS Portal - примеры

- **Документация**
- **Записи**
  - Тренинги
  - Метрики
  - Аудиты
  - И т.д.
- **Управление инцидентами**

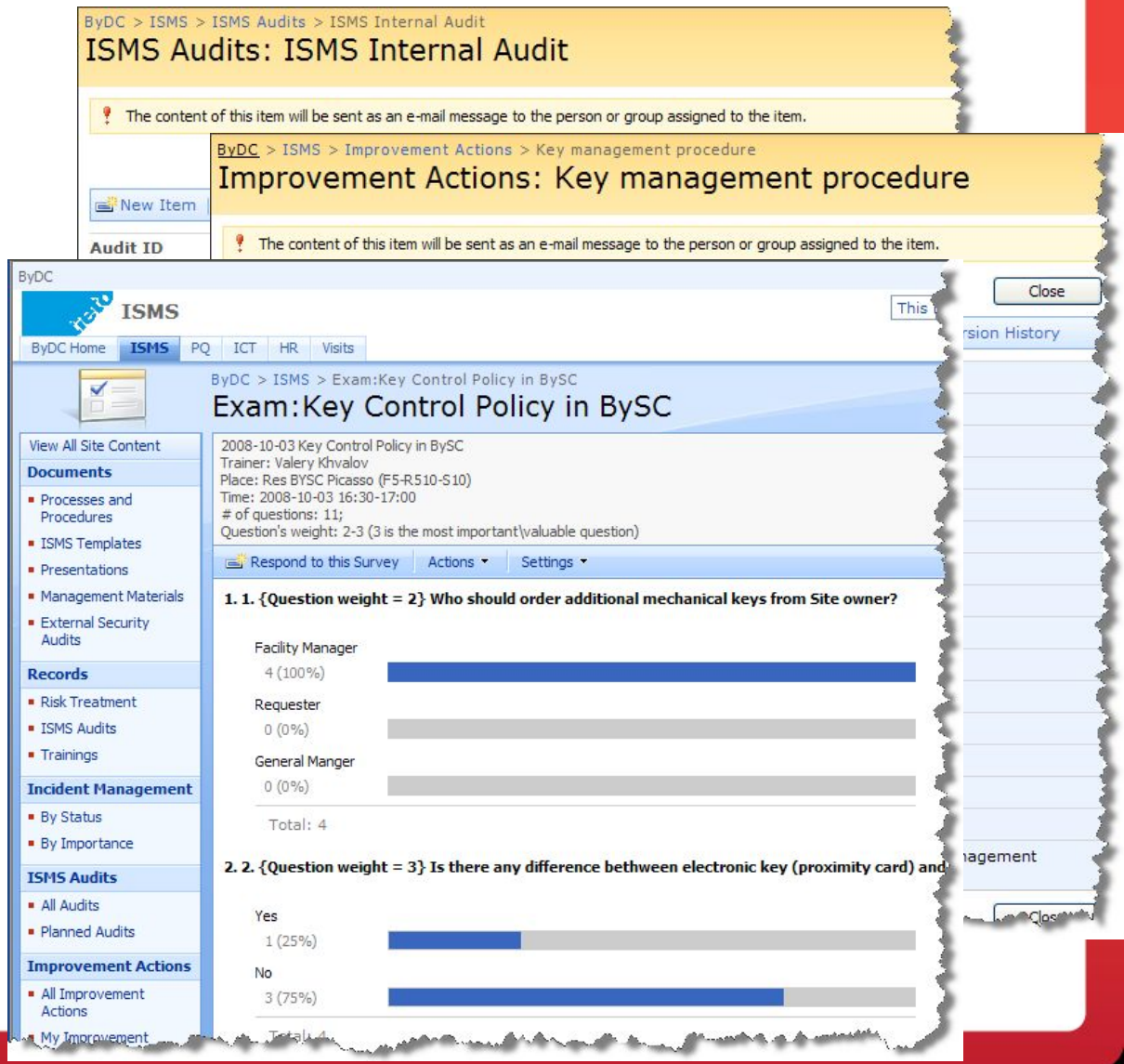


Software Engineering Forum

S·E·F

ISMS Portal - примеры

- **Аудиты**
  - Записи об аудите
  - Несоответствия
- **Экзамены и оценка тренинга**
- **Линки, объявления, календари, задачи и многое другое.**



Software Engineering Forum

S·E·F

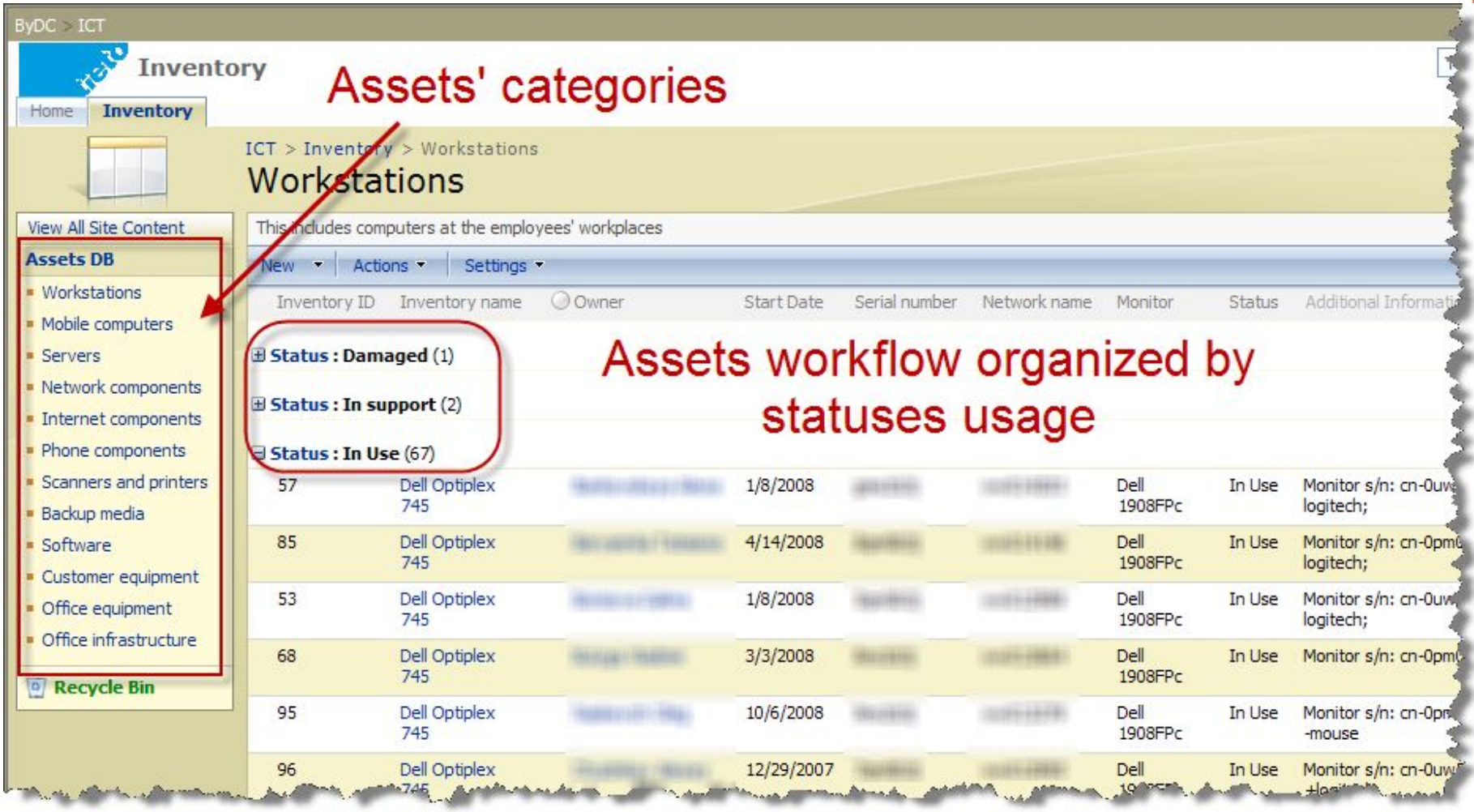
Inventory DB

- Детальное управление активами
- Оперативное отслеживание статуса активов
- Возможность настройки под любые типы активов

Software Engineering Forum

SEF

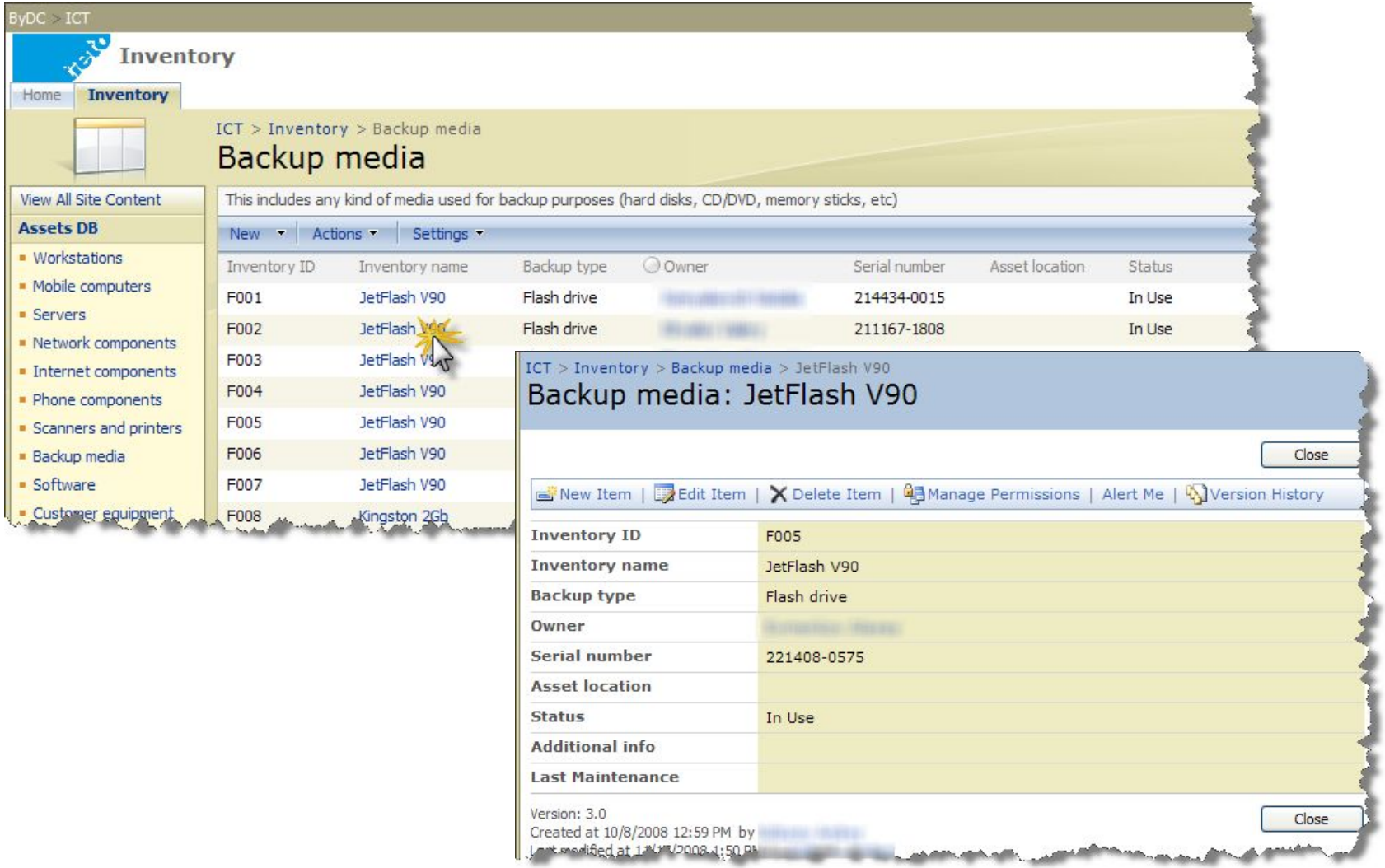
Inventory DB - реализация



Software Engineering Forum

S·E·F

Inventory DB - реализация



Software Engineering Forum

S·E·F

Заключение

Software Engineering Forum
S·E·F

ИБ и разработка ПО

- Целый раздел защитных мер стандарта посвящен «правильной разработке ПО»: «Разработка, внедрение и обслуживание информационных систем»

- В целом содержит здравые рекомендации по разработке
  - Например «проверка достоверности входных данных», «целостность сообщений»

- На практике все выливается финансовые возможности Ваши\заказчика
- Также важен профессионализм Ваших разработчиков
  - Правила хорошего программирования покрывают большинство требований стандарта

Software Engineering Forum
S·E·F

Процесс сертификации

- Тема для отдельного разговора (выбор сертифицирующего органа, общение с консалтерами, внутренняя организация)

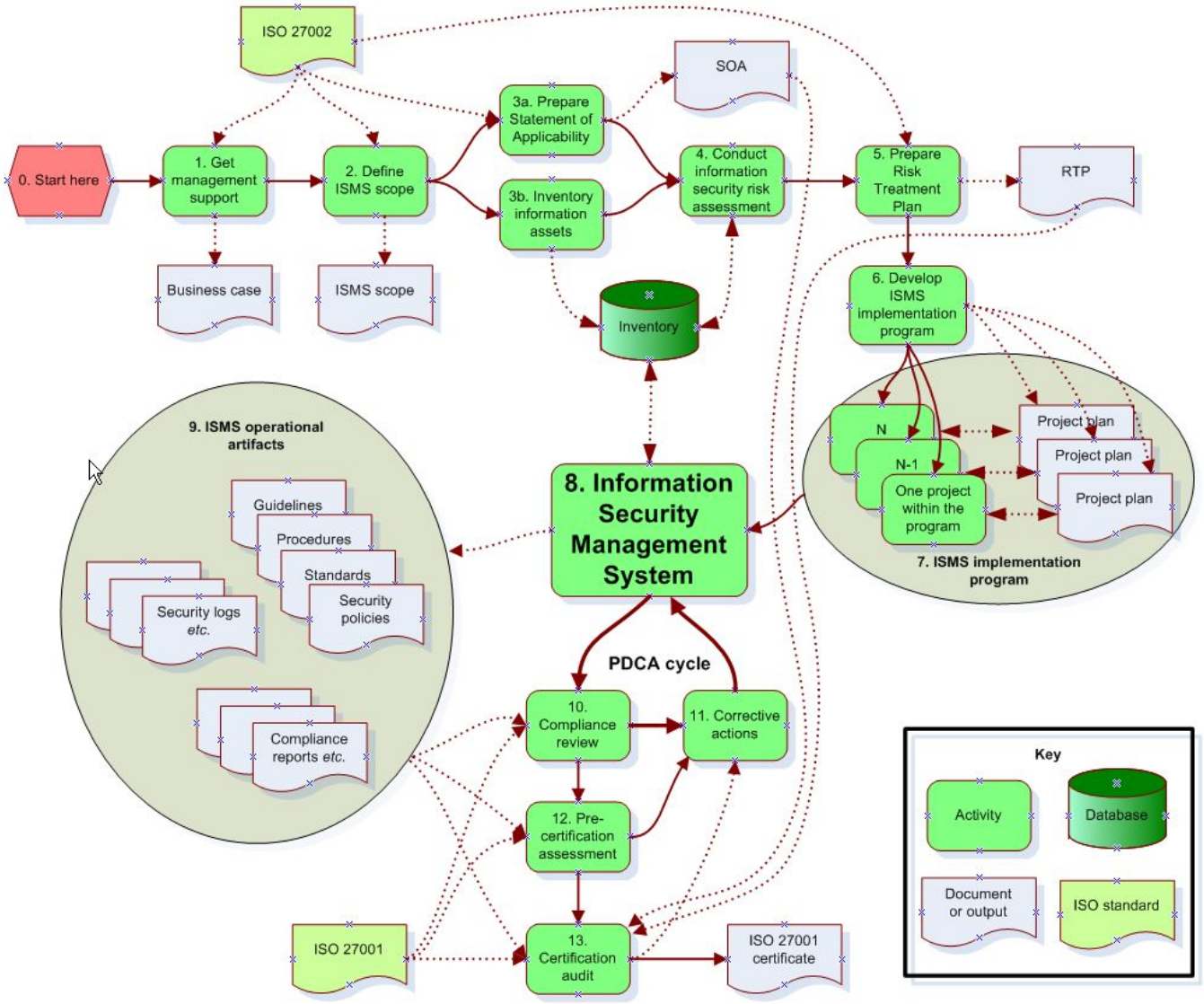
Некоторые рекомендации:

- Требует серьезного подхода, детального планирования, «вовлеченности руководства»
- При отсутствии собственных специалистов по безопасности, проходивших сертификацию – рекомендуется нанять организацию – консалтера
- Тренинги – основа работающей на практике СУИБ; также формально закрывает многие требования стандарта

Software Engineering Forum

S·E·F

Процесс сертификации



Software Engineering Forum

S·E·F

Вопросы и ответы

Спасибо за внимание!

Вопросы?